

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์และขอบเขต

เพื่อให้กรมทางหลวงสามารถใช้ระบบเทคโนโลยีสารสนเทศประกอบการปฏิบัติงาน การดำเนินการใดๆด้วยวิธีทางอิเล็กทรอนิกส์ การให้บริการหน่วยงาน และประชาชนได้อย่างเหมาะสมมีประสิทธิภาพ ตลอดจนเป็นการสร้างความเชื่อมั่นของหน่วยงานและประชาชนต่อการดำเนินการของกรมทางหลวง จึงได้จัดทำ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวงขึ้น โดยแต่ละส่วนจะประกอบด้วย วัตถุประสงค์ รายละเอียดและขั้นตอนของแนวทางในการปฏิบัติ

๒. องค์ประกอบของแนวปฏิบัติ

ส่วนที่ ๑ ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ส่วนที่ ๔ การจัดการการเข้าถึงระบบเครือข่าย (Network Access Control)

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ส่วนที่ ๗ การจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมในกรณีฉุกเฉิน

ส่วนที่ ๘ การตรวจสอบและประเมินความเสี่ยง (Risk Assessment)

ส่วนที่ ๑

ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

กรมทางหลวงมีการกำหนด ประเภทของข้อมูลดังนี้

๑.ประเภทข้อมูล

แบ่งตามลักษณะการใช้งานได้ดังนี้

- (๑) ข้อมูลด้านการบริหาร หมายถึง เอกสารหรือข้อมูลต่างๆรวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่างๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่ใช้ในการบริหารหน่วยงาน มีความสำคัญและให้ล่วงรู้ได้เฉพาะบุคคลหรือกลุ่มบุคคลที่มีหน้าที่โดยตรงต่อข้อมูลนั้นๆ ได้แก่ ข้อมูลสารสนเทศด้านการบริหาร ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลงบประมาณการเงินและบัญชี
- (๒) ข้อมูลภายใน (Internal Data) หมายถึง เอกสารหรือข้อมูลต่างๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่างๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่ใช้ภายในหน่วยงาน ได้แก่
 - (๒.๑) ข้อมูลสารสนเทศกระบวนการหลัก ประกอบด้วย ข้อมูลงานก่อสร้างทางหลวง ข้อมูลงานสะพาน ข้อมูลบริหารบำรุงทาง ข้อมูลงานอำนวยความสะดวก
 - (๒.๒) ข้อมูลสารสนเทศกระบวนการสนับสนุน ประกอบด้วย ข้อมูลงานเครื่องกลและสื่อสาร ข้อมูลงานจัดกรรมสิทธิ์ที่ดิน ข้อมูลบุคลากร
 - (๒.๓) ข้อมูลภูมิศาสตร์สารสนเทศงานทาง ประกอบด้วย ข้อมูลพิกัดทางหลวง ข้อมูลพิกัดสะพาน
- (๓) ข้อมูลส่วนบุคคล (Personal Data) หมายถึงเอกสารหรือข้อมูลต่างๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่างๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก เช่น รหัสสมาชิก หมายเลขบัตรประชาชน ชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลอื่นๆที่สามารถบ่งชี้ตัวบุคคลได้ ได้แก่ ข้อมูลบุคลากร ข้อมูลบุคคลที่มาติดต่อกรมทางหลวง
- (๔) ข้อมูลที่เปิดเผยได้ หมายถึงเอกสารหรือข้อมูลต่างๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่างๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่สามารถเผยแพร่ให้ประชาชนหรือบุคคลทั่วไปรับทราบ ได้แก่ ข้อมูลสถิติอุบัติเหตุบนทางหลวง ข้อมูลระยะทางของทางหลวง ข้อมูลบริการประชาชน

๒.ระดับความสำคัญของข้อมูล

(๑) ความสำคัญระดับเคร่งครัด มีความสำคัญและให้ล่วงรู้ได้เฉพาะบุคคลหรือกลุ่มบุคคลที่มีหน้าที่โดยตรงต่อข้อมูลนั้นๆ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนอาจจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ ได้แก่

(สำคัญมาก) ได้แก่ ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย ข้อมูลคดีความ

(สำคัญปานกลาง) ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร ข้อมูลทะเบียนผู้รับเหมาก่อสร้างทาง

(๒) ความสำคัญระดับกลาง ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน ต่อบุคคลภายนอกอาจก่อให้เกิดความเสียหายแก่ประโยชน์ของหน่วยงาน หรือบุคลากรของหน่วยงาน ได้แก่ ข้อมูลสำหรับปฏิบัติงานภารกิจของหน่วยงาน

(๓) ความสำคัญระดับพื้นฐาน ได้แก่ ข้อมูลเผยแพร่ ข้อมูลเพื่อบริการประชาชน

๓. ชั้นความลับของข้อมูล

(๑) ลับที่สุด หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

(๒) ลับมาก หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

(๓) ลับ หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

(๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ได้

๔ การกำหนดให้ข้อมูลอยู่ในชั้นความลับใด ให้พิจารณาถึงองค์ประกอบต่อไปนี้ เช่น

(๑) ความสำคัญของเนื้อหา

(๒) แหล่งที่มาของข้อมูล

(๓) วิธีการนำไปใช้ประโยชน์

(๔) จำนวนบุคลากรที่ควรรับทราบ

(๕) ผลกระทบหากมีการเปิดเผย

(๖) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ

๕ ระดับชั้นการเข้าถึง

- (๑) ระดับชั้นสำหรับผู้บริหาร
- (๒) ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- (๓) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๖ เวลาที่เข้าถึงได้

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๗ ช่องทางการเข้าถึง

กำหนดเกณฑ์ในการอนุญาตให้ถึงการใช้สารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจดังนี้

- (๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องได้แก่ อ่านอย่างเดียว สร้างข้อมูล ป้อนข้อมูล แก้ไขข้อมูล อนุมัติ หรือ ไม่มีสิทธิ เป็นต้น
- (๒) กำหนดเกณฑ์การระบุสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่กำหนดไว้
- (๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- (๔) กำหนดช่วงเวลาที่สามารถเข้าถึงได้
- (๕) กำหนดจำนวนช่องทางที่สามารถเข้าถึง ได้แก่ ผ่านระบบอินเทอร์เน็ต ผ่านระบบอินทราเน็ต ผ่านระบบงานโดยตรง ผ่านเครื่องคอมพิวเตอร์ส่วนบุคคล ผ่านโทรศัพท์มือถือ ผ่านเจ้าหน้าที่หน่วยงานเป็นผู้ดำเนินการให้ เป็นต้น

ส่วนที่ ๒

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑. มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training)

(๑) เสริมสร้างความเข้าใจ ในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้งาน

(๒) จัดหลักสูตรฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒. การลงทะเบียนผู้ใช้งาน (User registration) มีขั้นตอนปฏิบัติในกรอบกลุ่มในเรื่องต่อไปนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ผู้ดูแลระบบตรวจสอบบัญชีผู้ใช้งาน ให้ไม่ซ้ำซ้อนกับบัญชีผู้ใช้งานที่มีอยู่เดิม

(๓) ผู้ดูแลระบบตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๔) ผู้ดูแลระบบจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งผู้ใช้งานต้องลงนามรับทราบด้วย

(๕) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบเทคโนโลยีสารสนเทศ

(๖) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๗) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๘) ผู้ดูแลระบบต้องทบทวนสิทธิ์ของบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

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

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เหมาะสมตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

(๒) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานให้เหมาะสมกับระบบเทคโนโลยีสารสนเทศ

- (๓) ผู้ดูแลระบบมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน
- (๔) ผู้ดูแลระบบต้องทบทวนสิทธิ์สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๔. มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

- (๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้ง หรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
- (๒) ผู้ดูแลระบบต้องตั้งรหัสผ่านชั่วคราวที่ยากต่อการเดา และต้องมีความแตกต่างกัน
- (๓) ผู้ดูแลระบบต้องให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา
- (๓) การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน
- (๕) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๕. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน

- (๑) ผู้ดูแลระบบต้องทบทวนสิทธิ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น
- (๒) ผู้ดูแลระบบทบทวนสิทธิ์ผู้ที่มีสิทธิ์ในระดับสูง ได้แก่ สิทธิ์ระดับผู้ดูแลระบบ ด้วยความถี่กว่าสิทธิ์ระดับผู้ใช้งาน

ส่วนที่ ๓

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อย ดังนี้

๑. มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

- (๑) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
- (๒) ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา
- (๓) ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
- (๔) ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- (๕) ผู้ใช้งานต้องไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน
- (๖) ผู้ใช้งานต้องไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้เพิ่มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- (๗) ผู้ใช้งานต้องเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- (๘) ผู้ใช้งานต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในคอมพิวเตอร์
- (๙) ผู้ใช้งานต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)
- (๑๐) ผู้ใช้งานต้องไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
- (๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้วทำการเปลี่ยนรหัสผ่านโดยทันที
- (๑๒) ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
- (๑๓) ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน
- (๑๔) ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดิม

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

- (๑) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน

(๒) ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๓) ผู้ใช้งานต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

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

- (๑) ผู้ใช้งานทุกคนต้องออกจากระบบที่ใช้งานทันที เมื่อจำเป็นต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแล
- (๒) ผู้ใช้งานมีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
- (๓) ผู้ใช้งานทุกคนต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญของกรม ไว้ในที่ปลอดภัย เช่น เก็บไว้ในตู้เอกสารที่มีระบบล็อก และมีกุญแจเปิดปิด
- (๔) ผู้ใช้งานต้องลงชื่อออก(Logoff)จากเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน และทำการล็อกประตูห้อง ระหว่างพักเที่ยงหรือเมื่อผู้ใช้งานกลับบ้านหลังเลิกงาน
- (๕) ผู้ใช้งานต้องทำการล็อกประตูห้อง ที่มีเครื่องโทรสารระหว่างพักเที่ยง หรือเมื่อผู้ใช้งานกลับบ้านหลังเลิกงาน
- (๖) ผู้ใช้งานต้องทำการป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- (๗) ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต
- (๘) ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- (๙) เอกสารสำคัญ และสื่อบันทึกข้อมูลแบบใช้ครั้งเดียวที่ผ่านการใช้งานแล้วต้องถูกทำลายโดยการแยกทำลายโดยใช้เครื่องทำลายเอกสาร
- (๑๐) เอกสารบนสื่อบันทึกข้อมูลแบบใช้ซ้ำต้องทำการลบข้อมูลแบบถาวรป้องกันการกู้คืน โดยใช้มาตรฐาน DoD 5220-22.M หรือมาตรฐานการลบทำลายข้อมูลที่สูงกว่า

๔. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ ดังนี้

ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

ส่วนที่ ๔

การจัดการการเข้าถึงระบบเครือข่าย (Network Access Control)

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรม

๑. แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

- (๑) ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น
- (๒) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อบุคคลอื่น
- (๓) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- (๔) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการพาณิชย์
- (๕) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่กรม ไม่ว่าจะเป็นข้อมูลของกรม หรือบุคคลภายนอกก็ตาม
- (๖) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของกรมหรือ ของบุคคลอื่น
- (๗) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิในข้อมูลดังกล่าว
- (๘) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายต่อกรม เช่นการรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังผู้ใช้งานหรือบุคคลอื่น เป็นต้น
- (๙) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อขัดขวางการใช้งานระบบเทคโนโลยีสารสนเทศของกรม หรือของผู้ใช้งานอื่นของกรม หรือเพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมไม่สามารถใช้งานได้ตามปกติ

- (๑๐) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวกับการดำเนินงานของกรมไปยังที่อยู่เว็บไซต์ใดๆในลักษณะที่จะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- (๑๑) ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของกรม หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อกรม
- (๑๒) ผู้ใช้งานต้องทำการเข้าถึงระบบเครือข่ายตามสิทธิและหน้าที่ของตนเองเท่านั้นห้ามมิให้ทำการใช้งานระบบเครือข่ายโดยใช้สิทธิของผู้อื่น

๒. แนวปฏิบัติสำหรับการเชื่อมต่อจากภายนอกองค์กร

- (๑) การเข้าสู่เครือข่ายของกรมผ่านทางเครือข่ายภายนอก หรือระบบอินเทอร์เน็ต ต้องทำโดยผ่านทางช่องทางการเชื่อมต่อแบบปลอดภัย
- (๒) การเข้าสู่เครือข่ายของกรมผ่านทางเครือข่ายภายนอกต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง และต้องมีการบันทึกข้อมูลจราจรที่ได้ทำการใช้งานไว้ไม่ต่ำกว่า ๙๐ วัน

๓. แนวปฏิบัติสำหรับการระบุอุปกรณ์บนเครือข่าย

- (๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของกรมต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อนจึงจะสามารถดำเนินการได้
- (๒) ผู้ดูแลระบบต้องทำการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดอุปกรณ์ที่นำมาเชื่อมต่อ IP Address และสถานที่ตั้ง
- (๓) ผู้ดูแลระบบมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิในการเชื่อมต่อตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนด และระงับสัญญาณการเชื่อมต่อเมื่อสิ้นสุดการอนุญาต
- (๔) ให้มีการจัดทำผังเครือข่าย (Network Diagram) ซึ่งมีการระบุรายละเอียดของอุปกรณ์บนเครือข่าย IP Address , Bandwidth , เวลาที่อนุญาตให้เชื่อมต่อ มีขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก รวมถึงมีการปรับปรุงผังให้เป็นปัจจุบัน

๔. แนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

- (๑) มีการติดตั้งอุปกรณ์ IPS เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่าย

- (๒) ผู้ดูแลระบบต้องทำการป้องกันอุปกรณ์เครือข่ายจากการเข้าถึงเพื่อเปลี่ยนแปลงค่าโดยไม่ได้รับอนุญาตโดย ต้องทำการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึง โดยทำการปิดพอร์ตที่ไม่มีความจำเป็นในการใช้งาน และกำหนดพอร์ตเฉพาะในการเข้าถึงอุปกรณ์
- (๓) ผู้ดูแลระบบต้องทำการกำหนดรหัสผ่านในการเข้าถึงเพื่อเปลี่ยนแปลงค่าของอุปกรณ์ให้ยากแก่การคาดเดา และมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

๕. แนวปฏิบัติในการแบ่งแยกเครือข่าย

- (๑) ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่ายแต่ละสำนักออกจากกัน เพื่อป้องกันการละเมิดสิทธิและทรัพยากรเครือข่ายของแต่ละหน่วยงาน
- (๒) ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายออกเป็นโซนเพื่อความมั่นคงปลอดภัยของระบบงานจากการบุกรุกทางเครือข่าย

๖. แนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย

- (๑) ผู้ใช้งานมีสิทธิในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิที่ได้รับตามอำนาจหน้าที่ของตนเอง
- (๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการใช้งานเครือข่ายทุกครั้ง
- (๓) ผู้ใช้งานต้องไม่นำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต
- (๔) ผู้ดูแลระบบต้องทำการตรวจสอบการเชื่อมต่อบนเครือข่ายหากพบการเชื่อมต่อจากอุปกรณ์นอกเหนือจากที่ได้รับอนุญาตต้องทำการระงับการเชื่อมต่อโดยทันที
- (๕) ผู้ดูแลระบบต้องทำการจำกัดสิทธิในการใช้งานระบบเครือข่ายร่วมกัน เช่นการแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่ายของแต่ละระบบงานตามความเหมาะสม
- (๖) ระบบเครือข่ายที่มีการเชื่อมต่อไปยังเครือข่ายภายนอกต้องเชื่อมต่อผ่านอุปกรณ์ IPS และ Firewall

๗. แนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย

- (๑) ผู้ดูแลระบบต้องทำการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง
- (๒) ผู้ดูแลระบบต้องทำการกำหนดหมายเลขเครือข่ายให้เหมาะสมตามความจำเป็นในการใช้งาน
- (๓) ผู้ดูแลระบบต้องทำการจำกัดสิทธิในการใช้งานในแต่ละกลุ่มเครือข่ายย่อยให้มีการใช้งานเฉพาะกลุ่มของตนเองเพื่อป้องกันการละเมิดและถูกละเมิด

ส่วนที่ ๕

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจน ปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้อง และ มีความพร้อมใช้งานอยู่เสมอ

๑. แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

- (๑) ผู้ใช้งานต้องทำการกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบ
- (๒) ผู้ใช้งานต้องทำการตั้งค่าให้ระบบปฏิบัติการทำการป้องกันด้วยรหัสผ่านทุกครั้งที่เปิดใช้งาน
- (๓) ผู้ใช้งานต้องทำการตั้งค่าการใช้งานโปรแกรมถอนหน้าจอเมื่อไม่มีการใช้งานให้ทำการล็อก ด้วยรหัสผ่าน
- (๔) ผู้ใช้งานต้องทำการลงบันทึกออกทุกครั้งเมื่อไม่ได้ใช้งานเป็นเวลานาน

๒. แนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน

- (๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- (๒) การเข้าใช้งานระบบปฏิบัติการต้องมีพิสูจน์ตัวตนด้วยบัญชีผู้ใช้ทุกครั้ง
- (๓) ผู้ใช้งานต้องทำการลงชื่อออกทันทีที่เลิกใช้งานหรือว่างเว้นจากการใช้งานเป็นเวลานาน
- (๔) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ เข้า ใช้งาน หากพบว่าการยืนยันตัวตนผิดพลาดไม่สามารถเข้าใช้งานได้ต้องทำการแจ้ง ผู้ดูแล ระบบให้ทำการแก้ไขทันที
- (๕) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ต้องรับผิดชอบผลจากการใช้งานบัญชีผู้ใช้ของตนเองทุกกรณี
- (๖) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ให้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามมิให้มีการ จำหน่ายแจกจ่ายให้ผู้อื่น หรือมีการใช้งานร่วมกัน

๓. แนวปฏิบัติในการบริหารจัดการรหัสผ่าน

- (๑) รหัสผ่านที่ใช้งานในระบบต้องมีความยาวไม่น้อยกว่า ๖ ตัวอักษร
- (๒) ระบบต้องทำการระงับสิทธิในการเข้าสู่ระบบหากมีการป้อนรหัสผ่านผิดเกิน ๓ ครั้ง
- (๓) ระบบจะต้องไม่แสดงข้อมูลรหัสผ่านระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่าน
- (๔) รหัสผ่านของผู้ใช้ต้องมีการเปลี่ยนรหัสผ่านทุกๆ ๖ เดือน

๔. แนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์

- (๑) ผู้ใช้ต้องไม่ทำการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมาย อันจะก่อให้เกิดความเสียหายต่อตนเอง และต่อกรม
- (๒) ผู้ใช้ต้องไม่ติดตั้งใช้งานโปรแกรมอรรถประโยชน์ที่เป็นการตรวจสอบ หรือหลีกเลียงระบบ ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และระบบเครือข่าย
- (๓) ผู้ใช้ต้องไม่ทำการติดตั้งโปรแกรมอรรถประโยชน์โดยไม่จำเป็น และถอนการติดตั้งโปรแกรม อรรถประโยชน์ทันทีหากไม่มีความจำเป็นในการใช้งาน เพื่อลดช่องโหว่ของระบบ คอมพิวเตอร์ที่ใช้
- (๔) ผู้ใช้ต้องทำการติดตั้งโปรแกรมป้องกันผู้ไม่ประสงค์ดีที่ศูนย์เทคโนโลยีสารสนเทศจัดหาให้

๕. แนวปฏิบัติเมื่อมีการว่างเว้นจากการใช้งานระบบสารสนเทศ

- (๑) ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาในการใช้งาน หากไม่มีการ ใช้งานเป็นเวลาระยะหนึ่งที่ได้กำหนดไว้
- (๒) ผู้ใช้ต้องทำการล้างหน้าจอหรือทำการล็อกหน้าจอเมื่อมีการว่างเว้นจากการใช้งานและต้องลุก หรือเคลื่อนย้ายจากเครื่องคอมพิวเตอร์ที่กำลังทำงานอยู่
- (๓) ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อที่สั้นลงสำหรับระบบเทคโนโลยีสารสนเทศ ที่ มีความเสี่ยงสูง เพื่อเพิ่มความปลอดภัยให้กับระบบงานจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. แนวปฏิบัติในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

- (๑) ผู้ดูแลระบบต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบงานภายในให้ใช้งานได้เฉพาะ ช่วงเวลาปกติ เมื่อเลยกำหนดเวลาให้ตัดการเชื่อมต่อทันที ในกรณีที่ต้องมีการเชื่อมต่อใน ช่วงเวลาอื่นให้ทำการร้องขอการใช้งานให้ศูนย์เทคโนโลยีสารสนเทศพิจารณาเป็นครั้งๆไป
- (๒) การเชื่อมต่อที่ให้บริการแก่ประชาชนให้ใช้งานได้ตลอดเวลาแต่จำกัดการเชื่อมต่อให้สามารถ ใช้งานได้นานที่สุดไม่เกิน ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง
- (๓) การเชื่อมต่อจากภายนอกผ่าน SSL VPN ให้จำกัดเวลาการเชื่อมต่อที่ ๓ ชั่วโมงต่อการ เชื่อมต่อ ๑ ครั้ง หากต้องการใช้งานต่อต้องทำการพิสูจน์ตัวตนเพื่อเข้าใช้งานอีกครั้ง

ส่วนที่ ๖

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(Application and Information Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกจากโปรแกรมไม่พึงประสงค์และการบุกรุกจากผู้ไม่ประสงค์ดีที่จะสร้างความเสียหายให้แก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก

๑. แนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

- (๑) ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งให้สิทธิตามอำนาจหน้าที่ที่ควรได้รับ
- (๒) ผู้ดูแลระบบต้องจัดให้มีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ
- (๓) ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อให้กับระบบงาน และหากมีการว่างเว้นจากการใช้งานเกินระยะเวลา ๑๕ นาทีให้ทำการยุติการใช้งานทันที
- (๔) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้
 - (๔.๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
 - (๔.๒) กำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล และห้ามมิให้ใช้รายชื่อผู้ใช้และรหัสผ่านชุดเดียวกันในชั้นความลับของข้อมูล
 - (๔.๓) ให้มีการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดตามระดับความสำคัญของข้อมูล
 - (๔.๔) กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัส SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ
 - (๔.๕) การนำคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงานต้องมีการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล
 - (๔.๖) การเข้าถึงเครือข่ายของผู้ปฏิบัติงานชั่วคราวให้ทำการลงทะเบียนและได้รับสิทธิเป็นการชั่วคราวตามระยะเวลาการปฏิบัติงาน หากพ้นจากช่วงเวลาดังกล่าวให้ระงับสิทธิในการเข้าถึง และต้องทำการลงทะเบียนเพื่อรับสิทธิในการเข้าถึงใหม่ทุกครั้ง

๒. แนวปฏิบัติการจัดการระบบซึ่งไวต่อการรบกวน

- (๑) ผู้ดูแลระบบต้องจัดให้ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมได้รับการติดตั้งแยกออกจากระบบงานอื่น มีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ได้แก่ ระบบปรับอากาศ ระบบสำรองไฟ
- (๒) ผู้ดูแลระบบต้องจัดให้ระบบซึ่งไวต่อการรบกวนมีช่องทางการเชื่อมต่อของตนเองโดยเฉพาะ หรือ หากมีการใช้ช่องสัญญาณร่วมกันต้องมีการประกันคุณภาพของสัญญาณ (QoS) สำหรับระบบนั้นๆ
- (๓) ผู้ดูแลระบบต้องมีการจัดให้ระบบซึ่งไวต่อการรบกวนมีห้องปฏิบัติการแยกเป็นสัดส่วน และจำกัด ผู้เข้าออกเฉพาะผู้มีหน้าที่รับผิดชอบเท่านั้น

๓. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๑) การใช้งานทั่วไป

- (๑.๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน
- (๑.๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอก โปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๑.๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน
- (๑.๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น
- (๑.๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบโปรแกรมไม่ประสงค์ดีโดยโปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี
- (๑.๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่
- (๑.๗) ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- (๑.๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive
- (๑.๙) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน ได้แก่ การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

- (๑.๑๐) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- (๑.๑๑) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง ได้แก่ ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- (๑.๑๒) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (๑.๑๓) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- (๑.๑๔) ไม่ใช่หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น ได้แก่ อาหาร น้ำกาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
- (๑.๑๕) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งานไม่วางเครื่องทิ้งไว้ในที่สาธารณะ 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) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
- (๒.๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๔. แนวปฏิบัติการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

- (๑) ผู้ใช้ที่ต้องการปฏิบัติงานจากภายนอกสำนักงานต้องทำการลงทะเบียนเพื่อขอบัญชีผู้ใช้และรหัสผ่านสำหรับเชื่อมต่อจากภายนอก
- (๒) ผู้ดูแลระบบทำการสร้างบัญชีผู้ใช้งานสำหรับการเชื่อมต่อจากภายนอกสำนักงานโดยบัญชีผู้ใช้และรหัสผ่านต้องไม่เป็นบัญชีผู้ใช้หรือรหัสผ่านชุดเดียวกับบัญชีผู้ใช้และรหัสผ่านที่ใช้ในสำนักงาน
- (๓) ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งาน

- (๔) ผู้ดูแลระบบต้องกำหนดช่วงเวลาที่สามารถใช้งานได้คือช่วงเวลาราชการ
- (๕) กำหนดให้มีช่องทางเชื่อมต่อแบบ SSL VPN ในการเชื่อมต่อจากภายนอกสำนักงาน

ส่วนที่ ๗

การจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้กรมมีแนวทางปฏิบัติหรือมาตรการในการจัดทำระบบสำรองข้อมูล (Backup System) และแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อป้องกันข้อมูลสูญหายเพิ่มความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศของกรมในกรณีฉุกเฉินหรือสถานการณ์ ไม่ปกติหรือมีภัยพิบัติเกิดขึ้น และสามารถกู้คืนระบบสารสนเทศ ภายในระยะเวลาที่เหมาะสม

๑. แนวปฏิบัติในการสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

- (๑) ศูนย์เทคโนโลยีสารสนเทศต้องทำการคัดเลือกระบบที่จะสำรอง ชนิดการสำรองข้อมูล ช่วงเวลาในการสำรองข้อมูล สื่อบันทึกที่ใช้ในการสำรองข้อมูลตามความเหมาะสม
- (๒) ผู้ดูแลระบบต้องมีการสำรองข้อมูลและทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของกรม
- (๓) ผู้ดูแลระบบต้องทำการบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่สำรอง สื่อบันทึกได้สำรองข้อมูล
- (๔) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
- (๕) หากเกิดข้อผิดพลาดในการสำรองข้อมูล ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจาก การสำรองข้อมูล รวมทั้งวิธีการแก้ไข
- (๖) ให้มีการมอบหมายเจ้าหน้าที่สำรองในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้
- (๗) ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยเลือกใช้วิธีการที่เหมาะสมเพื่อป้องกันการรั่วไหลของข้อมูล
- (๘) ให้ศูนย์เทคโนโลยีสารสนเทศจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และแผนเตรียมความพร้อมในกรณีที่ไม่สามารถดำเนินการได้ด้วยวิธีการทางอิเล็กทรอนิกส์ และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวปีละ ๑ ครั้ง

๒. การกำหนดหน้าที่ความรับผิดชอบ

- (๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

(๑.๑) กำกับดูแลให้เจ้าหน้าที่ทุกหน่วยงานในกรมทางหลวงปฏิบัติตามนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศอย่างถูกต้อง เพื่อให้มั่นใจได้ว่าการใช้ระบบสารสนเทศมีความมั่นคงปลอดภัย

(๑.๒) ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศในฐานะประธานศูนย์ฯ

(๑.๓) เป็นผู้รับผิดชอบในการทบทวนนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศ

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๒.๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

(๒.๒) มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

(๒.๓) มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุดิบอันตรายเพื่อการระงับเหตุฉุกเฉิน

(๒.๔) ประชุมหารือกับผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่าย และคณะกรรมการอื่นที่เกี่ยวข้องในการจัดการกรณีฉุกเฉิน

(๒.๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯตามความเหมาะสม

(๒.๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริการเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

(๓) ผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่าย

(๓.๑) วิเคราะห์สถานการณ์ที่เกิดขึ้นแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๓.๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ จะมาถึงที่เกิดเหตุ

(๓.๓) ดำเนินการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

(๓.๔) ทำหน้าที่แทนผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศตามที่ได้รับมอบหมาย หรือขณะที่ท่านผู้อำนวยการศูนย์สารสนเทศไม่อยู่

(๓.๕) ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

(๓.๖) รายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

(๓.๗) กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

(๓.๘) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

(๔) ผู้ดูแลระบบเครือข่าย

(๔.๑) หากมีเหตุการณ์ฉุกเฉินหลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รับดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้บังคับบัญชาทราบ

(๔.๒) เตรียมพร้อมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจน อุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบหากเกิดเหตุการณ์ฉุกเฉิน

(๔.๓) ทำการเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดย แยกเก็บไว้ต่างหาก จากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการ ฮาร์ดแวร์สำรอง สำเนาคู่มือ

(๔.๔) ทำการสำรองข้อมูลตามแผนการสำรองข้อมูล

๓. การกู้คืนระบบ

(๑) ผู้ดูแลระบบต้องทำการบันทึกการกู้คืนระบบทุกครั้งที่มีการกู้คืนระบบ แล้วรายงานให้ ผู้บังคับบัญชาทราบ

(๒) ผู้ดูแลระบบต้องทำการแก้ไขหากเกิดปัญหารวมถึงรายงานผู้บังคับบัญชาถึงปัญหาและวิธีการ แก้ไขในการกู้คืนระบบ

(๓) ผู้ดูแลระบบต้องทำการกู้คืนระบบโดยใช้ข้อมูลสำรองที่ทันสมัยที่สุดที่ได้สำรองไว้

(๔) ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยระบบละ ๑ ครั้งต่อปี

๔. แผนเตรียมพร้อมกรณีฉุกเฉิน

(๑) ศูนย์เทคโนโลยีสารสนเทศต้องมีการกำหนดให้มีกระบวนการรับมือสำหรับกรณีฉุกเฉิน และ แผนฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ได้

(๒) ศูนย์เทคโนโลยีสารสนเทศต้องมีการกำหนดชนิดของภัยพิบัติที่มีผลกระทบต่อระบบ เทคโนโลยีสารสนเทศ

(๓) ศูนย์เทคโนโลยีสารสนเทศต้องมีการประเมินความเสี่ยงที่มีผลกระทบต่อระบบเทคโนโลยี สารสนเทศ

(๔) ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีการซักซ้อม และทบทวนแผนเตรียมพร้อมในกรณี ฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๘

การตรวจสอบและประเมินความเสี่ยง (Risk Assessment)

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ กรมจึงจัดให้มีระบบบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศขึ้น เพื่อการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการต่างๆ โดยลดโอกาส และผลกระทบที่อาจเกิดขึ้นในอนาคตให้อยู่ในระดับที่ยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบสามารถควบคุมความเสี่ยงด้านระบบสารสนเทศได้อย่างดี กรมจึงมีแนวทางการปฏิบัติ ดังนี้

๑. ระบุความเสี่ยง สาเหตุของความเสี่ยงและผลกระทบที่เกิดขึ้นจากความเสี่ยง

๒. จัดลำดับความสำคัญของความเสี่ยง

๓. จัดทำมาตรการในการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน และมาตรการในภาวะฉุกเฉิน

๔. ให้จัดทำรายงานการควบคุมความเสี่ยงประจำปี

๕. หากมีความเสี่ยงที่เกิดขึ้นใหม่ ให้มีการจัดทำรายงานและวิเคราะห์การแก้ไขความเสี่ยง เพื่อไม่ให้เกิดขึ้นซ้ำอีก เป็นการดำเนินการต่อเนื่องว่าแผนบริหารความเสี่ยงมีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไปหรือไม่ รวมถึงทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอนและพัฒนา ระบบให้ดียิ่งขึ้น

๖. ให้มีการทบทวนประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๗. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้กรมทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ