เอกสารแนบท้ายประกาศ

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมทางหลวง
พ.ศ.๒๕๖๖

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบายและการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วยหลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมทางหลวงจึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวง ประจำปีงบประมาณ พ.ศ.๒๕๖๖ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในกรมทางหลวง เพื่อให้บุคลากรทุกคนในกรมทางหลวง มีความรู้ เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวง และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

กรมทางหลวง

สารบัญ

หน้าที่

บทนำ

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรที่ต้องได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ยังคงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีความสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๒. วัตถุประสงค์

เพื่อให้กรมทางหลวงสามารถใช้ระบบเทคโนโลยีสารสนเทศประกอบการปฏิบัติงาน การดำเนินการใด ๆ ด้วยวิธีทางอิเล็กทรอนิกส์ การให้บริการหน่วยงานและประชาชนได้อย่างเหมาะสมมีประสิทธิภาพ ตลอดจนเป็นการสร้างความเชื่อมั่นของหน่วยงานและประชาชนต่อการดำเนินการของกรมทางหลวง จึงได้จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวงขึ้น โดยแต่ละส่วนประกอบด้วย วัตถุประสงค์ รายละเอียด และขั้นตอนของแนวทางในการปฏิบัติ

๓. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทางหลวง โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ และมาตรฐานสากล ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ โดยแนวทางปฏิบัตินี้ประกอบด้วย วัตถุประสงค์ และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมทางหลวง

๔. บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมทางหลวง บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุนและติดตามการประยุกต์ใช้โดยอธิบดีกรมทางหลวง

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อธิบดีกรมทางหลวงเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๕. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทางหลวงฉบับนี้จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) กรมทางหลวง จัดพิมพ์เผยแพร่เพื่อให้บุคลากรกรมทางหลวง และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

คำนิยาม

๑. หน่วยงาน หรือ องค์กร หมายถึง กรมทางหลวง

๒. ผู้บริหารระดับสูง หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของกรมทางหลวง

๓. การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศของกรมทางหลวง

๔. ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่

๔.๑ ผู้บริหารสูงสุด หมายความว่า อธิบดีกรมทางหลวง

๔.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer : DCIO) หมายความว่า รองอธิบดีกรมทางหลวง ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๓ ผู้ดูแลระบบ/ผู้ดูแลห้องเครื่อง หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์

๔.๔ ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอปพลิเคชัน

๔.๕ เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการของกรมทางหลวง

๔.๖ บุคคลภายนอก หมายความว่า บุคคลที่กรมทางหลวงอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมทางหลวงได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของกรมทางหลวง เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับกรมทางหลวง หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิต/นักศึกษาฝึกงาน

๕. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๖. สินทรัพย์ (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

๖.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๖.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๘. ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security) หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๙. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

๑๐. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวด ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ส่วนที่ ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล

๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

๑.๓ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้

๑.๓.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๑.๓.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๓.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓.๔ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

๒.๑ ประเภทข้อมูล แบ่งตามลักษณะการใช้งานได้ดังนี้

(๑) ข้อมูลด้านการบริหาร หมายถึง เอกสารหรือข้อมูลต่าง ๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเอง หรือได้รับจากภายนอกที่ใช้ในการบริหารหน่วยงาน มีความสำคัญและให้ล่วงรู้ได้เฉพาะบุคคลหรือกลุ่มบุคคลที่มีหน้าที่โดยตรงต่อข้อมูลนั้น ๆ ได้แก่ ข้อมูลสารสนเทศด้านการบริหารข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลงบประมาณการเงินและบัญชี

(๒) ข้อมูลภายใน (Internal Data) หมายถึง เอกสารหรือข้อมูลต่าง ๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเอง หรือได้รับจากภายนอกที่ใช้ภายในหน่วยงาน ได้แก่

(๒.๑) ข้อมูลสารสนเทศกระบวนการหลัก ประกอบด้วย ข้อมูลงานก่อสร้างทางหลวง ข้อมูลงานสะพาน ข้อมูลบริหารบำรุงทาง ข้อมูลงานอำนวยความปลอดภัย

(๒.๒) ข้อมูลสารสนเทศกระบวนการสนับสนุน ประกอบด้วย ข้อมูลงานเครื่องกลและสื่อสาร ข้อมูลงานจัดกรรมสิทธิ์ที่ดิน ข้อมูลบุคลากร

(๒.๓) ข้อมูลภูมิศาสตร์สารสนเทศงานทาง ประกอบด้วย ข้อมูลพิกัดทางหลวง ข้อมูลพิกัดสะพาน

(๓) ข้อมูลส่วนบุคคล (Personal Data) หมายถึง เอกสารหรือข้อมูลต่าง ๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ได้แก่ รหัสสมาชิก หมายเลขบัตรประชาชน ชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลอื่น ๆ ที่สามารถบ่งชี้ตัวบุคคลได้ ได้แก่ ข้อมูลบุคลากร ข้อมูลบุคคลที่มาติดต่อกรมทางหลวง

(๔) ข้อมูลที่เปิดเผยได้ หมายถึง เอกสารหรือข้อมูลต่าง ๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่สามารถเผยแพร่ให้ประชาชนหรือบุคคลทั่วไปรับทราบ ได้แก่ ข้อมูลสถิติอุบัติเหตุบนทางหลวง ข้อมูลระยะทางของทางหลวง ข้อมูลบริการประชาชน

๒.๒ ระดับความสำคัญของข้อมูล

(๑) ความสำคัญระดับเคร่งครัด มีความสำคัญและให้ล่วงรู้ได้เฉพาะบุคคลหรือกลุ่มบุคคลที่มีหน้าที่โดยตรงต่อข้อมูลนั้น ๆ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนอาจก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ ได้แก่

(สำคัญมาก) ได้แก่ ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย ข้อมูลคดีความ

(สำคัญปานกลาง) ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร ข้อมูลทะเบียนผู้รับเหมาก่อสร้างทาง

(๒) ความสำคัญระดับกลาง ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน ต่อบุคคลภายนอก อาจก่อให้เกิดความเสียหายแก่ประโยชน์ของหน่วยงาน หรือบุคลากรของหน่วยงาน ได้แก่ ข้อมูลสำหรับปฏิบัติงานภารกิจของหน่วยงาน

(๓) ความสำคัญระดับพื้นฐาน ได้แก่ ข้อมูลเผยแพร่ ข้อมูลเพื่อบริการประชาชน

๒.๓ ชั้นความลับของข้อมูล

(๑) ลับที่สุด หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

(๒) ลับมาก หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

(๓) ลับ หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

(๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ได้

๒.๔ การกำหนดให้ข้อมูลอยู่ในชั้นความลับใด ให้พิจารณาถึงองค์ประกอบต่อไปนี้

(๑) ความสำคัญของเนื้อหา

(๒) แหล่งที่มาของข้อมูล

(๓) วิธีการนำไปใช้ประโยชน์

(๔) จำนวนบุคลากรที่ควรรับทราบ

(๕) ผลกระทบหากมีการเปิดเผย

(๖) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ

๒.๕ ระดับชั้นการเข้าถึง

(๑) ระดับชั้นสำหรับผู้บริหาร

(๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๒.๖ เวลาที่เข้าถึงได้

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๒.๗ ช่องทางการเข้าถึง

ช่องทางที่สามารถเข้าถึง ได้แก่ ผ่านระบบอินเตอร์เน็ต ผ่านระบบอินทราเน็ต ผ่านระบบงานโดยตรง ผ่านเครื่องคอมพิวเตอร์ส่วนบุคคล ผ่านโทรศัพท์มือถือ ผ่านเจ้าหน้าที่หน่วยงานเป็นผู้ดำเนินการให้ เป็นต้น

ส่วนที่ ๒
การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ
(Business Requirement for access control)

วัตถุประสงค์

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ

๑.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๒ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๒. จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิและภารกิจ ดังนี้

๒.๑ กลุ่มผู้บริหาร ได้แก่ อธิบดี, รองอธิบดี, ผู้อำนวยการสำนัก/ศูนย์/กอง

๒.๒ กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศ

๒.๓ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของกรมทางหลวง

๒.๔ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับกรมทางหลวง

๒.๕ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

๓. การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๑ ทบทวนสิทธิการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อได้รับเอกสารแจ้งจากหน่วยงานต้นสังกัดของผู้ใช้งานระบบ เพื่อปรับปรุงการให้สิทธิแก่ผู้ใช้งานให้สอดคล้องกับการปฏิบัติงานที่เปลี่ยนไป เช่น เมื่อเปลี่ยนแปลงตำแหน่งงาน ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงานภายในองค์กร เป็นต้น

๓.๒ หน่วยงานต้นสังกัดของผู้ใช้งานต้องแจ้งเอกสารอย่างเป็นทางการแก่ผู้ดูแลระบบให้กำหนดสิทธิตามหน้าที่ความรับผิดชอบในการปฏิบัติงานเมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงาน หรือยกเลิกสิทธิต่าง ๆ ในการเข้าใช้ระบบสารสนเทศเมื่อมีผู้ใช้งานโยกย้าย หรือลาออก เป็นต้น

ส่วนที่ ๓
การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training)

(๑) เสริมสร้างความเข้าใจ ในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้งาน

(๒) จัดหลักสูตรฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒. การลงทะเบียนผู้ใช้งาน (User registration) มีขั้นตอนปฏิบัติครอบคลุมในเรื่องต่อไปนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ผู้ดูแลระบบตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้ซ้ำซ้อนกับบัญชีผู้ใช้งานที่มีอยู่เดิม

(๓) ผู้ดูแลระบบตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๔) ผู้ดูแลระบบจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งผู้ใช้งานต้องลงนามรับทราบด้วย

(๕) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบเทคโนโลยีสารสนเทศ

(๖) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๗) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๘) ผู้ดูแลระบบต้องทบทวนสิทธิของบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓. มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเหมาะสมตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานให้เหมาะสมกับระบบเทคโนโลยีสารสนเทศ

(๓) ผู้ดูแลระบบมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๔) ผู้ดูแลระบบต้องทบทวนสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๔. มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้ง หรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) ผู้ดูแลระบบต้องตั้งรหัสผ่านชั่วคราวที่ยากต่อการคาดเดา และต้องมีความแตกต่างกัน

(๓) ผู้ดูแลระบบต้องให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการคาดเดา

(๔) การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๕) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน

(๑) ผู้ดูแลระบบต้องทบทวนสิทธิอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๒) ผู้ดูแลระบบทบทวนสิทธิ ผู้ที่มีสิทธิในระดับสูง ได้แก่ สิทธิระดับผู้ดูแลระบบด้วยความถี่กว่าสิทธิระดับผู้ใช้งาน

ส่วนที่ ๔
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อย ดังนี้

แนวปฏิบัติ

๑. การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ ดังนี้

(๑) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ผู้ใช้งานต้องไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ผู้ใช้งานต้องไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) ผู้ใช้งานต้องเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ผู้ใช้งานต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในคอมพิวเตอร์

(๙) ผู้ใช้งานต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๑๐) ผู้ใช้งานต้องไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยต้องทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน

(๑๔) ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดิม

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน

(๒) ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๓) ผู้ใช้งานต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) ผู้ใช้งานทุกคนต้องออกจากระบบที่ใช้งานทันที เมื่อจำเป็นต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

(๒) ผู้ใช้งานมีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๓) ผู้ใช้งานทุกคนต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญของกรมทางหลวงไว้ในที่ปลอดภัย โดยเก็บไว้ในตู้เอกสารที่มีระบบล็อค และมีกุญแจเปิดปิด

(๔) ผู้ใช้งานต้องลงชื่อออก (Logoff) จากเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน และทำการล็อคประตูห้องระหว่างพักเที่ยงหรือเมื่อผู้ใช้งานกลับบ้านหลังเลิกงาน

(๕) ผู้ใช้งานต้องทำการล็อคประตูห้องที่มีเครื่องโทรสารระหว่างพักเที่ยง หรือเมื่อผู้ใช้งานกลับบ้านหลังเลิกงาน

(๖) ผู้ใช้งานต้องทำการป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

(๗) ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

(๘) ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๙) ข้อมูลสำคัญที่บันทึกไว้ในกระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟ หรือฮาร์ดดิสก์ เมื่อไม่ได้ใช้งานต้องเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

(๑๐) เอกสารสำคัญและสื่อบันทึกข้อมูลแบบใช้ครั้งเดียวที่ผ่านการใช้งานแล้ว ต้องถูกทำลายโดยการแยกทำลายโดยใช้เครื่องทำลายเอกสาร

(๑๑) เอกสารบนสื่อบันทึกข้อมูลแบบใช้ซ้ำต้องทำการลบข้อมูลแบบถาวรป้องกันการกู้คืน โดยใช้มาตรฐาน DoD 5220.22-M หรือมาตรฐานการลบทำลายข้อมูลที่สูงกว่า

๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ ดังนี้

ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

ส่วนที่ ๕
การจัดการการเข้าถึงระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมทางหลวง

แนวปฏิบัติ

๑. การเข้าใช้งานที่มั่นคงปลอดภัย

(๑) ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตเท่านั้น

(๒) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อบุคคลอื่น

(๓) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๔) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการพาณิชย์

(๕) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ไม่ว่าจะเป็นข้อมูลของกรมทางหลวงหรือบุคคลภายนอกก็ตาม

(๖) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของกรมทางหลวงหรือของบุคคลอื่น

(๗) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิในข้อมูลดังกล่าว

(๘) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายต่อกรมทางหลวง ได้แก่ การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังผู้ใช้งานหรือบุคคลอื่น เป็นต้น

(๙) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อขัดขวางการใช้งานระบบเทคโนโลยีสารสนเทศของกรมทางหลวงหรือของผู้ใช้งานอื่น หรือเพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมทางหลวงไม่สามารถใช้งานได้ตามปกติ

(๑๐) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวกับการดำเนินงานของกรมทางหลวงไปยังที่อยู่เว็บไซต์ใด ๆ ในลักษณะที่จะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

(๑๑) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย ในทางที่ผิดต่อกฎหมายหรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อกรมทางหลวง

(๑๒) ผู้ใช้งานต้องทำการเข้าถึงระบบเครือข่ายตามสิทธิและหน้าที่ของตนเองเท่านั้น ห้ามมิให้ทำการเข้าใช้งานระบบเครือข่ายโดยใช้สิทธิของผู้อื่น

๒. การเชื่อมต่อจากภายนอกองค์กร

(๑) การเข้าสู่เครือข่ายของกรมทางหลวงผ่านทางเครือข่ายภายนอก หรือระบบอินเทอร์เน็ต ต้องทำโดยผ่านทางช่องทางการเชื่อมต่อแบบปลอดภัย

(๒) การเข้าสู่เครือข่ายของกรมทางหลวงผ่านทางเครือข่ายภายนอก ต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง และต้องมีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ที่ได้ทำการใช้งานไว้ไม่ต่ำกว่า ๙๐ วัน

๓. การระบุอุปกรณ์บนเครือข่าย

(๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของกรมทางหลวงต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อนจึงจะสามารถดำเนินการได้

(๒) ผู้ดูแลระบบต้องทำการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดอุปกรณ์ที่นำมาเชื่อมต่อ IP Address และสถานที่ตั้ง

(๓) ผู้ดูแลระบบมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนด และระงับสัญญาณการเชื่อมต่อเมื่อสิ้นสุดการอนุญาต

(๔) ให้มีการจัดทำผังเครือข่าย (Network Diagram) ซึ่งมีการระบุรายละเอียดของอุปกรณ์บนเครือข่าย IP Address, Bandwidth, ช่วงเวลาที่อนุญาตให้เชื่อมต่อ มีขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก รวมถึงมีการปรับปรุงผังให้เป็นปัจจุบัน

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

(๑) มีการติดตั้งอุปกรณ์ IPS เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่าย

(๒) ผู้ดูแลระบบต้องทำการป้องกันอุปกรณ์เครือข่ายจากการเข้าถึงเพื่อเปลี่ยนแปลงค่าโดยไม่ได้รับอนุญาต โดยต้องทำการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึง โดยทำการปิดพอร์ตที่ไม่มีความจำเป็นในการใช้งาน และกำหนดพอร์ตเฉพาะในการเข้าถึงอุปกรณ์

(๓) ผู้ดูแลระบบต้องทำการกำหนดรหัสผ่านในการเข้าถึงเพื่อเปลี่ยนแปลงค่าของอุปกรณ์ให้ยากแก่การคาดเดา และมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

๕. การแบ่งแยกเครือข่าย

(๑) ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่ายแต่ละสำนักออกจากกัน เพื่อป้องกันการละเมิดสิทธิและทรัพยากรเครือข่ายของแต่ละหน่วยงาน

(๒) ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายออกเป็นโซน เพื่อความมั่นคงปลอดภัยของระบบงานจากการบุกรุกทางเครือข่าย

๖. การควบคุมการเชื่อมต่อทางเครือข่าย

(๑) ผู้ใช้งานมีสิทธิในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตนเอง

(๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการใช้งานเครือข่ายทุกครั้ง

(๓) ผู้ใช้งานต้องไม่นำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

(๔) ผู้ดูแลระบบต้องทำการตรวจสอบการเชื่อมต่อบนเครือข่ายหากพบการเชื่อมต่อจากอุปกรณ์นอกเหนือจากที่ได้รับอนุญาตต้องทำการระงับการเชื่อมต่อโดยทันที

(๕) ผู้ดูแลระบบต้องทำการจำกัดสิทธิในการใช้งานระบบเครือข่ายร่วมกัน ได้แก่ การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่ายของแต่ละระบบงานตามความเหมาะสม

(๖) ระบบเครือข่ายที่มีการเชื่อมต่อไปยังเครือข่ายภายนอกต้องเชื่อมต่อผ่านอุปกรณ์ IPS และ Firewall

๗. การควบคุมการจัดเส้นทางบนเครือข่าย

(๑) ผู้ดูแลระบบต้องทำการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

(๒) ผู้ดูแลระบบต้องทำการกำหนดหมายเลขเครือข่ายให้เหมาะสมตามความจำเป็นในการใช้งาน

(๓) ผู้ดูแลระบบต้องทำการจำกัดสิทธิในการใช้งานในแต่ละกลุ่มเครือข่ายย่อยให้มีการใช้งานเฉพาะกลุ่มของตนเองเพื่อป้องกันการละเมิดและถูกละเมิด

ส่วนที่ ๖
การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

แนวปฏิบัติ

๑. การเข้าใช้งานที่มั่นคงปลอดภัย

(๑) ผู้ใช้งานต้องทำการกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบ

(๒) ผู้ใช้งานต้องทำการตั้งค่าให้ระบบปฏิบัติการทำการป้องกันด้วยรหัสผ่านทุกครั้งที่เปิดใช้งาน

(๓) ผู้ใช้งานต้องทำการตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเมื่อไม่มีการใช้งานให้ทำการล็อคด้วยรหัสผ่าน

(๔) ผู้ใช้งานต้องทำการลงบันทึกออกทุกครั้งเมื่อไม่ได้ใช้งานเป็นเวลานาน

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) การเข้าใช้งานระบบปฏิบัติการต้องมีพิสูจน์ตัวตนด้วยบัญชีผู้ใช้ทุกครั้ง

(๓) ผู้ใช้งานต้องทำการลงชื่อออกทันทีที่เลิกใช้งานหรือว่างเว้นจากการใช้งานเป็นเวลานาน

(๔) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งาน หากพบว่าการยืนยันตัวตนผิดพลาดไม่สามารถเข้าใช้งานได้ต้องทำการแจ้งผู้ดูแลระบบให้ทำการแก้ไขทันที

(๕) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ต้องรับผิดชอบผลจากการใช้งานบัญชีผู้ใช้ของตนเองทุกกรณี

(๖) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ให้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามมิให้มีการจำหน่ายจ่ายแจกให้ผู้อื่น หรือมีการใช้งานร่วมกัน

๓. การบริหารจัดการรหัสผ่าน

(๑) รหัสผ่านที่ใช้งานในระบบต้องมีความยาวไม่น้อยกว่า ๖ ตัวอักษร

(๒) ระบบต้องทำการระงับสิทธิในการเข้าสู่ระบบหากมีการป้อนรหัสผ่านผิดเกิน ๓ ครั้ง

(๓) ระบบจะต้องไม่แสดงข้อมูลรหัสผ่านระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านโดยให้แสดงเป็นสัญลักษณ์แทน

(๔) รหัสผ่านของผู้ใช้ต้องมีการเปลี่ยนรหัสผ่านทุก ๆ ๖ เดือน

๔. การใช้งานโปรแกรมอรรถประโยชน์

(๑) ผู้ใช้ต้องไม่ทำการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อกรมทางหลวง

(๒) ผู้ใช้ต้องไม่ติดตั้งใช้งานโปรแกรมอรรถประโยชน์ที่เป็นการตรวจสอบ หรือหลีกเลี่ยงระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่าย

(๓) ผู้ใช้ต้องไม่ทำการติดตั้งโปรแกรมอรรถประโยชน์โดยไม่จำเป็น และถอนการติดตั้งโปรแกรมอรรถประโยชน์ทันทีหากไม่มีความจำเป็นในการใช้งาน เพื่อลดช่องโหว่ของระบบคอมพิวเตอร์

(๔) ผู้ใช้ต้องทำการติดตั้งโปรแกรมป้องกันผู้ไม่ประสงค์ดีที่ศูนย์เทคโนโลยีสารสนเทศจัดหาให้

๕. การว่างเว้นจากการใช้งานระบบสารสนเทศ

(๑) ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาในการใช้งาน หากไม่มีการใช้งานเป็นเวลาระยะหนึ่งที่ได้กำหนดไว้

(๒) ผู้ใช้ต้องทำการล้างหน้าจอหรือทำการล็อคหน้าจอเมื่อมีการว่างเว้นจากการใช้งานและต้องลุกหรือเคลื่อนย้ายจากเครื่องคอมพิวเตอร์ที่กำลังทำงานอยู่

(๓) ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อที่สั้นลงสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เพื่อเพิ่มความปลอดภัยให้กับระบบงานจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

(๑) ผู้ดูแลระบบต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบงานภายในให้ใช้งานได้เฉพาะช่วงเวลาปกติ เมื่อเลยกำหนดเวลาให้ตัดการเชื่อมต่อทันที ในกรณีที่ต้องมีการเชื่อมต่อในช่วงเวลาอื่น ให้ทำการร้องขอการใช้งานต่อศูนย์เทคโนโลยีสารสนเทศเพื่อพิจารณาเป็นครั้ง ๆ ไป

(๒) การเชื่อมต่อที่ให้บริการแก่ผู้ใช้งานให้ใช้งานได้ตลอดเวลาแต่จำกัดการเชื่อมต่อให้สามารถใช้งานได้นานที่สุดไม่เกิน ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

(๓) การเชื่อมต่อจากภายนอกผ่าน SSL VPN ให้จำกัดเวลาการเชื่อมต่อที่ ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง หากต้องการใช้งานต่อต้องทำการพิสูจน์ตัวตนเพื่อเข้าใช้งานอีกครั้ง

ส่วนที่ ๗

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของกรมทางหลวง และป้องกันการบุกรุกจากโปรแกรมไม่พึงประสงค์และการบุกรุกจากผู้ไม่ประสงค์ดีที่จะสร้างความเสียหายให้แก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

(๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งให้สิทธิตามอำนาจหน้าที่ที่ควรได้รับ

(๒) ผู้ดูแลระบบต้องจัดให้มีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อให้กับระบบงาน และหากมีการว่างเว้นจากการใช้งานเกินระยะเวลา ๑๕ นาที ให้ทำการยุติการใช้งานทันที

(๔) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๔.๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๔.๒) กำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล และห้ามมิให้ใช้รายชื่อผู้ใช้และรหัสผ่านชุดเดียวกันในชั้นความลับของข้อมูล

(๔.๓) ให้มีการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดตามระดับความสำคัญของข้อมูล

(๔.๔) กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัส SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ

(๔.๕) การนำคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงานต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

(๔.๖) การเข้าถึงเครือข่ายของผู้ปฏิบัติงานชั่วคราวให้ทำการลงทะเบียนและได้รับสิทธิเป็นการชั่วคราวตามระยะเวลาการปฏิบัติงาน หากพ้นจากช่วงเวลาดังกล่าวให้ระงับสิทธิในการเข้าถึง และต้องทำการลงทะเบียนเพื่อรับสิทธิในการเข้าถึงใหม่ทุกครั้ง

๒. การจัดการระบบซึ่งไวต่อการรบกวน

(๑) ผู้ดูแลระบบต้องจัดให้ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมทางหลวง ได้รับการติดตั้งแยกออกจากระบบงานอื่น มีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ได้แก่ ระบบปรับอากาศ ระบบสำรองไฟ

(๒) ผู้ดูแลระบบต้องจัดให้ระบบซึ่งไวต่อการรบกวน มีช่องทางการเชื่อมต่อของตนเองโดยเฉพาะ หรือหากมีการใช้ช่องสัญญาณร่วมกันต้องมีการประกันคุณภาพของสัญญาณ (QoS) สำหรับระบบนั้นๆ

(๓) ผู้ดูแลระบบต้องมีการจัดให้ระบบซึ่งไวต่อการรบกวน มีห้องปฏิบัติการแยกเป็นสัดส่วนและจำกัดผู้เข้าออกเฉพาะผู้มีหน้าที่รับผิดชอบเท่านั้น

๓. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๑) การใช้งานทั่วไป

(๑.๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้งานได้ใช้งาน เป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

(๑.๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๑.๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

(๑.๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๑.๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบโปรแกรมไม่ประสงค์ดีโดยโปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี

(๑.๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

(๑.๗) ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

(๑.๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

(๑.๙) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน ได้แก่ การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๑.๑๐) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑.๑๑) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง ได้แก่ ปลายปากกา กดสัมผัสหน้าจอ LCD อาจทำให้เกิดเป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๑.๑๒) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๑.๑๓) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๑.๑๔) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น ได้แก่ อาหาร น้ำกาแฟ เครื่องดื่มต่างๆ เป็นต้น

(๑.๑๕) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๑.๑๖) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

(๒) การสำรองข้อมูลและการกู้คืน

(๒.๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD, DVD, External Hard Disk เป็นต้น

(๒.๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๒.๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๔. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(๑) ผู้ใช้ที่ต้องการปฏิบัติงานจากภายนอกสำนักงานต้องทำการลงทะเบียนเพื่อขอบัญชีผู้ใช้และรหัสผ่านสำหรับเชื่อมต่อจากภายนอก

(๒) ผู้ดูแลระบบทำการสร้างบัญชีผู้ใช้งานสำหรับการเชื่อมต่อจากภายนอกสำนักงาน โดยบัญชีผู้ใช้และรหัสผ่านต้องไม่เป็นบัญชีผู้ใช้หรือรหัสผ่านชุดเดียวกับบัญชีผู้ใช้และรหัสผ่านที่ใช้ในสำนักงาน

(๓) ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำ สำหรับการปฏิบัติงานจากระยะไกลและกำหนดชั้นความลับของข้อมูลที่อนุญาตให้ใช้งาน

(๔) ผู้ดูแลระบบต้องกำหนดช่วงเวลาที่สามารถใช้งานได้คือช่วงเวลาราชการ

(๕) กำหนดให้มีช่องทางเชื่อมต่อแบบ SSL VPN ในการเชื่อมต่อจากภายนอกสำนักงาน

ส่วนที่ ๘
การใช้งานอินเทอร์เน็ต (Use of Internet)

วัตถุประสงค์

เพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย

แนวปฏิบัติ

๑. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เว้นแต่มีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๓. การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๔. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของกรมทางหลวง เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับกรมทางหลวง

๕. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมทางหลวงที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๖. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๘. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๙. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑๐. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๙

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic mail)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานจดหมายอิเล็กทรอนิกส์ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์ ผู้ใช้จะต้องเข้าใจนโยบายและแนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ที่ศูนย์เทคโนโลยีสารสนเทศได้ประกาศไว้ ไม่ละเมิดสิทธิกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพนโยบายและแนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบฯ อย่างเคร่งครัด จึงจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติ

๑. การใช้งานจดหมายอิเล็กทรอนิกส์

๑.๑ ผู้ใช้มีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ และไม่อนุญาตให้ผู้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี

๑.๒ ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๑.๓ ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์จากการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเองและจากการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้อื่น

๑.๔ ผู้ดูแลระบบไม่มีสิทธิที่จะถามหรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

๑.๕ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ในงานตามภารกิจของหน่วยงานเพื่อติดต่องานของราชการเท่านั้น และห้ามมิให้ใช้จดหมายอิเล็กทรอนิกส์อื่นเว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์กรมทางหลวงขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๑.๖ การใช้จดหมายอิเล็กทรอนิกส์ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

๑.๖.๑ ผู้ใช้งานต้องไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อประกอบธุรกิจส่วนตัวหรือของบุคคลอื่น

๑.๖.๒ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่จดหมายลูกโซ่

๑.๖.๓ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อมูลชั้นความลับของหน่วยงานและไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑.๖.๔ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารหรือในการประชุมอื่น ๆ โดยที่มิได้มีหน้าที่หรือมิได้รับมอบหมายจากประธานในที่ประชุม

๑.๖.๕ ผู้ใช้งานต้องไม่ทำการปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้น ๆ ส่งมาจากบุคคลอื่น

๑.๖.๖ ผู้ใช้งานต้องไม่ทำการปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ให้ทราบชื่อผู้ส่ง

๑.๖.๗ ผู้ใช้งานต้องไม่ทำการปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง

๑.๖.๘ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

๑.๖.๙ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่ดูหมิ่นเหยียดหยามหรือแบ่งแยกทางศาสนา เชื้อชาติ หรือเพศ

๑.๖.๑๐ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่มีลักษณะหยาบคายหรือลามกอนาจาร

๑.๖.๑๑ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่โปรแกรมหรืองานหรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองานในลักษณะที่ละเมิดลิขสิทธิ์

๑.๖.๑๒ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

๑.๖.๑๓ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์โฆษณาสินค้าผลิตภัณฑ์หรือส่งข้อความลักษณะของสแปมเมล (Spam Mail) ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

๑.๖.๑๔ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ซึ่งส่งผลกระทบให้ระบบจดหมายอิเล็กทรอนิกส์หรือเครือข่ายลดทอนประสิทธิภาพลง

๑.๖.๑๕ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์กระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

๑.๖.๑๖ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑.๖.๑๗ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดและตรวจสอบไฟล์แนบโดยใช้โปรแกรมป้องกัน

๑.๖.๑๘ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีเนื้อหาขัดต่อจริยธรรม ปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย ข้อมูลอันเป็นเท็จที่กระทบความมั่นคงของประเทศหรือกระทบต่อการดำเนินงานของหน่วยงาน

๑.๖.๑๙ ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ที่เป็นความเห็นส่วนบุคคลโดยอ้างว่าเป็นความเห็นของหน่วยงานหรือก่อให้เกิดความเสียหายต่อหน่วยงาน

๑.๖.๒๐ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมหรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงานทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางระบบจดหมายอิเล็กทรอนิกส์

๒. การระงับบัญชีจดหมายอิเล็กทรอนิกส์

กรมทางหลวงขอสงวนสิทธิซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิการใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหาความมั่นคงปลอดภัยหรือเสถียรภาพของระบบเครือข่าย หรือระบบจดหมายอิเล็กทรอนิกส์ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์มีแนวทางปฏิบัติ ดังนี้

๒.๑ เมื่อผู้ใช้พ้นสภาพการอยู่ในสังกัดของกรมทางหลวง ศูนย์เทคโนโลยีสารสนเทศสามารถระงับบัญชีผู้ใช้ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย

๒.๒ บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลงหรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้งานโดยผู้ใช้หรือการลักลอบเข้าใช้งานโดยผู้อื่น ทั้งนี้ศูนย์เทคโนโลยีสารสนเทศมีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

๒.๓ กรณีผู้ใช้ไม่ได้เข้าสู่บัญชีจดหมายอิเล็กทรอนิกส์ภายในระยะเวลา ๖ เดือน ผู้ดูแลระบบขอสงวนสิทธิในการระงับสิทธิการใช้งานจดหมายอิเล็กทรอนิกส์บัญชีนั้น

๓. การใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ใช้งาน (User)

๓.๑ ผู้ใช้งานที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลคำขอใช้งานจดหมายอิเล็กทรอนิกส์ผ่านช่องทางออนไลน์ พร้อมให้หัวหน้าหน่วยงานระดับผู้อำนวยการหรือเทียบเท่าลงนามด้วยวิธีทางอิเล็กทรอนิกส์เพื่อรับรองข้อมูลของผู้ขอใช้งาน และยื่นคำขอมาที่ศูนย์เทคโนโลยีสารสนเทศทาง E-mail เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password) ต่อไป

๓.๒ เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันทีหลังจากการเข้าสู่ระบบเป็นครั้งแรก

๓.๓ ควรกำหนดรหัสผ่านที่ยากต่อการคาดเดาให้มีตัวอักษรไม่น้อยกว่า ๘ ตัวอักษรโดยมีการผสมกันระหว่างตัวอักษรภาษาอังกฤษที่เป็นตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก และตัวเลขเข้าด้วยกัน

๓.๔ ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๓.๕ ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุก ๆ ๖ เดือนหรือตามความเหมาะสม

๓.๖ หลังจากการใช้งานควรลงชื่อออกจากระบบทุกครั้ง (Log out) เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

๓.๗ เนื้อที่ในการเก็บข้อมูลของจดหมายอิเล็กทรอนิกส์มีขนาด ๑๐ GB และแนบไฟล์ในการส่งแต่ละครั้งได้ไม่เกิน ๒๕ MB

๓.๘ ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบจดหมายอิเล็กทรอนิกส์ให้เหลือจำนวนน้อยที่สุด

๓.๙ ไม่ควรเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในกล่องขาเข้า ควรสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังไว้ที่เครื่องคอมพิวเตอร์ของตน เนื่องจากอาจมีความเสียหายที่เกิดจากระบบจดหมายอิเล็กทรอนิกส์ได้

๓.๑๐ ผู้ใช้งานสามารถเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์กรมทางหลวงได้ที่ http://mail.doh.go.th หรือเว็บไซต์กรมทางหลวง (http://www.doh.go.th-> Webmail)

๓.๑๑ ผู้ใช้งานสามารถดาวน์โหลดคู่มือการใช้งานระบบฯ ได้ที่เว็บไซต์ภายในกรมทางหลวง (http://intranet.doh.go.th)

๓.๑๒ กรณีพบปัญหาหรือมีข้อสงสัยเกี่ยวกับการใช้งานสามารถสอบถามได้ที่เบอร์โทรศัพท์: ๐-๒๓๕๔-๖๖๖๘-๗๖ ต่อ ๒๖๗๓๓, ๒๖๗๓๕

๔. การใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ดูแลระบบ (System Administrator)

๔.๑ กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้และหน้าที่ความรับผิดชอบของผู้ใช้งาน

๔.๒ มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งานปีละ ๒ ครั้ง (ทุกเดือนเมษายนและตุลาคม) หรือเมื่อมีการเปลี่ยนแปลง เช่น เกษียณอายุราชการ การลาออก โอน ย้าย หรือพ้นสภาพการอยู่ในสังกัดของกรมทางหลวง เป็นต้น

๔.๓ มีการควบคุมการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ตามนโยบายการใช้งานจดหมายอิเล็กทรอนิกส์กรมทางหลวงที่ได้กำหนดไว้อย่างเคร่งครัด

ส่วนที่ ๑๐

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการการป้องกันบุคคลภายนอกจากการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต กับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูล และสารสนเทศที่เป็นทรัพย์สินของกรมทางหลวง ซึ่งอาจก่อให้เกิดความเสียหายและทำการก่อกวน หรือแทรกแซงต่อทรัพย์สินสารสนเทศของกรมทางหลวง ส่งผลกระทบต่อการปฏิบัติภารกิจด้านความมั่นคงปลอดภัยสารสนเทศ ทำให้ไม่สามารถปฏิบัติภารกิจได้อย่างต่อเนื่องและมีประสิทธิภาพ

แนวปฏิบัติ

๑. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

๑.๑ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงาน พื้นที่ควบคุมเฉพาะให้ชัดเจน พื้นที่จัดเก็บอุปกรณ์ต่าง ๆ พื้นที่เก็บเอกสาร สื่อบันทึกข้อมูล เป็นต้น และจัดทำแผนผังแสดงตำแหน่งพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

๑.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิและลำดับชั้นในการเข้าถึงพื้นที่ใช้งานข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสาร

๑.๓ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ของศูนย์เทคโนโลยีสารสนเทศทั้งหมด และกำหนดพื้นที่ที่มีความเสี่ยง ห้ามบุคคลภายนอกหรือผู้มีส่วนเกี่ยวข้องเข้าถึงได้

๑.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑.๕ จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานและมีความพร้อมในการใช้งาน ดังนี้

๑) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

๒) ติดตั้งระบบน้ำ และเครื่องดับเพลิง

๓) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

๔) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๕) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

๒. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงให้ติดตั้งระบบป้องกันที่ปลอดภัย

๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒.๔ ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๒.๕ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติกแทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๓. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๓.๑ วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

๓.๒ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๓.๓ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๓.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่เข้ามาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษผู้ดูแลระบบจะต้องอยู่ในพื้นที่ทุกครั้ง

๓.๕ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างให้บริการจากภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๔.๑ ต้องขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือนำไปซ่อมบำรุงภายนอก

๔.๒ ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนดและตรวจสอบอยู่ในสภาพดี

๔.๓ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน และบันทึกส่งคืนเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

๕. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off Premises)

๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๕.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

๕.๓ เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๖. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

๖.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

๖.๒ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

หมวด ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อให้กรมทางหลวงมีแนวทางปฏิบัติหรือมาตรการในการจัดทำระบบสำรองข้อมูล (Backup System) และแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อป้องกันข้อมูลสูญหายเพิ่มความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศของกรมทางหลวง ในกรณีฉุกเฉินหรือสถานการณ์ไม่ปกติหรือมีภัยพิบัติเกิดขึ้น และสามารถกู้คืนระบบสารสนเทศภายในระยะเวลาที่เหมาะสม

แนวปฏิบัติ

๑. การสำรองข้อมูล

(๑) ศูนย์เทคโนโลยีสารสนเทศต้องทำการคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(๒) จัดทำบัญชีระบบสารสนเทศทั้งหมดที่มีความสำคัญของกรมทางหลวง พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง

(๓) มีการวางแผนสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ กำหนดชนิดการสำรองข้อมูล สื่อบันทึกที่ใช้ในการสำรองข้อมูลตามความเหมาะสม ช่วงเวลาในการสำรองข้อมูลโดยพิจารณาจากความสำคัญของข้อมูล ความถี่ในการเปลี่ยนแปลงข้อมูล

(๔) ผู้ดูแลระบบต้องทำการบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่สำรอง สื่อบันทึกที่ได้สำรองข้อมูล โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย

(๕) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็น การสำรองข้อมูลแบบเต็ม (Full Backup) การสำรองข้อมูลแบบส่วนเพิ่ม (Incremental Backup) หรือการสำรองข้อมูลแบบเฉพาะส่วนต่าง (Differential Backup)

(๖) หากเกิดข้อผิดพลาดในการสำรองข้อมูล ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูล รวมทั้งวิธีการแก้ไข

(๗) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

(๘) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยเลือกใช้วิธีการที่เหมาะสมเพื่อป้องกันการรั่วไหลของข้อมูล

(๙) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติต่างๆ

(๑๐) ให้มีการมอบหมายเจ้าหน้าที่สำรองในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

(๑๑) ผู้ดูแลระบบต้องมีการสำรองข้อมูลและทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอเพื่อตรวจสอบว่ายังสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรมทางหลวง

๒. การกู้คืนระบบ

(๑) ผู้ดูแลระบบต้องทำการบันทึกการกู้คืนระบบทุกครั้งที่มีการกู้คืนระบบ แล้วรายงานให้ผู้บังคับบัญชาทราบ

(๒) ผู้ดูแลระบบต้องทำการแก้ไขหากเกิดปัญหารวมถึงรายงานผู้บังคับบัญชาถึงปัญหาและวิธีการแก้ไขในการกู้คืนระบบ

(๓) ผู้ดูแลระบบต้องทำการกู้คืนระบบโดยใช้ข้อมูลสำรองที่ทันสมัยที่สุดที่ได้สำรองไว้

(๔) ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยระบบละ ๑ ครั้งต่อปี

๓. แผนเตรียมพร้อมกรณีฉุกเฉิน

ให้ศูนย์เทคโนโลยีสารสนเทศจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และแผนเตรียมความพร้อมในกรณีที่ไม่สามารถดำเนินการได้ด้วยวิธีการทางอิเล็กทรอนิกส์ และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวปีละ ๑ ครั้ง โดยมีรายละเอียดอย่างน้อยดังนี้

(๑) ศูนย์เทคโนโลยีสารสนเทศต้องมีการกำหนดให้มีกระบวนการรับมือสำหรับกรณีฉุกเฉิน และแผนฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ได้

(๒) ศูนย์เทคโนโลยีสารสนเทศต้องมีการกำหนดชนิดของภัยพิบัติที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ

(๓) ศูนย์เทคโนโลยีสารสนเทศต้องมีการประเมินความเสี่ยงที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ทำให้ไม่สามารถเข้าใช้งานระบบสารสนเทศได้

(๔) กำหนดขั้นตอนปฏิบัติในกู้คืนระบบ และการทดสอบแผนฉุกเฉิน

(๕) กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในหน่วยงาน และผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ

(๖) สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(๗) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

(๘) กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

(๙) ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีการซักซ้อม และทบทวนแผนเตรียมพร้อมในกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๔. การกำหนดหน้าที่ความรับผิดชอบ

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer: DCIO)

(๑.๑) กำกับดูแลให้เจ้าหน้าที่ทุกหน่วยงานในกรมทางหลวงปฏิบัติตามนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศอย่างถูกต้อง เพื่อให้มั่นใจได้ว่าการใช้ระบบสารสนเทศมีความมั่นคงปลอดภัย

(๑.๒) ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศในฐานะประธานศูนย์เทคโนโลยีสารสนเทศ

(๑.๓) เป็นผู้รับผิดชอบในการทบทวนนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศ

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๒.๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

(๒.๒) มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

(๒.๓) มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

(๒.๔) ประชุมหารือกับผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่าย และคณะกรรมการอื่นที่เกี่ยวข้องในการจัดการกรณีฉุกเฉิน

(๒.๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

(๒.๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ทราบ

(๓) ผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่าย

(๓.๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๓.๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศจะมาถึงที่เกิดเหตุ

(๓.๓) ดำเนินการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

(๓.๔) ทำหน้าที่แทนผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศไม่อยู่

(๓.๕) ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง ได้แก่ ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

(๓.๖) รายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

(๓.๗) กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

(๓.๘) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

(๔) ผู้ดูแลระบบเครือข่าย

(๔.๑) หากมีเหตุการณ์ฉุกเฉินหลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้บังคับบัญชาทราบ

(๔.๒) เตรียมพร้อมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบหากเกิดเหตุการณ์ฉุกเฉิน

(๔.๓) ทำการเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหาก จากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

(๔.๔) ทำการสำรองข้อมูลตามแผนการสำรองข้อมูล

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment)

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ กรมทางหลวงจึงจัดให้มีระบบบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศขึ้น เพื่อการบริหารปัจจัยและควบคุม กิจกรรม รวมทั้งกระบวนการทำงานต่าง ๆ โดยลดโอกาส และผลกระทบที่อาจจะเกิดขึ้นในอนาคตให้อยู่ในระดับที่ยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ สามารถควบคุมความเสี่ยงด้านระบบสารสนเทศได้อย่างดี

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบด้วย

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้กรมทางหลวงได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. กำหนดแนวทางในการประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อย ดังนี้

๒.๑ ระบุความเสี่ยง สาเหตุของความเสี่ยงและผลกระทบที่เกิดขึ้นจากความเสี่ยง

๒.๒ จัดลำดับความสำคัญของความเสี่ยง

๒.๓ จัดทำมาตรการในการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน และมาตรการในภาวะฉุกเฉิน

๒.๔ ให้จัดทำรายงานการควบคุมความเสี่ยงประจำปี

๒.๕ หากมีความเสี่ยงที่เกิดขึ้นใหม่ ให้มีการจัดทำรายงานและวิเคราะห์การแก้ไขความเสี่ยงเพื่อไม่ให้เกิดขึ้นซ้ำอีก เป็นการดำเนินการต่อเนื่องว่าแผนบริหารความเสี่ยงมีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไปหรือไม่ รวมถึงทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอนและพัฒนาระบบให้ดียิ่งขึ้น

๒.๖ ให้มีการทบทวนประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๓. มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

๓.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

๓.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

๓.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๓.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

๓.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวด ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

แนวปฏิบัติ

๑. ระดับนโยบาย ประกอบด้วย

๑.๑ ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) กรมทางหลวงเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer : DCIO) กรมทางหลวงเป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแลและควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศของกรมทางหลวง เป็นผู้รับผิดชอบ ดังนี้

๑.๓.๑ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูล และเทคโนโลยีสารสนเทศ

๑.๓.๒ ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๑.๓.๓ วางแผน จัดทำ ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

๒. ระดับปฏิบัติงาน

ระดับปฏิบัติงาน ประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งานเป็นผู้รับผิดชอบตามภารกิจ ดังนี้

๒.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ ดังนี้

๒.๑.๑ ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๑.๓ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ระบบเครือข่ายระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๑.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๖ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทางหลวง

๒.๒ ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด