นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ ๑
คณะกรรมการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
(IT Security Committee)

ข้อ ๑ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า "คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ" ประกอบด้วย ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศของกรมทางหลวง เป็นประธานกรรมการ ผู้อำนวยการกลุ่มบริหารจัดการระบบความปลอดภัยเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศเป็นกรรมการและเลขานุการ และผู้อำนวยการกลุ่ม/ฝ่าย ของศูนย์เทคโนโลยีสารสนเทศเป็นกรรมการ

หมวดที่ ๒
นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)

ข้อ ๒ นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมทางหลวง มีวัตถุประสงค์เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย มีประสิทธิภาพ สามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม รวมทั้งเป็นการกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้งาน

โดยนโยบายดังกล่าวนี้ มีเป้าประสงค์ให้บรรลุผลต่อการดำเนินงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ดังนี้

๒.๑ การจัดทำนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ของกรมทางหลวงโดยอ้างอิงมาตรฐานสากล ได้แก่ ISO/IEC 27001 Annex A และเป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ พร้อมกับกำหนดแนวปฏิบัติที่เป็นไปตามนโยบายนี้

๒.๒ นโยบายนี้จะต้องมีการเผยแพร่ อบรม และประชาสัมพันธ์ผ่านทางหนังสือเวียนภายในกรมทางหลวง และทางเว็บไซต์กรมทางหลวง ให้แก่เจ้าหน้าที่ทุกคนรับทราบ ยอมรับ โดยให้ถือปฏิบัติตามที่ได้กำหนดในความมั่นคงปลอดภัยตามนโยบายนี้ อย่างเคร่งครัดเพื่อให้เกิดความเข้าใจและสอดคล้องต่อการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้การปฏิบัติงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศสัมฤทธิ์ผลตามที่กำหนดไว้จะต้องมีการดำเนินการทบทวนตรวจสอบ สอบทาน และประเมินผลตามระยะเวลา ๑ ครั้งต่อปี พร้อมทั้งมีการปรับปรุงเนื้อหาของนโยบายตามระยะเวลาที่เหมาะสมเพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของกรมทางหลวง

๒.๔ เพื่อสร้างเสริมสมรรถนะ ศักยภาพ และความตื่นตัวต่อเจ้าหน้าที่ให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายอินเทอร์เน็ตในขณะปฏิบัติงาน

หมวดที่ ๓
โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศของกรมทางหลวง
(Organization of Information Security)

ข้อ ๓ โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศของกรมทางหลวง มีวัตถุประสงค์เพื่อบริหารและจัดการ ความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ ของกรมทางหลวง ผู้บริหารสูงสุดจะต้องให้การสนับสนุนอย่างเต็มที่ต่อการรักษาความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจนมีการมอบหมายงาน และสร้างการรับรู้ถึงความรับผิดชอบที่มีต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ จัดให้มีรูปแบบการประสานงานระหว่างหน่วยงานต่าง ๆ ภายในองค์กร การจัดทำผังโครงสร้างการทำงาน (Organization Chart) หรือผังการปฏิบัติงาน (Operation Chart) และการกำหนดหน้าที่ ความรับผิดชอบในส่วนที่เกี่ยวกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างชัดเจน

ข้อ ๔ ให้มีการกำหนดกระบวนการในการอนุมัติ กรณีที่มีการจัดซื้อหรือจัดหาอุปกรณ์ เครื่องมือหรือสิ่งอำนวยความสะดวกใหม่ ๆ สำหรับการนำมาใช้งาน รวมถึงจะต้องมีการจัดทำข้อตกลงในการดูแลรักษาความลับ (Confidentiality Agreement) กับทุก ๆ ส่วนที่เกี่ยวข้อง นอกจากนั้น จะต้องจัดให้มีการทบทวนด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบ นโยบาย กระบวนการและวิธีการปฏิบัติงาน สำหรับการรักษาความมั่นคงปลอดภัย ตามแผนงานที่ได้กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกับการปฏิบัติงานเกิดขึ้น

ข้อ ๕ ให้มีการกำหนดการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอกโดยระบุและจัดทำข้อกำหนดทางด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศระหว่างกรมทางหลวงกับหน่วยงานภายนอกในการใช้งาน หรือมีความเกี่ยวข้องกับสารสนเทศ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวดที่ ๔
การบริหารจัดการสินทรัพย์ (Asset Management)

ข้อ ๖ การบริหารจัดการสินทรัพย์ มีวัตถุประสงค์เพื่อป้องกันสินทรัพย์ของกรมทางหลวงจากความเสียหายที่อาจจะเกิดขึ้นได้ โดยต้องมีการจัดทำและปรับปรุงบัญชีสินทรัพย์ที่มีความสำคัญต่อกรมทางหลวงให้ถูกต้องอยู่เสมอ มีการกำหนดเจ้าของที่รับผิดชอบสารสนเทศและสินทรัพย์ที่เกี่ยวข้อง กำหนดแนวทางในการใช้งานสารสนเทศ และการรักษาความมั่นคงปลอดภัยของสินทรัพย์อย่างเหมาะสม

ข้อ ๗ ให้มีการกำหนดกระบวนการในการจัดหมวดหมู่ของสินทรัพย์สารสนเทศ (Information Classification) โดยพิจารณาจากชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และความสำคัญที่มีกับกรมทางหลวง มีการจัดทำฉลาก (Labeling) เพื่อแสดงสถานะของสารสนเทศ รวมถึงแนวทางในการจัดการตลอดช่วงอายุของสารสนเทศนั้น ๆ

หมวดที่ ๕
ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

ข้อ ๘ การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to Employment) มีวัตถุประสงค์เพื่อให้การจ้างงานและจ้างบุคลากร เข้าใจในบทบาทและหน้าที่ความรับผิดชอบของตนที่จะได้รับการว่าจ้างให้ปฏิบัติตามและเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้ระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์

ข้อ ๙ ก่อนที่จะมีการจ้างงาน จะต้องมีการกำหนดบทบาท หน้าที่ความรับผิดชอบที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ ไว้เป็นเอกสารอย่างชัดเจนโดยจะต้องสอดคล้องนโยบายความมั่นคงปลอดภัยสารสนเทศของกรมทางหลวงด้วย รวมถึงจะต้องมีการกำหนดแนวทางในการคัดเลือก (Screening) โดยจะต้องมีการตรวจสอบคุณสมบัติของผู้สมัครอย่างละเอียด และมีการกำหนดเงื่อนไขการจ้างงานที่เหมาะสม ครอบคลุมถึงเงื่อนไขในส่วนที่เกี่ยวกับความรับผิดชอบในส่วนของความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๐ ในระหว่างการจ้างงาน ต้องมีการกำหนดให้เจ้าหน้าที่และผู้รับจ้างจะต้องปฏิบัติตามนโยบายและวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยสารสนเทศ จะต้องจัดให้มีการฝึกอบรม และสร้างการรับรู้ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ นอกจากนั้นยังต้องกำหนดแนวทางในการลงโทษสำหรับพนักงานที่ไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคงปลอดภัยของกรมทางหลวง

ข้อ ๑๑ เมื่อมีการสิ้นสุดหรือการเปลี่ยนการจ้างงาน กรมทางหลวงจะต้องมีการกำหนดผู้รับผิดชอบในการจัดการเมื่อมีการสิ้นสุดหรือการเปลี่ยนการจ้างงานไว้อย่างชัดเจน ทั้งนี้เจ้าหน้าที่และผู้รับจ้างจะต้องส่งสินทรัพย์ทั้งหมดคืนให้กับกรมทางหลวง และให้ทำการยกเลิกสิทธิในการเข้าถึงสารสนเทศ หรือสถานที่ปฏิบัติงานที่จะต้องมีการควบคุมทั้งหมด เมื่อได้ยกเลิกการจ้างงานแล้ว

หมวดที่ ๖
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

ข้อ ๑๒ ให้มีการกำหนดมาตรการการป้องกันบุคคลภายนอกจากการเข้าถึงทางกายภาพ โดยไม่ได้รับอนุญาตกับสถานที่ซึ่งเป็นที่ตั้ง และพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศที่เป็นทรัพย์สินของกรมทางหลวง ซึ่งอาจก่อให้เกิดความเสียหายและทำการก่อกวนหรือแทรกแซงต่อทรัพย์สิน สารสนเทศของกรมทางหลวง รวมทั้งกำหนดให้มีการดูแลความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกต่าง ๆ รวมถึงมีการป้องกันผลกระทบจากภัยธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อการร้าย การประท้วง และอื่น ๆ สำหรับการปฏิบัติงานในพื้นที่ที่สำคัญ (Secure Areas) จะต้องมีการกำหนดแนวปฏิบัติ (Guideline) สำหรับการปฏิบัติงานในพื้นที่ดังกล่าวอย่างชัดเจน

ข้อ ๑๓ ให้มีการกำหนดการดูแลความมั่นคงปลอดภัยของเครื่องมือ และอุปกรณ์ต่าง ๆ โดยจะต้องมีการจัดวางอย่างเหมาะสม มีการบำรุงรักษา (Maintenance) อุปกรณ์อย่างต่อเนื่อง เพื่อให้มั่นใจได้ถึงความพร้อมใช้และความสมบูรณ์ต่อการนำมาใช้งาน เพื่อลดความเสี่ยงจากภัยอันตราย รวมถึงป้องกันโอกาสที่จะถูกนำไปใช้งานโดยไม่ได้รับอนุญาต และป้องกันความเสียหายที่จะเกิดขึ้นจากความล้มเหลวของอุปกรณ์สนับสนุนต่าง ๆ ได้แก่ ระบบไฟฟ้า ระบบควบคุมอุณหภูมิ ระบบปรับอากาศ ในส่วนของสายเคเบิล ทั้งสายเคเบิลไฟฟ้า และสายเคเบิลสื่อสาร จะต้องมีมาตรการการปกป้องดูแลจากความเสียหายที่อาจจะเกิดขึ้น

ข้อ ๑๔ ในกรณีที่มีการนำอุปกรณ์ออกไปใช้นอกสถานที่ (Off-Premises) ซึ่งจะมีความเสี่ยงที่แตกต่างจากการใช้งานภายในกรมทางหลวง จะต้องมีการกำหนดแนวทางในการดูแลความมั่นคงปลอดภัยในการนำไปใช้งานอย่างเหมาะสม

ข้อ ๑๕ ให้มีข้อกำหนดเมื่อมีการยกเลิกการใช้งานอุปกรณ์นั้น ๆ แล้ว จะต้องดูแลให้มั่นใจว่าข้อมูลสารสนเทศ หรือซอฟท์แวร์ต่าง ๆ ที่อยู่ในอุปกรณ์ได้รับการกำจัด หรือลบทิ้งจนหมดสิ้นก่อนที่จะทำการทิ้งหรือกำจัดอุปกรณ์นั้น ๆ

ข้อ ๑๖ ในกรณีที่มีการอนุญาตให้ใช้สื่อบันทึกข้อมูลที่ถอดแยก/เคลื่อนย้ายได้ (Management of Removable Media) ต้องกำหนดมาตรการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลที่ถอดแยกได้ และอุปกรณ์คอมพิวเตอร์พกพา ที่จะเชื่อมต่อกับบริการที่สำคัญ โดยต้องปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมดที่รองรับสื่อบันทึกข้อมูลที่ถอดแยกได้ และอุปกรณ์คอมพิวเตอร์แบบพกพาและเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีต้องการใช้งานให้แจ้งขึ้นทะเบียนสื่อบันทึกข้อมูล และขออนุญาตการเชื่อมต่อเป็นรายกรณี พร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลที่ถอดแยกได้ และอุปกรณ์คอมพิวเตอร์แบบพกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ และหากมีกรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ต้องจัดให้มีกระบวนการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล และไม่ให้สามารถกู้คืนข้อมูลได้

หมวดที่ ๗
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของกรมทางหลวง (Communications and Operations Management)

ข้อ ๑๗ ให้มีการแบ่งหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือมีการใช้งานที่ผิดวัตถุประสงค์ของสินทรัพย์ของกรมทางหลวงและขั้นตอนการปฏิบัติงานให้เป็นไปอย่างถูกต้องเหมาะสมปลอดภัยและเป็นปัจจุบัน รวมถึงการบริหารจัดการการเปลี่ยนแปลง (Change Management) ที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสี่ยงต่าง ๆ ที่ทำให้ระบบไม่สามารถให้บริการได้

ข้อ ๑๘ ให้มีการแบ่งแยกกระบวนการออกแบบ ทดสอบ และการใช้งานจริงออกจากกันอย่างชัดเจน เพื่อป้องกันความเสี่ยงจากการใช้งาน รวมถึงการเปลี่ยนแปลงระบบการปฏิบัติงานโดยไม่ได้รับอนุญาต

ข้อ ๑๙ การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management) จะต้องมีการกำหนดให้ผู้ให้บริการจากหน่วยงานภายนอกปฏิบัติตามข้อตกลงที่จัดทำขึ้นโดยเป็นไปตามมาตรการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ รวมถึงต้องมีการกำหนดการเฝ้าติดตาม ทบทวน และตรวจประเมิน (Audit) และปรับปรุงแก้ไขข้อตกลงในการให้บริการ ในกรณีที่มีการเปลี่ยนแปลงเกิดขึ้น

ข้อ ๒๐ ให้มีการวางแผนความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพที่ความเหมาะสมและเพียงพอต่อการใช้งานและจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติม โดยมีการดำเนินการทดสอบตามเกณฑ์ที่กำหนดก่อนที่จะมีการยอมรับเพื่อนำมาใช้งานต่อไป

ข้อ ๒๑ ให้มีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืน กำหนดข้อห้ามการติดตั้งโปรแกรมหรือระบบสารสนเทศที่ไม่ได้รับอนุญาต การกำหนดมาตรการ หลักเกณฑ์ การควบคุมและการตรวจสอบการรับข้อมูลหรือไฟล์ที่ส่งมาจากภายนอกเข้ามายังผู้ใช้งานภายในกรมทางหลวง การติดตั้งอุปกรณ์หรือโปรแกรม หรือระบบสารสนเทศ เพื่อป้องกันโปรแกรมที่ไม่พึงประสงค์ดีประเภทต่าง ๆ ในการปกป้อง

และรักษาสินทรัพย์ของกรมทางหลวง ให้มีความปลอดภัย รวมถึงข้อปฏิบัติ และกำหนดผู้รับผิดชอบเมื่อเกิดความเสียหายจากโปรแกรมไม่ประสงค์ดี

ข้อ ๒๒ ให้มีการกำหนดมาตรการการสำรอง (Backup) ระบบสารสนเทศ โดยกำหนดวิธีการขั้นตอนการปฏิบัติ สถานที่จัดเก็บและผู้รับผิดชอบการสำรอง (Backup) ระบบสารสนเทศแต่ละประเภทให้เหมาะสม รวมถึงการทดสอบการกู้คืนข้อมูลที่ได้สำรองไว้ เพื่อให้มั่นใจได้ว่าระบบสารสนเทศที่ได้สำรองไว้สามารถนำกลับมาใช้งานได้เมื่อต้องการ

ข้อ ๒๓ ให้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบเครือข่ายและอุปกรณ์ที่สนับสนุนการทำงาน เพื่อป้องกันการเข้าถึงข้อมูลที่ส่งผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาตรวมถึงการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) โดยต้องครอบคลุม ดังนี้

๑) บันทึกข้อมูลกิจกรรมการใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัย (Audit log)

๒) Log เกี่ยวกับการดูแลนะบบสารสนเทศโดยผู้ดูแลระบบ (System Administrator หรือ System Operator)

๓) Log เข้า - ออก พื้นที่สำคัญ

๔) Log กล้องวงจรปิด

๕) การป้องกันการเข้าถึง หรือแก้ไขเปลี่ยนแปลง ระบบสารสนเทศที่จัดเก็บ Log โดยไม่ได้รับอนุญาต

๖) ระยะเวลาการจัดเก็บ Log ตามที่กฎหมายกำหนด

ข้อ ๒๔ ให้กำหนดมาตรการการดูแลและจัดการสื่อ (Media) ที่ใช้บันทึกข้อมูลต่าง ๆ เพื่อป้องกันการเปิดเผย การแก้ไข การเปลี่ยนแปลง การลบหรือการทำลายโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงต่อการสูญหายหรือข้อมูลความลับรั่วไหล และป้องกันไม่ให้การปฏิบัติงานของกรมทางหลวงหยุดชะงัก

ข้อ ๒๕ ให้กำหนดมาตรการการแลกเปลี่ยนข้อมูลสารสนเทศและโปรแกรมที่ใช้ภายในกรมทางหลวงหรือระหว่างกรมทางหลวงกับหน่วยงานภายนอกที่ชัดเจน เพื่อลดความเสี่ยงข้อมูลสารสนเทศรั่วไหลข้อมูลถูกดักแอบดูในระหว่างที่ส่ง

ข้อ ๒๖ ให้กำหนดมาตรการความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce Services) การทำธุรกรรมทางอิเล็กทรอนิกส์ (On-line Transactions) และการเผยแพร่ข้อมูลสารสนเทศออกสู่สาธารณะ เพื่อป้องกันจากการฉ้อโกง การปฏิเสธ การเปิดเผย การเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต การส่งข้อมูลไม่ครบถ้วน ถูกต้องสมบูรณ์ ในการใช้งานและสามารถนำข้อมูลสารสนเทศมาตรวจสอบและอ้างอิงได้

ข้อ ๒๗ ให้กำหนดมาตรการการตรวจสอบและเฝ้าระวัง (Monitoring) การใช้งานสารสนเทศเพื่อป้องกันการประมวลผลหรือการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาตและให้เป็นไปตามขอบเขตของกฎหมาย และกำหนดการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงเวลาด้วย Network Time Protocol (NTP) ไปยัง Server ที่ให้บริการข้อมูลเวลาที่ถูกต้อง ได้แก่

๑) NTP Server กรมทางหลวง

๒) เวลามาตรฐานประเทศไทย โดย กรมอุทกศาสตร์ กองทัพเรือ

หมวดที่ ๘
การควบคุมการเข้าถึง (Access Control)

ข้อ ๒๘ ให้จัดทำนโยบายการควบคุมการเข้าถึงระบบ (Access Control Policy) เป็นลายลักษณ์อักษรอย่างชัดเจน และมีการทบทวนตามระยะเวลาที่กำหนดไว้ โดยพิจารณาถึงความต้องการในการดำเนินงานและทางด้านความมั่นคงปลอดภัยในการเข้าถึงสินทรัพย์สารสนเทศ

ข้อ ๒๙ ให้กำหนดวิธีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) โดยกำหนดขั้นตอนในการขึ้นทะเบียนของผู้ใช้งาน (User Registration) และการยกเลิกทะเบียนของผู้ใช้งาน หรือมีการเปลี่ยนแปลงตำแหน่งหน้าที่งาน การจำกัดและควบคุมสิทธิ์ในการใช้งานระบบ และรหัสผ่านสำหรับผู้ใช้งาน มีการทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งานอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับภาระหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

ข้อ ๓๐ ให้กำหนดหน้าที่ความรับผิดชอบและแนวปฏิบัติของผู้ใช้งาน เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ในการเลือกและการใช้งานรหัสผ่าน (Password) การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแลการป้องกันหน้าจอเครื่อง การควบคุมการจัดเก็บเอกสาร หรือสื่อที่ใช้บันทึกข้อมูลต่าง ๆ ไว้ในที่ที่ปลอดภัย

ข้อ ๓๑ ให้กำหนดนโยบายสำหรับการควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) โดยต้องระบุอย่างชัดเจนถึงบริการใดที่ผู้ใช้งานสามารถเข้าถึงได้ บริการใดไม่สามารถเข้าถึงได้ มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งานจากภายนอกกรมทางหลวง (External Connection) สามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศได้มีการพิสูจน์ตัวตนของอุปกรณ์บนระบบเครือข่ายเพื่อบ่งบอกการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว มีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและการปรับแต่งระบบ รวมถึงในการพิจารณาเพื่อแบ่งแยกเครือข่าย (Network Segregation) ตามความเหมาะสมของการใช้งาน โดยพิจารณาถึงความมั่นคงและปลอดภัย ประสิทธิภาพและความสะดวกในการใช้งานเป็นสำคัญ ทั้งนี้การควบคุมการเชื่อมต่อระบบเครือข่ายจะต้องจำกัดผู้ใช้งานในการเชื่อมต่อเครือข่ายระหว่างองค์กร ให้เป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานได้ระบุไว้ รวมถึงจะต้องมีการควบคุมการกำหนดเส้นทางบนระบบเครือข่าย เพื่อควบคุมการเชื่อมต่อทางระบบเครือข่ายและการไหลเวียนของสารสนเทศ บนระบบเครือข่ายให้เป็นตามนโยบายควบคุมการเข้าถึง

ข้อ ๓๒ ให้กำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System) โดยจะต้องมีการกำหนดขั้นตอนการปฏิบัติงานที่เหมาะสมในการเข้าถึง หรือการใช้งานระบบปฏิบัติการ โดยผู้ใช้งานทั้งหมดจะต้องมีการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (Unique Identifier and Authentication) ก่อนใช้งาน มีระบบในการจัดการรหัสผ่านอย่างมีคุณภาพ มีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (Utility Program) เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ มีการควบคุมเวลาการใช้งานระบบสารสนเทศ (Session Time-out) โดยจะต้องมีการตัดหรือหยุดการใช้งานเมื่อผู้ใช้งานไม่ได้มีการใช้ระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ มีการกำหนดเวลาในการเชื่อมต่อเครือข่าย (Connection Time) สำหรับระบบสารสนเทศที่มีความสำคัญสูง

ข้อ ๓๓ ให้กำหนดการควบคุมการเข้าถึงแอพพลิเคชั่น และสารสนเทศ (Application and Information Access Control) มีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชั่นตามนโยบายควบคุมการเข้าถึงสารสนเทศ (Access Control Policy) ที่ได้กำหนดไว้ มีการแยกการเข้าถึง

ระบบตามประเภทของผู้ใช้งาน และแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

ข้อ ๓๔ ให้กำหนดการควบคุมอุปกรณ์สื่อสารประเภทพกพาอย่างเป็นทางการ และมาตรการความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันความเสี่ยงจากการใช้งานอุปกรณ์สื่อสารประเภทพกพา และกำหนดการปฏิบัติงานจากภายนอกองค์กร โดยมีการกำหนดนโยบาย แผนงาน และขั้นตอนการปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานจากภายนอกองค์กร (Teleworking)

หมวดที่ ๙
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
(Information Systems Acquisition, Development and Maintenance)

ข้อ ๓๕ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศใหม่ หรือระบบสารสนเทศที่มีการปรับปรุงจากระบบที่มีอยู่ในปัจจุบัน ให้มีการวิเคราะห์ และมีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) อย่างน้อย ดังต่อไปนี้

๑) สิทธิ์พิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) การแบ่งแยกหน้าที่ (Separation of Duties)

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) การลบบัญชีที่ไม่ได้ใช้

๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware) และ

๘) การปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ

ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลง หรือปรับปรุงบริการที่สำคัญของกรมทางหลวง

ข้อ ๓๖ ให้มีการระบุวิธีการและขั้นตอนการประมวลผลสารสนเทศ การตรวจสอบข้อมูลนำเข้าข้อมูลที่อยู่ระหว่างการประมวลผล ความถูกต้องของข้อความ (Message) ที่แสดงในแอปพลิเคชัน รวมถึงในส่วนของข้อมูลที่ได้จากการประมวลผลของแอปพลิเคชัน โดยมีการทวนสอบถึงความถูกต้องและความเหมาะสมของข้อมูลที่นำมาใช้ในการประมวลผล เพื่อป้องกันความผิดพลาดของข้อมูล การสูญหายของข้อมูล หรือมีการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต หรือการใช้ข้อมูลผิดวัตถุประสงค์

ข้อ ๓๗ ให้มีการกำหนดมาตรการการเข้ารหัสข้อมูล (Cryptographic Controls) โดยกำหนดนโยบายในการควบคุมเข้ารหัสข้อมูล และมีการนำไปใช้ทั่วทั้งกรมทางหลวง รวมถึงจะต้องมีมาตรการในการจัดการกับกุญแจที่ใช้ในการเข้ารหัสหรือถอดรหัสข้อมูล โดยจะใช้งานร่วมกันกับเทคนิคที่ใช้ในการเข้ารหัสข้อมูล

ข้อ ๓๘ ให้มีการกำหนดมาตรการการสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of System Files) โดยกำหนดวิธีการปฏิบัติงานในการควบคุมการติดตั้งซอฟท์แวร์ลงในระบบปฏิบัติการ (Operational System) การป้องกันข้อมูลที่ใช้ในการทดสอบ การควบคุมการเข้าถึงซอร์สโค๊ด สำหรับระบบที่ให้บริการ เพื่อป้องกัน การเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา

ข้อ ๓๙ ให้มีการกำหนดมาตรการการสร้างความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและกระบวนการสนับสนุน โดยมีการกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศต้องมีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) การทดสอบ (Test) และระบบที่ให้บริการจริง (Production) ออกจากกัน จะต้องมีการทบทวน และทดสอบแอปพลิเคชัน เพื่อให้มั่นใจได้ว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน หรือต่อความมั่นคงปลอดภัยของระบบ มีการจำกัดการเปลี่ยนแปลงแก้ไขซอฟท์แวร์จากผู้ผลิต และถ้าจะต้องมีการเปลี่ยนแปลง จะต้องได้รับการควบคุมอย่างเข็มงวด รวมถึงจะต้องมีการป้องกันการรั่วไหลของสารสนเทศ ในกรณีที่การพัฒนาซอฟท์แวร์ดำเนินการโดยหน่วยงานภายนอก จะต้องมีการกำหนดขั้นตอน หรือมาตรการเพื่อควบคุมการพัฒนาระบบสารสนเทศ ให้เป็นไปตามวงจรการพัฒนาซอฟต์แวร์ (Software Development Lifecycle : SDLC) ที่เป็นมาตรฐาน และกรณีจ้างผู้รับจ้างที่เป็นผู้ให้บริการภายนอกให้ระบุเงื่อนไขของสัญญา หรือข้อตกลงระดับการให้บริการ (Service Level Agreement)

ข้อ ๔๐ ให้มีการกำหนดมาตรการในการบริหารจัดการช่องโหว่ทางด้านเทคนิค (Technical Vulnerability Management) เพื่อทำการประเมินความเสี่ยงที่จะเกิดขึ้น และกำหนดมาตรการรองรับเพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่นั้น ๆ โดยมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งานอย่างต่อเนื่อง

หมวดที่ ๑๐
การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของกรมทางหลวง
(Information Security Incident Management)

ข้อ ๔๑ ให้มีการรายงานเหตุการณ์และจุดอ่อนต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information Security Events) โดยเจ้าหน้าที่ทุกคน และผู้รับจ้าง รวมถึงหน่วยงานภายนอกที่ปฏิบัติงานในกรมทางหลวง จะต้องทำการบันทึก และรายงานถึงจุดอ่อนเกี่ยวกับความมั่นคงปลอดภัยของระบบหรือบริการ ที่สังเกตพบหรือสงสัยว่าจะเกิดขึ้นในระบบ จะต้องมีการรายงานผ่านช่องทางการรายงานอย่างเหมาะสมด้วยความรวดเร็วที่สุดเท่าที่จะทำได้

ข้อ ๔๒ ให้มีการกำหนดบทบาท หน้าที่ความรับผิดชอบที่ชัดเจน ในการจัดการกับเหตุการณ์ที่เกิดขึ้นด้วยความรวดเร็ว และมีประสิทธิผล รวมถึงจะต้องจัดให้มีกลไกในการพิจารณาถึงประเภทของเหตุการณ์ ปริมาณและต้นทุนที่เกิดขึ้น ต้องมีการรวบรวม จัดเก็บ และดูแลรักษาหลักฐานต่าง ๆ ที่เกี่ยวกับการดำเนินการจากเหตุการณ์ต่าง ๆ ที่เกิดขึ้น เพื่อใช้เป็นประโยชน์ในการดำเนินการทางคดีความ

ข้อ ๔๓ การอนุญาตให้มีการใช้งาน Mobile code หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile Code (เช่น Script บางอย่างของเว็บแอปพลิเคชันที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ควรมีการตั้งค่าการทำงาน (Configuration) เพื่อให้มั่นใจได้ว่าการทำงานของ Mobile Code นั้นเป็นไปตามความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ ๑๑
การบริหารความต่อเนื่องในการดำเนินงานของกรมทางหลวง
(Business Continuity Management)

ข้อ ๔๔ ให้มีการกำหนดกระบวนการในการสร้างความต่อเนื่องในการดำเนินงาน เพื่อป้องกันการติดขัด หรือการหยุดชะงักของการดำเนินงานต่าง ๆ อันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศและให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม มีการบริหารจัดการและการปรับปรุงกระบวนการอย่างสม่ำเสมอ จะต้องมีการระบุถึงเหตุการณ์ที่จะมีผลให้เกิดการหยุดชะงักของกระบวนการดำเนินงานโอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของกรมทางหลวง

ข้อ ๔๕ ให้มีการจัดทำและใช้งานแผนสร้างความต่อเนื่องในการดำเนินงานต่าง ๆ ให้สามารถดำเนินงานต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้การดำเนินงานเกิดการหยุดชะงัก หรือความผิดพลาดขึ้น

ข้อ ๔๖ ให้มีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับการดำเนินงาน เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้และจัดความสำคัญของงานต่าง ๆ ที่ต้องดำเนินการ ต้องจัดให้มีการทดสอบ และปรับปรุงแผนความต่อเนื่องในการดำเนินงานอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ถึงความทันสมัย และความมีประสิทธิผล

หมวดที่ ๑๒
การปฏิบัติตามข้อกำหนด (Compliance)

ข้อ ๔๗ ให้มีการดำเนินการตามข้อกำหนดทางกฎหมาย (Legal Requirements) การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย ระเบียบปฏิบัติ ข้อบังคับ ประกาศ และข้อกำหนดในสัญญาต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานโดยต้องบันทึกข้อกำหนดเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัยอยู่เสมอ รวมถึงมีการกำหนดแนวทางปฏิบัติเพื่อให้สอดคล้องตามข้อกำหนดต่าง ๆ ด้วย

ข้อ ๔๘ ให้มีการกำหนดแนวทางในการดำเนินงาน เพื่อปกป้องจากการดำเนินงานในลักษณะที่เป็นการละเมิดสิทธิ์ หรือสินทรัพย์ทางปัญญา (Intellectual Property Rights, IPR) การดูแลป้องกันข้อมูลที่สำคัญของกรมทางหลวง และข้อมูลส่วนบุคคล จากการสูญหาย เสียหาย หรือมีการปลอมแปลง มีมาตรการในการป้องกันการนำอุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศ ไปใช้ผิดวัตถุประสงค์ และมีมาตรการในการควบคุมการเข้ารหัสข้อมูลให้สอดคล้องตามข้อตกลง ข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง

ข้อ ๔๙ ให้มีการกำหนดการปฏิบัติตามนโยบายมาตรฐานความมั่นคงปลอดภัย และข้อกำหนดทางเทคนิค มีการกำหนดให้ผู้บังคับบัญชาในหน่วยงานต่าง ๆ คอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนอย่างถูกต้อง ตามนโยบายและมาตรฐานความมั่นคงปลอดภัยกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัย

ข้อ ๕๐ ให้มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) โดยมีการวางแผนระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศของกรมทางหลวง การดำเนินการตรวจสอบระบบการปฏิบัติงานอย่างระมัดระวัง โดยให้เกิดผลกระทบต่อการหยุดชะงักของกระบวนการดำเนินงานน้อยที่สุด รวมถึงจะต้องมีการกำหนดมาตรการในการเข้าถึงเครื่องมือที่ใช้

ในการตรวจประเมินระบบสารสนเทศ เพื่อป้องกันการนำไปใช้งานผิดวัตถุประสงค์ ในระหว่างที่ทำการตรวจประเมิน

ข้อ ๕๑ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๕๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๕ กุมภาพันธ์ พ.ศ. ๒๕๖๘

(นายอภิรัฐ ไชยวงศ์น้อย)
อธิบดีกรมทางหลวง

เอกสารแนบท้ายประกาศ

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของ กรมทางหลวง พ.ศ.๒๕๖๘

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนรวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบายและการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดย ผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น 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 ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมทางหลวงจึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวง ประจำปีงบประมาณ พ.ศ.๒๕๖๘ ขึ้น เพื่อให้ทุกหน่วยงานในกรมทางหลวง เผยแพร่ให้บุคลากรทุกคน มีความรู้ เข้าใจในนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวง และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

กรมทางหลวง

สารบัญ

	หน้าที่
บทนำ	๑
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. องค์ประกอบของนโยบาย	๑
๔. บทบังคับใช้	๒
๕. การเผยแพร่และทบทวน	๒
คำนิยาม	๓
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๕
ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	๕
๑. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล	๕
๒. การแบ่งประเภทของข้อมูลและการจัดระดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล	๖
ส่วนที่ ๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for access control)	๘
ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๙
๑. การกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ	๙
๒. การลงทะเบียนผู้ใช้งาน (User registration)	๙
๓. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)	๙
๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)	๙
๕. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)	๑๐
ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	๑๒
๑. การใช้งานรหัสผ่าน (Password Use)	๑๒
๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์	๑๒
๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)	๑๒
๔. การเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ	๑๓
ส่วนที่ ๕ การจัดการการเข้าถึงระบบเครือข่าย (Network Access Control)	๑๔
๑. การเข้าใช้งานระบบเครือข่ายที่มั่นคงปลอดภัย	๑๔
๒. การเชื่อมต่อระบบเครือข่ายจากภายนอกองค์กร	๑๖
๓. การระบุอุปกรณ์บนเครือข่าย	๑๖
๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ	๑๖

หน้าที่

๕. การแบ่งแยกเครือข่าย ๑๗
๖. การควบคุมการเชื่อมต่อทางเครือข่าย ๑๗
๗. การควบคุมการจัดเส้นทางบนเครือข่าย ๑๗
ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) ๑๘
๑. การเข้าใช้งานที่มั่นคงปลอดภัย ๑๘
๒. การระบุและยืนยันตัวตนของผู้ใช้งาน ๑๘
๓. การบริหารจัดการรหัสผ่าน ๑๘
๔. การใช้งานโปรแกรมอรรถประโยชน์ ๑๙
๕. การว่างเว้นจากการใช้งานระบบสารสนเทศ ๑๙
๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ๑๙
๗. การอนุญาตมีการใช้ Mobile Code ๑๙
ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) ๒๑
๑. การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ ๒๑
๒. การควบคุมการเปลี่ยนแปลง หรือการแก้ไขระบบสารสนเทศ ๒๑
๓. การควบุมการเข้าถึงสารสนเทศ (Information Access Restriction) ๒๑
๔. การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ๒๕
๕. การทบทบการกำหนดค่ามาตรฐานขั้นต่ำ ๒๖
๖. การคัดเลือกผู้ให้บริการ ๒๖
๗. การจัดการระบบซึ่งไวต่อการรบกวน ๒๗
๘. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ๒๗
๙. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ๒๘
ส่วนที่ ๘ การใช้งานอินเทอร์เน็ต (Use of Internet) ๓๐
ส่วนที่ ๙ การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic mail) ๓๑
ส่วนที่ ๑๐ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) ๓๕
ส่วนที่ ๑๑ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ ๔๐
ส่วนที่ ๑๒ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) ๔๓
ส่วนที่ ๑๓ หน้าที่และความรับผิดชอบด้านสารสนเทศ ๔๕

บทนำ

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ *"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"* และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรที่ต้องได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีความสำคัญอย่างยิ่งต่อองค์กรที่จะต้องมีการวางแผนและมีกระบวนการบริหารด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๒. วัตถุประสงค์

เพื่อให้กรมทางหลวงสามารถใช้ระบบเทคโนโลยีสารสนเทศประกอบการปฏิบัติงาน การดำเนินการใด ๆ ด้วยวิธีทางอิเล็กทรอนิกส์ การให้บริการหน่วยงานและประชาชนได้อย่างเหมาะสมมีประสิทธิภาพ ตลอดจนเป็นการสร้างความเชื่อมั่นของหน่วยงานและประชาชนต่อการดำเนินการของกรมทางหลวง จึงได้จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมทางหลวงขึ้น โดยแต่ละส่วนจะประกอบด้วย วัตถุประสงค์ รายละเอียด และขั้นตอนของแนวทางในการปฏิบัติ

๓. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทางหลวง โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ อ้างอิงตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ และมาตรฐานสากล ISO/IEC 27001 : 2013 โดยแนวทางปฏิบัตินี้ประกอบด้วย วัตถุประสงค์ และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมทางหลวง

๔. บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูล และระบบสารสนเทศของกรมทางหลวง บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุนและติดตามการประยุกต์ใช้ โดยอธิบดีกรมทางหลวง

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อธิบดีกรมทางหลวง เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

๕. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทางหลวงฉบับนี้จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) กรมทางหลวง จัดพิมพ์เผยแพร่เพื่อให้บุคลากรกรมทางหลวงและบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

คำนิยาม

๑. **หน่วยงาน หรือ องค์กร** หมายถึง กรมทางหลวง

๒. **ผู้บริหารระดับสูง** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของ กรมทางหลวง

๓. **การรักษาความมั่นคงปลอดภัย** หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศของกรมทางหลวง

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

๔.๑ ผู้บริหารสูงสุด หมายถึง อธิบดีกรมทางหลวง

๔.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) ประจำกรมทางหลวง หมายถึง ผู้ที่ได้รับการแต่งตั้งเป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม

๔.๓ ผู้ดูแลระบบ/ผู้ดูแลห้องเครื่อง หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์

๔.๔ ผู้พัฒนาระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอพพลิเคชั่น

๔.๕ เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการของกรมทางหลวง

๔.๖ บุคคลภายนอก หมายถึง บุคคลที่กรมทางหลวงอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมทางหลวงได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของกรมฯ เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับกรมทางหลวง หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิต/นักศึกษาฝึกงาน

๕. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๖. **สินทรัพย์ (Asset) หรือ ทรัพย์สินสารสนเทศ** หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

๖.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๖.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)** หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๘. **ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security)** หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผยขัดขวาง เปลี่ยนแปลงแก้ไขทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๙. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัย

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

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูล และอุปกรณ์ประมวลผลข้อมูล

๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑) ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของกรมทางหลวง และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(ก) ชื่อ/คำอธิบายของทรัพย์สิน

(ข) ฟังก์ชันที่สำคัญของทรัพย์สิน

(ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สิน

(ง) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน

(จ) ตำแหน่งทางกายภาพของทรัพย์สินแต่ละรายการ

(ฉ) การขึ้นต่อกันของทรัพย์สิน

หมายเหตุ การขึ้นต่อกันของทรัพย์สิน ฯ หมายถึง ทรัพย์สินนั้นมีความสัมพันธ์หรือความเกี่ยวข้องกับทรัพย์สินอื่นใดหรือไม่ เช่น เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์กับทรัพย์สินนั้น จะทำให้ทรัพย์สินอื่นที่เกี่ยวข้อง ได้รับผลกระทบด้วย

๒) ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของกรมทางหลวง และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง และมีนัยสำคัญ (Direct and Significant Interface)

๓) ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้งหากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของกรมทางหลวง ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๒ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ก็ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

๑.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

๒) กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

๒.๑ ประเภทข้อมูล แบ่งตามลักษณะการใช้งานได้ดังนี้

๑) ข้อมูลด้านการบริหาร หมายถึง เอกสารหรือข้อมูลต่าง ๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่ใช้ในการบริหารหน่วยงาน มีความสำคัญและให้ล่วงรู้ได้เฉพาะบุคคลหรือกลุ่มบุคคลที่มีหน้าที่โดยตรงต่อข้อมูลนั้น ๆ ได้แก่ข้อมูลสารสนเทศด้านการบริหาร ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลงบประมาณการเงินและบัญชี

๒) ข้อมูลภายใน (Internal Data) หมายถึง เอกสารหรือข้อมูลต่างๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่ใช้ภายในหน่วยงาน ได้แก่

(ก) ข้อมูลสารสนเทศกระบวนการหลัก ประกอบด้วย ข้อมูลงานก่อสร้างทางหลวงข้อมูลงานสะพาน ข้อมูลบริหารบำรุงทาง ข้อมูลงานอำนวยความปลอดภัย

(ข) ข้อมูลสารสนเทศกระบวนการสนับสนุน ประกอบด้วย ข้อมูลงานเครื่องกลและสื่อสาร ข้อมูลงานจัดกรรมสิทธิ์ที่ดิน ข้อมูลบุคลากร

(ค) ข้อมูลภูมิศาสตร์สารสนเทศงานทาง ประกอบด้วย ข้อมูลพิกัดทางหลวงข้อมูลพิกัดสะพาน

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

๔) ข้อมูลที่เปิดเผยได้ หมายถึงเอกสารหรือข้อมูลต่าง ๆ รวมถึงข้อมูลทางอิเล็กทรอนิกส์และสารสนเทศต่าง ๆ ที่กรมทางหลวงสร้างขึ้นมาเองหรือได้รับจากภายนอก ที่สามารถเผยแพร่ให้ประชาชนหรือบุคคลทั่วไปรับทราบ ได้แก่ ข้อมูลสถิติอุบัติเหตุบนทางหลวง ข้อมูลระยะทางของทางหลวง ข้อมูลบริการประชาชน

๒.๒ ระดับความสำคัญของข้อมูล

๑) ความสำคัญระดับเคร่งครัด มีความสำคัญและให้ล่วงรู้ได้เฉพาะบุคคลหรือกลุ่มบุคคลที่มีหน้าที่โดยตรงต่อข้อมูลนั้น ๆ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนอาจจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ ได้แก่

สำคัญมาก ได้แก่ ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลด้านการวิจัย ข้อมูลคดีความ

สำคัญปานกลาง ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร ข้อมูลทะเบียนผู้รับเหมาก่อสร้างทาง

๒) ความสำคัญระดับกลาง ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน ต่อบุคคลภายนอก อาจก่อให้เกิดความเสียหายแก่ประโยชน์ของหน่วยงาน หรือบุคลากรของหน่วยงาน ได้แก่ ข้อมูลสำหรับปฏิบัติงานภารกิจของหน่วยงาน

๓) ความสำคัญระดับพื้นฐาน ได้แก่ข้อมูลเผยแพร่ 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 ผ่านระบบอินเทอร์เน็ต ผ่านระบบอินทราเน็ต ผ่านระบบงานโดยตรง ผ่านเครื่องคอมพิวเตอร์ส่วนบุคคล ผ่านโทรศัพท์มือถือ ผ่านเจ้าหน้าที่หน่วยงานเป็นผู้ดำเนินการให้ เป็นต้น

๓. การจัดเก็บและบันทึกข้อมูล Log

๓.๑ มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง

๓.๒ มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไข เปลี่ยนแปลงโดยไม่ได้รับอนุญาต

๓.๓ มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator)

๓.๔ มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ไว้ไม่น้อยกว่า ๙๐ วัน หรือตามที่กฎหมายกำหนด

ส่วนที่ ๒
การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ
(Business Requirement for access control)

วัตถุประสงค์

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศขององค์กร และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ

๑.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๒ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๒. จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ์ และภารกิจดังนี้

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

๒.๒ กลุ่มของผู้ดูแลระบบศูนย์เทคโนโลยีสารสนเทศ

๒.๓ กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของกรมทางหลวง

๒.๔ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับกรมทางหลวง

๒.๕ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

๓. การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๑ ทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อได้รับเอกสารแจ้งจากหน่วยงานต้นสังกัดของผู้ใช้งานระบบ เพื่อปรับปรุงการให้สิทธิ์แก่ผู้ใช้งานให้สอดคล้องกับการปฏิบัติงานที่เปลี่ยนไป เช่น เมื่อเปลี่ยนแปลงตำแหน่งงาน ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงานภายในองค์กร เป็นต้น

๓.๒ หน่วยงานต้นสังกัดของผู้ใช้งานต้องแจ้งเอกสารอย่างเป็นทางการแก่ผู้ดูแลระบบให้กำหนดสิทธิ์ตามหน้าที่ความรับผิดชอบในการปฏิบัติงานเมื่อมีผู้ใช้งานใหม่เข้ามาปฏิบัติงาน หรือยกเลิกสิทธิ์ต่าง ๆ ในการเข้าใช้ระบบสารสนเทศเมื่อมีผู้ใช้งานโยกย้าย หรือลาออก เป็นต้น

ส่วนที่ ๓
การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อความมั่นคงปลอดภัยของระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

แนวปฏิบัติ

๑. มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) อย่างน้อยปีละ ๑ ครั้ง

๑.๑ เสริมสร้างความเข้าใจ ในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้งาน

๑.๒ จัดหลักสูตรฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารเทคโนโลยีสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒. การลงทะเบียนผู้ใช้งาน (User registration) มีขั้นตอนปฏิบัติในครอบคลุมในเรื่องต่อไปนี้

๒.๑ จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิ์และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

๒.๒ ผู้ดูแลระบบตรวจสอบบัญชีผู้ใช้งาน ให้ไม่ซ้ำซ้อนกับบัญชีผู้ใช้งานที่มีอยู่เดิม

๒.๓ ผู้ดูแลระบบตรวจสอบและมอบหมายสิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒.๔ ผู้ดูแลระบบจัดทำเอกสารแสดงถึงสิทธิ์ และหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งผู้ใช้งานต้องลงนามรับทราบด้วย

๒.๕ ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบเทคโนโลยีสารสนเทศ

๒.๖ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๗ มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๒.๘ ผู้ดูแลระบบต้องทบทวนสิทธิ์ของบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓. มีการบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ์เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๓.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เหมาะสมตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานให้เหมาะสมกับระบบเทคโนโลยีสารสนเทศ

๓.๓ ผู้ดูแลระบบมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๓.๔ ผู้ดูแลระบบต้องทบทวนสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๔. มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวน การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๔.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้ง หรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๔.๒ ผู้ดูแลระบบต้องตั้งรหัสผ่านชั่วคราวที่ยากต่อการเดา และต้องมีความแตกต่างกัน

๔.๓ ผู้ดูแลระบบต้องให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

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

๔.๕ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

๕. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน

๕.๑ ผู้ดูแลระบบต้องทบทวนสิทธิ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออกเปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๕.๒ ผู้ดูแลระบบทบทวนสิทธิ์ ผู้ที่มีสิทธิ์ในระดับสูง ได้แก่ สิทธิ์ระดับผู้ดูแลระบบ ด้วยความถี่กว่าสิทธิ์ระดับผู้ใช้งาน

๖. การยกระดับสิทธิ์

๖.๑ การขอใช้งานสิทธิ์สูงสุด หรือเทียบเท่า (High Privilege User) จะต้องมีการกรอกแบบฟอร์มขอใช้งานเมื่อมีเหตุจำเป็นเร่งด่วน และต้องมีการยืนยันตัวตนของผู้ร้องขอ โดยประกอบด้วย ดังนี้

๑) ต้องมีความเกี่ยวข้องกับระบบสารสนเทศนั้น ๆ

๒) ต้องได้รับมอบหมายจากผู้มีส่วนได้ส่วนเสียของระบบ

๓) ต้องมีเอกสารยืนยันตัวตนที่ชัดเจน เช่น สำเนาบัตรประชาชน

๔) ต้องกรอกแบบฟอร์มขอใช้สิทธิ์สูงสุด หรือเทียบเท่า (High Privilege User) และระบุเวลาขอใช้สิทธิ์ให้ชัดเจนเป็นรายครั้ง

๖.๒ ต้องจัดทำทะเบียนคุมการจัดสรรสิทธิ์สูงสุด หรือเทียบเท่า (High Privilege User) ครอบคลุมสิทธิ์ของ Server, Database, Network และ Application ซึ่งสามารถระบุได้ว่าเป็นใคร และใช้ทำงานในเรื่องใด

๖.๓ ผู้ที่ได้รับสิทธิ์สูงสุดจะต้องใช้งานอย่างระมัดระวังตลอดระยะเวลาใช้สิทธิ์ โดยสิทธิ์นั้นจะมีระยะเวลาตามที่ได้รับอนุญาต และต้องไม่ไม่ส่งต่อสิทธิ์ที่ได้รับให้บุคคลอื่น หากตรวจสอบพบจะดำเนินการตามบทลงโทษสูงสุด

๖.๔ เมื่อผู้ขอใช้งานสิทธิ์สูงสุด หรือเทียบเท่า (High Privilege User) ครบเวลาที่ได้รับอนุญาต ผู้ให้สิทธิ์จะทำการยกเลิกสิทธิ์ทันที และผู้ให้สิทธิ์จะมีการตรวจสอบความถูกต้อง สำรวจความเสียหายที่อาจจะเกิดขึ้น โดยผู้ที่ขอใช้สิทธิ์สูงสุดจะไม่สามารถเข้าถึงสิทธิ์ที่ได้รับอีกเลย จนกว่าจะมีการขอใช้สิทธิ์อีกครั้ง

๖.๕ หากมีข้อผิดพลาดระหว่างถือครองสิทธิ์สูงสุด หรือเทียบเท่า (High Privilege User) และผู้ดูแลระบบตรวจสอบได้ว่าการกระทำใด ๆ ที่เกิดขึ้นแล้วมีผลกระทบต่อระบบหรือเสียหาย ให้ถือเป็นความผิดของผู้ใช้สิทธิ์ และไม่สามารถปฏิเสธความรับผิดชอบได้

๖.๖ หากระบบสารสนเทศเกิดความเสียหาย และความเสียหายที่เกิดขึ้นนั้น ประเมินเป็นมูลค่า ผู้ที่กระทำให้เกิดความเสียหายนั้น ต้องกระทำการใด ๆ ให้ระบบสามารถใช้งานได้สมบูรณ์ ไม่เช่นนั้น

กรมทางหลวงมีสิทธิ์นำบุคคลอื่นเข้ามาดำเนินการเพื่อให้ระบบสารสนเทศกลับมาใช้งานได้ดังเดิม หากมีค่าใช้จ่ายที่เกิดขึ้นผู้กระทำให้เกิดความเสียหาย ต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้น

๖.๗ มีการทบทวนการใช้สิทธิ์สูงสุด หรือเทียบเท่า (High Privilege User) อย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง และลงนามเป็นหลักฐานในเอกสารการทบทวนสิทธิ์

ส่วนที่ ๔
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีแนวปฏิบัติอย่างน้อย ดังนี้

แนวปฏิบัติ

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

๑.๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

๑.๒ ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

๑.๓ ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๑.๔ ผู้ใช้งานต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๑.๕ ผู้ใช้งานต้องไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

๑.๖ ผู้ใช้งานต้องไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑.๗ ผู้ใช้งานต้องเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๑.๘ ผู้ใช้งานต้องไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในคอมพิวเตอร์

๑.๙ ผู้ใช้งานต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

๑.๑๐ ผู้ใช้งานต้องไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

๑.๑๑ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยต้องทำการเปลี่ยนรหัสผ่านโดยทันที

๑.๑๒ ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๑.๑๓ ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๑.๑๔ ผู้ใช้งานต้องหลีกเลี่ยงการใช้รหัสผ่านเดิม

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

๒.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน

๒.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาทีและต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๒.๓ ผู้ใช้งานต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือ

สารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

๓.๑ ผู้ใช้งานทุกคนต้องออกจากระบบที่ใช้งานทันที เมื่อจำเป็นต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

๓.๒ ผู้ใช้งานมีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๓.๓ ผู้ใช้งานทุกคนต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญของกรมทางหลวงไว้ในที่ปลอดภัย โดยเก็บไว้ในตู้เอกสารที่มีระบบล็อค และมีกุญแจเปิดปิด

๓.๔ ผู้ใช้งานต้องลงชื่อออก (Log out) จากเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน และทำการล็อคประตูห้องระหว่างพักเที่ยงหรือเมื่อผู้ใช้งานกลับบ้านหลังเลิกงาน

๓.๕ ผู้ใช้งานต้องทำการล็อคประตูห้อง ที่มีเครื่องโทรสารระหว่างพักเที่ยง หรือเมื่อผู้ใช้งานกลับบ้านหลังเลิกงาน

๓.๖ ผู้ใช้งานต้องทำการป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

๓.๗ ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสารโดยไม่ได้รับอนุญาต

๓.๘ ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๙ ข้อมูลสำคัญที่บันทึกไว้ในกระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟ หรือฮาร์ดดิสก์เมื่อไม่ได้ใช้งานต้องเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๓.๑๐ เอกสารสำคัญ และสื่อบันทึกข้อมูลแบบใช้ครั้งเดียวที่ผ่านการใช้งานแล้วต้องถูกทำลายโดยการแยกทำลายโดยใช้เครื่องทำลายเอกสาร

๓.๑๑ เอกสารบนสื่อบันทึกข้อมูลแบบใช้ซ้ำต้องทำการลบข้อมูลแบบถาวรป้องกันการกู้คืนโดยใช้มาตรฐาน DoD 5220.22-M หรือมาตรฐานการลบทำลายข้อมูลที่สูงกว่า

๔. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ ดังนี้

ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากลด้วย SSL เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

ส่วนที่ ๕
การจัดการการเข้าถึงระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมทางหลวง

แนวปฏิบัติ

๑. การเข้าใช้งานที่มั่นคงปลอดภัย

๑.๑ ศูนย์เทคโนโลยีสารสนเทศต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น

๑.๒ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อบุคคลอื่น

๑.๓ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๑.๔ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการพาณิชย์

๑.๕ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่กรมทางหลวง ไม่ว่าจะเป็นข้อมูลของกรมทางหลวง หรือบุคคลภายนอกก็ตาม

๑.๖ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการกระทำอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของกรมทางหลวงหรือของบุคคลอื่น

๑.๗ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้มีสิทธิ์ในข้อมูลดังกล่าว

๑.๘ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายต่อกรมทางหลวง ได้แก่ การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิ์ของบุคคลอื่นไปยังผู้ใช้งานหรือบุคคลอื่น เป็นต้น

๑.๙ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อขัดขวางการใช้งานระบบเทคโนโลยีสารสนเทศของกรมทางหลวง หรือของผู้ใช้งานอื่น หรือเพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมทางหลวงไม่สามารถใช้งานได้ตามปกติ

๑.๑๐ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวกับการดำเนินงานของกรมทางหลวงไปยังที่อยู่เว็บไซต์ใด ๆ ในลักษณะที่จะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

๑.๑๑ ผู้ใช้งานต้องไม่ใช้งานระบบเครือข่าย เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของกรมทางหลวงหรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อกรมทางหลวง

๑.๑๒ ผู้ใช้งานต้องทำการเข้าถึงระบบเครือข่ายตามสิทธิ์ และหน้าที่ของตนเองเท่านั้นห้ามมิให้ทำการใช้งานระบบเครือข่ายโดยใช้สิทธิ์ของผู้อื่น

๑.๑๓ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

๑.๑๔ ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก และแบบฟอร์มการขออนุญาตเข้า - ออกเป็นประจำทุกเดือน

๑.๕ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่ายกรมทางหลวง”

๑.๑๖ การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

๑.๑๗ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๑.๑๘ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๔) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System /Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๕) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๖) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

๗) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑.๑๙ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

๑.๒๐ กำหนดให้มีการจัดเก็บ Sauce code library และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๒. การเชื่อมต่อจากภายนอกองค์กร

๒.๑ การเข้าสู่เครือข่ายของกรมทางหลวงผ่านทางเครือข่ายภายนอก หรือระบบอินเทอร์เน็ตต้องทำโดยผ่านทางช่องทางการเชื่อมต่อแบบปลอดภัยด้วยวิธีการ VPN

๒.๒ การเข้าสู่เครือข่ายของกรมทางหลวงผ่านทางเครือข่ายภายนอกต้องมีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ทุกครั้ง และต้องมีการบันทึกข้อมูลจราจรที่ได้ทำการใช้งานไว้ไม่ต่ำกว่า ๙๐ วัน

๒.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๒.๔ มีการกำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อเว้นว่างจากการใช้งานเป็นเวลานาน

๓. การระบุอุปกรณ์บนเครือข่าย

๓.๑ ผู้ดูแลระบบต้องมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๓.๒ อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่ผู้ดูแลระบบเครือข่ายกำหนด

๓.๓ ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๓.๔ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๓.๕ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๓.๖ ผู้ขอใช้บริการต้องลงทะเบียน “คำขอมีบัญชีรายชื่อผู้ใช้งานระบบเครือข่ายสื่อสารข้อมูลกรมทางหลวง” โดยลงทะเบียนผ่านระบบพิสูจน์ตัวตน (Authentication) กรมทางหลวง

๓.๗ การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๔.๑ มีการติดตั้งอุปกรณ์ IPS เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่าย

๔.๒ ผู้ดูแลระบบต้องทำการป้องกันอุปกรณ์เครือข่ายจากการเข้าถึงเพื่อเปลี่ยนแปลงค่าโดยไม่ได้รับอนุญาตโดย ต้องทำการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึง โดยทำการปิดพอร์ตที่ไม่มีความจำเป็นในการใช้งาน และกำหนดพอร์ตเฉพาะในการเข้าถึงอุปกรณ์

๔.๓ ผู้ดูแลระบบต้องทำการกำหนดรหัสผ่านในการเข้าถึงเพื่อเปลี่ยนแปลงค่าของอุปกรณ์ให้ ยากแก่การคาดเดาและมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

๕. การแบ่งแยกเครือข่าย

๕.๑ ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายโดยใช้ VLAN แบ่งแยกเครือข่ายแต่ละสำนักออกจากกัน เพื่อป้องกันการละเมิดสิทธิ์และทรัพยากรเครือข่ายของแต่ละหน่วยงาน

๕.๒ ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายออกเป็นโซนเพื่อความมั่นคงปลอดภัยของระบบงานจากการบุกรุกทางเครือข่าย

๖. การควบคุมการเชื่อมต่อทางเครือข่าย

๖.๑ ผู้ใช้งานมีสิทธิ์ในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิ์ที่ได้รับตามอำนาจหน้าที่ของตนเอง

๖.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการใช้งานเครือข่ายทุกครั้ง

๖.๓ ผู้ใช้งานต้องไม่นำอุปกรณ์เครือข่ายมาติดตั้งก่อนได้รับอนุญาต

๖.๔ ผู้ดูแลระบบต้องทำการตรวจสอบการเชื่อมต่อบนเครือข่ายหากพบการเชื่อมต่อจากอุปกรณ์นอกเหนือจากที่ได้รับอนุญาตต้องทำการระงับการเชื่อมต่อโดยทันที

๖.๕ ผู้ดูแลระบบต้องทำการจำกัดสิทธิ์ในการใช้งานระบบเครือข่ายร่วมกัน ได้แก่ การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่ายของแต่ละระบบงานตามความเหมาะสม

๖.๖ ระบบเครือข่ายที่มีการเชื่อมต่อไปยังเครือข่ายภายนอกต้องเชื่อมต่อผ่านอุปกรณ์ IPS และ Firewall

๗. การควบคุมการเชื่อมต่อทางเครือข่ายแบบไร้สาย (Wireless LAN Access Control)

๗.๑ การกำหนดค่าอุปกรณ์กระจายสัญญาณ (Access Point) ให้มีความปลอดภัยก่อนติดตั้งใช้งาน

๗.๒ การเข้ารหัสข้อมูลระหว่างอุปกรณ์ (Wireless LAN Client) กับ อุปกรณ์กระจายสัญญาณ (Access Point)

๗.๓ การควบคุมสัญญาณของอุปกรณ์การจายสัญญาณ (Access Point)

๗.๔ การป้องการนำอุปกรณ์กระจายสัญญาณ (Access Point) ที่ไม่ได้รับอนุญาตมาใช้งาน

๗.๕ การควบคุมไม่ให้บุคคลไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สาย

๗.๖ การตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย

๘. การควบคุมการจัดเส้นทางบนเครือข่าย

๘.๑ ผู้ดูแลระบบต้องทำการกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

๘.๒ ผู้ดูแลระบบต้องทำการกำหนดหมายเลขเครือข่ายให้เหมาะสมตามความจำเป็นในการใช้งาน

๘.๓ ผู้ดูแลระบบต้องทำการจำกัดสิทธิ์ในการใช้งานในแต่ละกลุ่มเครือข่ายย่อยให้มีการใช้งานเฉพาะกลุ่มของตนเองเพื่อป้องกันการละเมิดและถูกละเมิด

ส่วนที่ ๖
การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

แนวปฏิบัติ

๑. การเข้าใช้งานที่มั่นคงปลอดภัย

๑.๑ ผู้ใช้งานต้องทำการกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบ

๑.๒ ผู้ใช้งานต้องทำการตั้งค่าให้ระบบปฏิบัติการทำการป้องกันด้วยรหัสผ่านทุกครั้งที่เปิดใช้งาน

๑.๓ ผู้ใช้งานต้องทำการตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเมื่อไม่มีการใช้งานให้ทำการล็อคด้วยรหัสผ่าน

๑.๔ ผู้ใช้งานต้องทำการลงบันทึกออกทุกครั้งเมื่อไม่ได้ใช้งานเป็นเวลานาน

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน

๒.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒.๒ การเข้าใช้งานระบบปฏิบัติการต้องมีพิสูจน์ตัวตนด้วยบัญชีผู้ใช้ทุกครั้ง

๒.๓ ผู้ใช้งานต้องทำการลงชื่อออกทันทีที่เลิกใช้งานหรือว่างเว้นจากการใช้งานเป็นเวลานาน

๒.๔ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งาน หากพบว่าการยืนยันตัวตนผิดพลาดไม่สามารถเข้าใช้งานได้ต้องทำการแจ้งผู้ดูแลระบบให้ทำการแก้ไขทันที

๒.๕ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ต้องรับผิดชอบผลจากการใช้งานบัญชีผู้ใช้ของตนเองทุกกรณี

๒.๖ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ให้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามมิให้มีการจำหน่ายจ่ายแจกให้ผู้อื่น หรือมีการใช้งานร่วมกัน

๓. การบริหารจัดการรหัสผ่าน

๓.๑ รหัสผ่านที่ใช้งานในระบบต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร ที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ กำหนดให้ระบบมีการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักขระ ตัวเลข และตัวอักขระพิเศษ

๓.๒ ระบบต้องทำการระงับสิทธิ์ในการเข้าสู่ระบบหากมีการป้อนรหัสผ่านผิดเกิน ๓ ครั้ง

๓.๓ ระบบจะต้องไม่แสดงข้อมูลรหัสผ่านระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านโดยให้แสดงเป็นสัญลักษณ์แทน

๓.๔ รหัสผ่านของผู้ใช้ต้องมีการเปลี่ยนรหัสผ่านทุก ๆ ๖ เดือน

๔. การใช้งานโปรแกรมอรรถประโยชน์

๔.๑ ผู้ใช้ต้องไม่ทำการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์ หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเอง และต่อกรมทางหลวง

๔.๒ ผู้ใช้ต้องไม่ติดตั้งใช้งานโปรแกรมอรรถประโยชน์ที่เป็นการตรวจสอบ หรือหลีกเลี่ยงระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และระบบเครือข่าย

๔.๓ ผู้ใช้ต้องไม่ทำการติดตั้งโปรแกรมอรรถประโยชน์โดยไม่จำเป็น และถอนการติดตั้งโปรแกรมอรรถประโยชน์ทันทีหากไม่มีความจำเป็นในการใช้งาน เพื่อลดช่องโหว่ของระบบคอมพิวเตอร์ที่ใช้

๔.๔ ผู้ใช้ต้องทำการติดตั้งโปรแกรมป้องกันผู้ไม่ประสงค์ดีที่ศูนย์เทคโนโลยีสารสนเทศจัดหาให้

๕. การว่างเว้นจากการใช้งานระบบสารสนเทศ

๕.๑ ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศมีการตัด และหมดเวลาในการใช้งาน หากไม่มีการใช้งานเป็นเวลา ๑๕ นาที

๕.๒ ผู้ใช้ต้องทำการล้างหน้าจอหรือทำการล็อคหน้าจอเมื่อมีการว่างเว้นจากการใช้งานและต้องลุกหรือเคลื่อนย้ายจากเครื่องคอมพิวเตอร์ที่กำลังทำงานอยู่

๕.๓ ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อที่สั้นลงสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เพื่อเพิ่มความปลอดภัยให้กับระบบงานจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

๖.๑ ผู้ดูแลระบบต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบงานภายในให้ใช้งานได้เฉพาะช่วงเวลาปกติ เมื่อเลยกำหนดเวลาให้ตัดการเชื่อมต่อทันที ในกรณีที่ต้องมีการเชื่อมต่อในช่วงเวลาอื่นให้ทำการร้องขอการใช้งานให้ศูนย์เทคโนโลยีสารสนเทศพิจารณาเป็นครั้ง ๆ ไป

๖.๒ การเชื่อมต่อที่ให้บริการแก่ประชาชนให้ใช้งานได้ตลอดเวลาแต่จำกัดการเชื่อมต่อให้สามารถใช้งานได้นานที่สุดไม่เกิน ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

๖.๓ การเชื่อมต่อจากภายนอกผ่าน SSL VPN ให้จำกัดเวลาการเชื่อมต่อที่ ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง หากต้องการใช้งานต่อต้องทำการพิสูจน์ตัวตนเพื่อเข้าใช้งานอีกครั้ง

๗. หากหน่วยงานอนุญาตให้มีการใช้งาน Mobile Code มีการกำหนดการใช้งาน Mobile Code (เช่น Script บางอย่างของเว็บแอปพลิเคชันที่มีการทำงานอัตโนมัติเมื่อเรียกดูเว็บ) ดังนี้

๗.๑ การอนุญาตใช้งาน Mobile Code

๑) อนุญาตเฉพาะ Mobile Code จากแหล่งที่เชื่อถือได้และผ่านการรับรอง

๒) ห้ามใช้ Mobile Code ที่ไม่ได้รับอนุญาตในระบบขององค์กร

๗.๒ การควบคุมแหล่งที่มา

๑) กำหนดรายการ (White List) ของแหล่งที่มาที่ได้รับอนุญาตสำหรับ Mobile Code

๒) บล็อกการดาวน์โหลดและการทำงานของ Mobile Code จากแหล่งที่ไม่ได้รับอนุญาต

๗.๓ การตรวจสอบและการอนุมัติ

๑) กำหนดกระบวนการตรวจสอบและอนุมัติ Mobile Code ก่อนการใช้งานในระบบขององค์กร

๒) ระบุบุคคลหรือทีมที่รับผิดชอบในการตรวจสอบและอนุมัติ

๗.๔ การจำกัดสิทธิ์

๑) จำกัดสิทธิ์การเข้าถึงของ Mobile Code ให้อยู่ในระดับต่ำสุดที่จำเป็น

๒) ห้าม Mobile Code เข้าถึงข้อมูลที่ละเอียดอ่อนหรือระบบสำคัญโดยไม่ได้รับอนุญาต

๗.๕ การใช้งาน Sandbox

๑) กำหนดให้ Mobile Code ทำงานในสภาพแวดล้อมแบบ Sandbox เพื่อจำกัดการเข้าถึงทรัพยากรระบบ

๒) ระบุข้อกำหนดสำหรับการตั้งค่า Sandbox

๗.๖ การอัปเดตและการจัดการแพตช์

๑) กำหนดนโยบายการอัปเดตและการจัดการแพตช์สำหรับซอฟต์แวร์ที่เกี่ยวข้องกับ Mobile Code

๒) ระบุระยะเวลาที่ยอมรับได้สำหรับการติดตั้งแพตช์ความปลอดภัยที่สำคัญ

๗.๗ การเฝ้าระวังและการตรวจสอบ

๑) กำหนดให้มีการเฝ้าระวังการทำงานของ Mobile Code อย่างต่อเนื่อง

๒) จัดทำบันทึกกิจกรรม (logs) และตรวจสอบอย่างสม่ำเสมอ

๗.๘ การฝึกอบรมพนักงาน

๑) จัดให้มีการฝึกอบรมความปลอดภัยเกี่ยวกับ Mobile Code สำหรับพนักงานทุกคน

๒) กำหนดความถี่ในการฝึกอบรมและการทดสอบความเข้าใจ

๗.๙ การจัดการเหตุการณ์

๑) กำหนดขั้นตอนการรายงานและการจัดการเหตุการณ์ที่เกี่ยวข้องกับ Mobile Code

๒) ระบุทีมรับผิดชอบและช่องทางการติดต่อในกรณีฉุกเฉิน

๗.๑๐ การทบทวนนโยบาย

๑) กำหนดให้มีการทบทวนและปรับปรุงนโยบายทุก ๑ ปี

๒) ระบุผู้รับผิดชอบในการทบทวนและอนุมัติการเปลี่ยนแปลงนโยบาย

ส่วนที่ ๗
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของกรมทางหลวง และป้องกันการบุกรุกจากโปรแกรมไม่พึงประสงค์และการบุกรุกจากผู้ไม่ประสงค์ดีที่จะสร้างความเสียหายให้แก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก

แนวปฏิบัติ

๑. การจัดหา การพัฒนาและบำรุงรักษาระบบสารสนเทศ

ในการพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของการ พัฒนาซอฟต์แวร์ (Software Development Lifecycle : SDLC) โดยครอบคลุมตั้งแต่ขั้นตอนการรวบรวมความต้องการ การออกแบบ การพัฒนา การทดสอบ การใช้งาน ตลอดไปจนถึงการยกเลิกการใช้งานระบบ

๑.๑ การวางแผนโครงการ (Planning)

จัดตั้งทีมงาน เพื่อเตรียมการดำเนินงานจากนั้นทีมงานดังกล่าวร่วมกันค้นหาสร้างแนวทางและเลือกทางที่ดีที่สุดในการนำระบบใหม่มาใช้งาน เมื่อได้ทางเลือกที่ดีและเหมาะสมที่สุดแล้ว ทีมงานจึงเริ่มวางแผนดำเนินงานโครงการ โดยศึกษาความเป็นไปได้ กำหนดระยะเวลาดำเนินงานแต่ละขั้นตอนและกิจกรรม ระยะของการวางแผนโครงการ จะประกอบด้วยกิจกรรมต่าง ๆ ดังนี้

๑) จัดตั้งทีมงาน
๒) กำหนดปัญหา
๓) ศึกษาความเป็นไปได้
๔) จัดทำตารางกำหนดเวลา
๕) ดำเนินการโครงการ

๑.๒ การกำหนดและวิเคราะห์ความต้องการ (Requirement & Analysis)

ศึกษาขั้นตอนการดำเนินการของระบบเดิมหรือระบบปัจจุบันเพื่อหาปัญหาที่เกิดขึ้น รวบรวมความต้องการในระบบใหม่ อาจมีการใช้เทคนิคในการเก็บรวบรวมข้อมูล เช่น การออกแบบสอบถาม การสัมภาษณ์ โดยการพัฒนาระบบใหม่ต้องมีการกำหนดความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่ แล้วนำความต้องการเหล่านั้นมาวิเคราะห์เพื่อแก้ปัญหาดังกล่าว ด้วยการใช้แบบจำลองต่าง ๆ ช่วยในการวิเคราะห์ ได้แก่ แบบจำลองขั้นตอนการทำงานของระบบ (Process Model) แบบจำลองข้อมูล (Data Model) เช่น แผนภาพกระแสข้อมูล (Data Flow Diagram) แผนภาพแสดงความสัมพันธ์ระหว่างข้อมูล (Entity Relationship Diagram) เป็นต้น ระยะของการกำหนดและวิเคราะห์ความต้องการ จะประกอบด้วยกิจกรรมต่าง ๆ ดังนี้

๑) วิเคราะห์ระบบงานเดิมหรือระบบปัจจุบัน
๒) รวบรวมความต้องการในด้านต่าง ๆ และนำมาสรุปเป็นข้อกำหนดที่ชัดเจน
๓) นำข้อกำหนดมาพัฒนาออกแบบเป็นระบบงานใหม่ โดยการพัฒนาระบบใหม่ต้องมีการกำหนดความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่
๔) สร้างแบบจำลองกระบวนการ ด้วยการวาดแผนภาพกระแสข้อมูล

๕) สร้างแบบจำลองข้อมูล ด้วยแผนภาพแสดงความสัมพันธ์ระหว่างข้อมูล (Entity Relationship Diagram)

๑.๓ การออกแบบระบบ (Design)

นำผลลัพธ์จากการกำหนดและวิเคราะห์ความต้องการมาออกแบบ สถาปัตยกรรมของระบบ ฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่าย ส่วนติดต่อผู้ใช้งาน (User Interface) รูปแบบรายงานการออกแบบฐานข้อมูล และการออกแบบระบบความปลอดภัยตามมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ได้กำหนดไว้

๑.๔ การพัฒนาระบบ (System Development)

การเลือกภาษาโปรแกรม เช่น PHP, JavaScript, Java ,ASP.NET Core, Node.js, Python, Ruby เป็นต้น ชุดคำสั่ง เครื่องมือ หรือโครงสร้าง เช่น Laravel, React, Angular, jQuery เป็นต้น ที่ทันสมัย หรือ Version ล่าสุด รวมถึงระบบฐานข้อมูลที่เหมาะสม คำนึงถึงความปลอดภัยของระบบและข้อมูล โดยกำหนดให้ระบบที่พัฒนาจะต้องมีการทำ Input Validation การป้องกัน Injection Attacks การตรวจสอบสิทธิ์ และการให้สิทธิ์ Authentication และAuthorization การใช้โปรโตคอล Secure Sockets Layer/Transport Layer Security (SSL/TLS) การใช้ Hashing และ Encryption ได้เป็นอย่างน้อย

การร่วมกันพัฒนาระบบในทีมงาน ใช้ Cloud Version Control ที่ช่วยให้ทีมนักพัฒนาซอฟต์แวร์สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ การจัดเก็บ Source Code บน Cloud ช่วยให้ทีมสามารถเก็บ Source code ของ Project ไว้บน Cloud ได้อย่างปลอดภัย สมาชิกในทีมสามารถเข้าถึงและแก้ไข Code ได้จากทุกที่ผ่านอินเตอร์เน็ต

การพัฒนาระบบต้องแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) การทดสอบ (Testing) และระบบที่ให้บริการจริง (Production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

๑.๕ การทดสอบระบบ (Testing)

ต้องมีการทดสอบการทำงานของระบบทั้ง ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และส่วนอื่น ๆ ที่เกี่ยวข้อง เพื่อแสดงว่าระบบสามารถทำงานได้ตรงตามความต้องการที่กำหนดไว้อย่างครบถ้วน ดังนี้

๑) มีการกำหนด Test Script Test Scenario หรือ Test Case

๒) ทดสอบการทำงานของแต่ระบบ (Unit Test)

๓) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (System Integration Test)

๔) ทดสอบความพร้อมใช้งานตามกระบวนการและความต้องการของผู้ใช้งาน (User Acceptance Test : UAT)

๕) ทดสอบความปลอดภัยของระบบ (Security Test) ตามมาตรฐานด้านความมั่นคงปลอดภัยที่กำหนดไว้

๖) ชุดข้อมูลที่ใช้ในการทดสอบระบบต้องใช้อย่างระมัดระวัง และมีการควบคุมและป้องกันข้อมูลรั่วไหล

๑.๖ การติดตั้งระบบและนำไปใช้ (Implementation)

ทำการติดตั้งซอฟต์แวร์ ฮาร์ดแวร์ และอุปกรณ์ที่เกี่ยวข้อง ที่ครบถ้วนสมบูรณ์ เพื่อนำระบบไปใช้และให้บริการจริง (Production) มีการแบ่งแยกบุคลากรที่มีหน้าที่โอนย้ายระบบขึ้นสู่ Production อย่างชัดเจน มีการจัดทำแผนย้อนกลับ (Roll Back Plan) หรือแผนสำรองฉุกเฉินกรณีเปลี่ยนแปลงไม่สำเร็จ

(Fail Back Plan) และมีการจัดทำคู่มือการใช้งานระบบ Infographic Clip Video สอนการใช้งาน รวมถึงคู่มือและเอกสารต่าง ๆ ในการพัฒนาระบบ Source Code และเครื่องมือต่าง ๆ ที่สมบูรณ์สามารถพัฒนาต่อได้

๑.๗ การบำรุงรักษา (Maintenance)

หลังจากระบบถูกนำไปใช้งาน จะต้องมีการบำรุงรักษาให้ระบบสามารถใช้งานได้เป็นปกติ ผู้ใช้อาจจะพบกับปัญหาที่เกิดขึ้น ผู้ดูแลระบบทำหน้าที่บันทึกและรวบรมปัญหา นำไปสู่การปรับปรุงเปลี่ยนแปลงระบบใหม่ ตามวงจรชีวิตการพัฒนาซอฟต์แวร์

๒. การควบคุมการเปลี่ยนแปลงหรือ แก้ไขระบบสารสนเทศ

การเปลี่ยนแปลงระบบงาน (Change Management) ต้องมีการควบคุมไม่ให้มีผลกระทบกับระบบงาน ระบบเครือข่าย ทั้ง การพัฒนาระบบ หรือการทดสอบระบบ การเปลี่ยนแปลงแก้ไขควรมีคำขอเปลี่ยนแปลงอย่างเป็นทางการ โดยมีแนวปฏิบัติ ดังนี้

๒.๑ การร้องขอเปลี่ยนแปลง ต้องจัดทำตามแบบฟอร์มขอเปลี่ยนแปลง (Request for Change) ที่กำหนดไว้โดยประกอบด้วย ๕ ส่วนหลัก ดังนี้

๑) การขอเปลี่ยนแปลง (Request for Change)

๒) การวิเคราะห์ผลกระทบ (Impact Analysis)

๓) การอนุมัติ/ไม่อนุมัติ (Approve/Deny)

๔) การดำเนินการเปลี่ยนแปลง (Implement Change)

๕) การตรวจสอบ/การรายงาน (Review/Reporting)

๒.๒ กำหนดประเภทการเปลี่ยนแปลงระบบตามความเสี่ยงและความสำคัญ ดังนี้

๑) การเปลี่ยนแปลงมาตรฐาน (Standard Change) สำหรับการเปลี่ยนแปลงที่เกิดขึ้นซ้ำ ๆ ความเสี่ยงต่ำ ได้รับอนุญาตไว้ล่วงหน้า เช่น การปรับปรุงโปรแกรมป้องกันไวรัสเป็นประจำ การขอรหัสผ่านใหม่

๒) การเปลี่ยนแปลงปกติ (Normal Change) เป็นรูปแบบการเปลี่ยนแปลงที่เกิดขึ้นมากที่สุด จะต้องผ่านขั้นตอนที่กำหนดไว้แน่นอนล่วงหน้าก่อนการดำเนินการ ต้องได้รับการอนุมัติ เช่น การเพิ่มฟีเจอร์ (Feature) ให้กับแอพพลิเคชันหรือการอัพเดทแพตช์ (Patch) ที่สำคัญของเครื่องคอมพิวเตอร์แม่ข่าย

๓) การเปลี่ยนแปลงฉุกเฉิน (Emergency Change) ใช้เมื่อจำเป็นต้องทำการเปลี่ยนแปลงที่สำคัญภายในระยะเวลาอันสั้นเพื่อเรียกคืนบริการหรือส่วนประกอบใด ๆ ที่ล้มเหลวโดยทั่วไปแล้วคำขอการเปลี่ยนแปลงประเภทนี้จะถูกยกมาจากการจัดการเหตุการณ์ (Incident Management) หรือกระบวนการจัดการปัญหา (Problem Management) เช่น การเปลี่ยนส่วนประกอบที่ผิดพลาดของเครื่องแม่ข่าย (Server) ที่สำคัญหรือการสร้างระบบที่ล้มเหลวขึ้นมาใหม่

๔) คำขอการเปลี่ยนแปลง (Change Request) ควรได้รับการ อนุมัติจากหน่วยงานเจ้าของระบบ (System Owner)หรือหน่วยงานที่เกี่ยวข้อง ก่อน และต้องได้รับอนุญาตก่อน เพื่อให้ มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็น อย่างเหมาะสม

๕) การเปลี่ยนแปลงระบบงานต้องไม่กระทบหรือขัดขวางการทำงานของ ระบบปัจจุบันและการเปลี่ยนแปลงดังกล่าวต้องสามารถใช้งานร่วมกับข้อมูลและระบบงานใช้อยู่ได้

๖) การจัดทำทะเบียนหรือระบบในการจัดเก็บคำขอเปลี่ยนแปลง และเอกสารรายละเอียดที่เกี่ยวข้องเพื่อใช้ควบคุมการปฏิบัติงาน ตั้งแต่ต้นจนจบกระบวนการ

๗) การประเมินผลกระทบการเปลี่ยนแปลงที่อาจกระทบกับโปรแกรม หรือระบบอื่น

๘) การทดสอบการเปลี่ยนแปลงโดยผู้ใช้งาน (User Acceptance Test: UAT) และการลงนามรับรอง (Sign Off)

๙) มีแผนย้อนกลับ (Roll Back Plan) กรณีเปลี่ยนแปลงไม่สำเร็จ (Fall Back Plan)

๑๐) การควบคุมเวอร์ชั่นการเปลี่ยนแปลง

๑๑) การปรับปรุงเอกสารที่เกี่ยวข้องให้สอดคล้องกับการเปลี่ยนแปลง

๑๒) การเปลี่ยนแปลงข้อมูลต้องไม่แก้ไขจากฐานข้อมูลโดยตรง แต่ ต้องดำเนินการผ่านหน้าจอโปรแกรม กรณีไม่สามารถแก้ไขผ่าน หน้าจอโปรแกรม ต้องทำเป็นสคริปต์ (Script) เพื่อให้สามารถตรวจสอบย้อนกลับในภายหลังได้กรณีพบปัญหาจากการแก้ไข เปลี่ยนแปลง

๑๓) แบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (Development) การทดสอบ (Testing) และระบบที่ให้บริการจริง (Production) ออกจากกัน เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นจากการนำระบบขึ้นใช้งานจริง

๑๔) ผู้ดูแลระบบต้องบันทึกข้อมูลของระบบเก่าเก็บไว้เพื่อใช้แก้ปัญหา

๑๕) ผู้ดูแลระบบจะต้องเก็บค่า Config ต่าง ๆ ของระบบเก่าเก็บไว้บัญชีผู้ใช้งานและรหัสผ่าน

๑๖) การเปลี่ยนแปลง Source Code ของระบบ ต้องมีการควบคุม Version ของ Source Code อย่างเคร่งครัด

๓. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

๓.๑ ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งให้สิทธิ์ตามอำนาจหน้าที่ที่ควรได้รับ

๓.๒ ผู้ดูแลระบบต้องจัดให้มีการทบทวนสิทธิ์การใช้งานอย่างสม่ำเสมอ

๓.๓ ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อให้กับระบบงาน และหากมีการว่างเว้นจากการใช้งานเกินระยะเวลา ๑๕ นาที ให้ทำการยุติการใช้งานทันที

๓.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒) กำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล และห้ามมิให้ใช้รายชื่อผู้ใช้และรหัสผ่านชุดเดียวกันในชั้นความลับของข้อมูล

๓) ให้มีการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดตามระดับความสำคัญของข้อมูล

๔) กำหนดให้มีการรับส่งข้อมูลที่มีการเข้ารหัส SSL VPN เมื่อมีการใช้งานผ่านเครือข่ายสาธารณะ

๕) การนำคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงานต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

๖) การเข้าถึงเครือข่ายของผู้ปฏิบัติงานชั่วคราวให้ทำการลงทะเบียนและได้รับสิทธิ์เป็นการชั่วคราวตามระยะเวลาการปฏิบัติงาน หากพ้นจากช่วงเวลาดังกล่าวให้ระงับสิทธิ์ในการเข้าถึง และต้องทำการลงทะเบียนเพื่อรับสิทธิ์ในการเข้าถึงใหม่ทุกครั้ง

๔. การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๔.๑ ข้อกำหนดด้านความมั่นคงปลอดภัยหรือมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของระบบสารสนเทศต้องครอบคลุมอย่างน้อยตามที่กฎหมายกำหนด มีการอนุมัติ และประกาศใช้อย่างเป็นทางการ

๔.๒ การพัฒนา หรือเปลี่ยนแปลงระบบสารสนเทศให้ใช้ข้อกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๑) สิทธิ์พิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- ให้สิทธิ์การเข้าถึงระบบ ข้อมูล หรือทรัพยากรเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น
- ผู้ใช้งานควรได้รับสิทธิ์ขั้นต่ำที่จำเป็นในการทำงานของตน
- ช่วยลดความเสี่ยงจากการใช้สิทธิ์เกินความจำเป็นที่อาจก่อให้เกิดความเสียหาย

๒) การแบ่งแยกหน้าที่ (Separation of Duties)
- การกระจายความรับผิดชอบในงานสำคัญให้แก่บุคคลหลายคน
- ป้องกันการรวมศูนย์อำนาจที่อาจนำไปสู่การทุจริตหรือความผิดพลาด
- เช่น แยกผู้อนุมัติรายการกับผู้ปฏิบัติงาน หรือแยกผู้พัฒนาระบบกับผู้ดูแลระบบ

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- กำหนดมาตรฐานรหัสผ่านที่มีความปลอดภัย
- ควรประกอบด้วย : ตัวอักษรพิมพ์ใหญ่, พิมพ์เล็ก, ตัวเลข, อักขระพิเศษ
- กำหนดความยาวขั้นต่ำ และอายุการใช้งานของรหัสผ่าน
- ห้ามใช้รหัสผ่านซ้ำกับรหัสผ่านเดิม

๔) การลบบัญชีที่ไม่ได้ใช้
- ตรวจสอบและลบบัญชีผู้ใช้ที่ไม่มีการใช้งานเป็นระยะเวลานาน
- ลบบัญชีของพนักงานที่ลาออกหรือเปลี่ยนตำแหน่ง
- กำหนดระยะเวลาการไม่ใช้งานที่จะนำไปสู่การระงับหรือลบบัญชี

๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น
- ลบโปรแกรมหรือบริการที่ไม่จำเป็นต่อการทำงาน
- ลบคอมไพเลอร์ที่อาจถูกใช้ในการสร้างโปรแกรมที่เป็นอันตราย
- ลบแอปพลิเคชันสนับสนุนของผู้ให้บริการที่ไม่ได้ใช้งาน
- ลดความเสี่ยงจากช่องโหว่ของโปรแกรมที่ไม่จำเป็น

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- ปิดพอร์ตการสื่อสารทั้งหมดที่ไม่จำเป็น
- เปิดเฉพาะพอร์ตที่จำเป็นสำหรับการให้บริการ
- ตรวจสอบและปิดพอร์ตที่ไม่ได้ใช้งานอย่างสม่ำเสมอ

๗) การป้องกันมัลแวร์ (Malware)
- ติดตั้งโปรแกรมป้องกันไวรัสและมัลแวร์
- อัพเดทฐานข้อมูลไวรัสอย่างสม่ำเสมอ
- ตั้งค่าการสแกนระบบอัตโนมัติ
- กำหนดนโยบายการจัดการเมื่อตรวจพบมัลแวร์

๘) การปรับปรุงซอฟต์แวร์และแพตช์ความมั่นคงปลอดภัย

- ติดตามการออกแพตช์ความปลอดภัยของซอฟต์แวร์
- ทดสอบแพตช์ก่อนติดตั้งในระบบจริง
- กำหนดกระบวนการติดตั้งแพตช์อย่างเป็นระบบ
- จัดทำแผนสำรองกรณีการติดตั้งแพตช์มีปัญหา

๕. มีการทบทวนข้อกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย Security Baseline Configuration Standards อย่างน้อยปีละ 1 ครั้ง

๖. การคัดเลือกผู้ให้บริการ และการควบคุมการเข้าถึงระบบของผู้ให้บริการภายนอก (Outsource)

๖.๑ การคัดเลือกผู้ให้บริการ

๑) ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุม และเป็นที่น่าเชื่อถือ

๒) ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) ตามภาคผนวก ก (เอกสารแนบ ๑ (แบบฟอร์ม NDA)) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

๖.๒) การควบคุมผู้ให้บริการ

๑) ควรมีการกำหนดสิทธิ์ให้สิทธิ์การเข้าถึงระบบของผู้ให้บริการภายนอก (Outsource) ตามหน้าที่ที่ควรได้รับ

๒) ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๓) ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข

๔) ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

๖.๓) กรณีมีการจ้างบำรุงรักษาระบบสารสนเทศ ให้ระบุเงื่อนไขของสัญญากับผู้ให้บริการภายนอก หรือข้อตกลงระดับการให้บริการ (Service Level Agreement) ให้มีการรายงานติดตามผลการใช้ทรัพยากรสารสนเทศของระบบที่บำรุงรักษา (ตามภาคผนวก ข) (ตารางจัดเก็บค่าการใช้งานเครื่องแม่ข่าย)

๖.๔) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญา กับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อยดังต่อไปนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงาน ของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์

(๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(๔) สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๖.๕ มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ใช้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน

๖.๖ สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของ หน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ควรมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง

๗. การจัดการระบบซึ่งไวต่อการรบกวน

๗.๑ ผู้ดูแลระบบต้องจัดให้ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมทางหลวง ได้รับการติดตั้งแยกออกจากระบบงานอื่น มีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ได้แก่ ระบบปรับอากาศ ระบบสำรองไฟ

๗.๒ ผู้ดูแลระบบต้องจัดให้ระบบซึ่งไวต่อการรบกวนมีช่องทางการเชื่อมต่อของตนเองโดยเฉพาะ หรือหากมีการใช้ช่องสัญญาณร่วมกันต้องมีการประกันคุณภาพของสัญญาณ (QoS) สำหรับระบบนั้น ๆ

๗.๓ ผู้ดูแลระบบต้องมีการจัดให้ระบบซึ่งไวต่อการรบกวนมีห้องปฏิบัติการแยกเป็นสัดส่วนและจำกัดผู้เข้าออกเฉพาะผู้มีหน้าที่รับผิดชอบเท่านั้น

๘. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๘.๑ การใช้งานทั่วไป

๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบโปรแกรมไม่ประสงค์ดี โดยโปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี

๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

๗) ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๙) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการระทบกระเทือน ได้แก่ การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๑๐) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๑) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง ได้แก่ ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๒) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑๓) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๔) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น ได้แก่อาหาร น้ำกาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๑๕) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล๊อคเครื่องขณะที่ไม่ได้ใช้งานไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๖) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๘.๒ การสำรองข้อมูลและการกู้คืน

๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD, DVD, External Hard Disk เป็นต้น

๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการ ของหน่วยงาน

๙. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑) ผู้ใช้ที่ต้องการปฏิบัติงานจากภายนอกสำนักงานต้องทำการลงทะเบียนเพื่อขอบัญชีผู้ใช้และรหัสผ่านสำหรับเชื่อมต่อจากภายนอก

๒) ผู้ดูแลระบบทำการสร้างบัญชีผู้ใช้งานสำหรับการเชื่อมต่อจากภายนอกสำนักงาน โดยบัญชีผู้ใช้และรหัสผ่านต้องไม่เป็นบัญชีผู้ใช้หรือรหัสผ่านชุดเดียวกับบัญชีผู้ใช้และรหัสผ่านที่ใช้ในสำนักงาน

๓) ผู้ดูแลระบบต้องกำหนดชนิดของงานที่อนุญาต และไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ที่อนุญาตให้ใช้งาน

๔) ผู้ดูแลระบบต้องกำหนดช่วงเวลาที่สามารถใช้งานได้คือช่วงเวลาราชการ

๕) กำหนดให้มีช่องทางเชื่อมต่อแบบ (SSL VPN) ในการเชื่อมต่อจากภายนอกสำนักงาน

๖) ต้องมีกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบสารสนเทศและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ส่วนที่ ๘
การใช้งานอินเทอร์เน็ต (Use of Internet)

วัตถุประสงค์

เพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย

แนวปฏิบัติ

๑. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๓. การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๔. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของกรมทางหลวง เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ ของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับกรมทางหลวง

๕. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมทางหลวง ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๖. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๘. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

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

๑๐. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๙
การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic mail)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานจดหมายอิเล็กทรอนิกส์ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์ผู้ใช้จะต้องเข้าใจนโยบายและแนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ที่ศูนย์เทคโนโลยีสารสนเทศได้ประกาศไว้ไม่ละเมิดสิทธิ์กระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพนโยบายและแนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบฯ อย่างเคร่งครัดจึงจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติ

๑. การใช้งานจดหมายอิเล็กทรอนิกส์

๑.๑ ผู้ใช้มีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบและไม่อนุญาตให้ผู้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี

๑.๒ ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๑.๓ ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์จากการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเองและจากการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้อื่น

๑.๔ ผู้ดูแลระบบไม่มีสิทธิ์ที่จะถามหรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

๑.๕ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ในงานตามภารกิจของหน่วยงานเพื่อติดต่องานของราชการเท่านั้นและห้ามมิให้ใช้จดหมายอิเล็กทรอนิกส์อื่นเว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์กรมทางหลวงขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๑.๖ การใช้จดหมายอิเล็กทรอนิกส์ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

๑) ผู้ใช้งานต้องไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อประกอบธุรกิจส่วนตัวหรือของบุคคลอื่น

๒) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่จดหมายลูกโซ่

๓) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อมูลชั้นความลับของหน่วยงานและไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๔) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารหรือในการประชุมอื่น ๆ โดยที่มิได้มีหน้าที่หรือมิได้รับมอบหมายจากประธานในที่ประชุม

๕) ผู้ใช้งานต้องไม่ทำการปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้น ๆ ส่งมาจากบุคคลอื่น

๖) ผู้ใช้งานต้องไม่ทำการปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ให้ทราบชื่อผู้ส่ง

๗) ผู้ใช้งานต้องไม่ทำการปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทางวันเวลาการส่ง

๘) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อความภาพวีดิโอเสียงที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

๙) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อความภาพวีดิโอเสียงที่ดูหมิ่นเหยียดหยามหรือแบ่งแยกทางศาสนาเชื้อชาติหรือเพศ

๑๐) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อความภาพวีดิโอเสียงที่มีลักษณะหยาบคายหรือลามกอนาจาร

๑๑) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่โปรแกรมหรืองานหรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองานในลักษณะที่ละเมิดลิขสิทธิ์

๑๒) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคมการเมืองศาสนาไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

๑๓) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์โฆษณาสินค้าผลิตภัณฑ์หรือส่งข้อความลักษณะของสแปมเมล (Spam Mail) ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

๑๔) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ซึ่งส่งผลกระทบให้ระบบจดหมายอิเล็กทรอนิกส์หรือเครือข่ายลดทอนประสิทธิภาพลง

๑๕) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์กระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

๑๖) ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๗) ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดและตรวจสอบไฟล์แนบโดยใช้โปรแกรมป้องกัน

๑๘) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์เผยแพร่ข้อมูลข้อความรูปภาพหรือสิ่งอื่นใดที่มีเนื้อหาขัดต่อจริยธรรมปลุกปั่นยั่วยุเสียดสีส่อไปในทางผิดกฎหมายข้อมูลอันเป็นเท็จที่กระทบความมั่นคงของประเทศหรือกระทบต่อการดำเนินงานของหน่วยงาน

๑๙) ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ที่เป็นความเห็นส่วนบุคคลโดยอ้างว่าเป็นความเห็นของหน่วยงานหรือก่อให้เกิดความเสียหายต่อหน่วยงาน

๒๐) ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมหรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงานทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางระบบจดหมายอิเล็กทรอนิกส์

๒. การระงับบัญชีจดหมายอิเล็กทรอนิกส์

กรมทางหลวงขอสงวนสิทธิ์ซึ่งอำนาจในการจำกัด ระงับหรือเพิกถอนสิทธิ์การใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา

ความมั่นคงปลอดภัยหรือเสถียรภาพของระบบเครือข่าย หรือระบบจดหมายอิเล็กทรอนิกส์ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐการระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์มีแนวทางปฏิบัติดังนี้

๒.๑ เมื่อผู้ใช้พ้นสภาพการอยู่ในสังกัดของกรมทางหลวงศูนย์เทคโนโลยีสารสนเทศสามารถระงับบัญชีผู้ใช้ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย

๒.๒ บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบให้ประสิทธิภาพระบบเครือข่ายด้อยลงหรือขัดต่อนโยบายไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่นทั้งนี้ศูนย์เทคโนโลยีสารสนเทศมีสิทธิ์ระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

๒.๓ กรณีผู้ใช้ไม่ได้เข้าสู่บัญชีจดหมายอิเล็กทรอนิกส์ภายในระยะเวลา ๖ เดือน ผู้ดูแลระบบขอสงวนสิทธิ์ในการระงับสิทธิ์การใช้งานจดหมายอิเล็กทรอนิกส์บัญชีนั้น

๓. การใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ใช้งาน (User)

๓.๑ ผู้ใช้งานที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลคำขอใช้งานจดหมายอิเล็กทรอนิกส์ผ่านช่องทางออนไลน์พร้อมให้หัวหน้าหน่วยงานระดับผู้อำนวยการหรือเทียบเท่าลงนามด้วยวิธีทางอิเล็กทรอนิกส์เพื่อรับรองข้อมูลของผู้ขอใช้งานและยื่นคำขอมาที่ศูนย์เทคโนโลยีสารสนเทศทาง E-mail เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password) ต่อไป

๓.๒ เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันทีหลังจากการเข้าสู่ระบบเป็นครั้งแรก

๓.๓ ควรกำหนดรหัสผ่านที่ยากต่อการคาดเดาให้มีตัวอักษรไม่น้อยกว่า ๘ ตัวอักษรโดยมีการผสมกันระหว่างตัวอักษรภาษาอังกฤษที่เป็นตัวพิมพ์ใหญ่ตัวพิมพ์เล็กและตัวเลขเข้าด้วยกัน

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 ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันเพื่อลดปริมาณการใช้พื้นที่ของระบบจดหมายอิเล็กทรอนิกส์ให้เหลือจำนวนน้อยที่สุด

๓.๙ ไม่ควรเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในกล่องขาเข้าสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังไว้ที่เครื่องคอมพิวเตอร์ของตนเสียหายที่อาจเกิดจากระบบจดหมายอิเล็กทรอนิกส์

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 กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้และหน้าที่ความรับผิดชอบของผู้ใช้งาน

๔.๒ มีการทบทวนสิทธิ์การเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งานปีละ ๒ ครั้ง (ทุกเดือนเมษายน และตุลาคม) หรือเมื่อมีการเปลี่ยนแปลงเช่นเกษียณอายุราชการการลาออกโอนย้ายหรือพ้นสภาพการอยู่ในสังกัดของกรมทางหลวงเป็นต้น

๔.๓ มีการควบคุมการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ตามนโยบายการใช้งานจดหมายอิเล็กทรอนิกส์กรมทางหลวงที่ได้กำหนดไว้อย่างเคร่งครัด

ส่วนที่ ๑๐
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการการป้องกันบุคคลภายนอกจากการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต กับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ข้อมูลและสารสนเทศที่เป็นทรัพย์สินของกรมทางหลวง ซึ่งอาจก่อให้เกิดความเสียหายและทำการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศของกรมทางหลวง ส่งผลกระทบต่อการปฏิบัติภารกิจด้านความมั่นคงปลอดภัยสารสนเทศ ทำให้ไม่สามารถปฏิบัติภารกิจได้อย่างต่อเนื่อง และมีประสิทธิภาพ

แนวปฏิบัติ

๑. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

๑.๑ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารโดยกำหนดพื้นที่ปฏิบัติงาน พื้นที่ควบคุมเฉพาะให้ชัดเจน พื้นที่จัดเก็บอุปกรณ์ต่าง ๆ พื้นที่เก็บเอกสารสื่อบันทึกข้อมูล เป็นต้น และจัดทำแผนผังแสดงตำแหน่งพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน

๑.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์และลำดับชั้นในการเข้าถึงพื้นที่ใช้งานข้อมูลระบบสารสนเทศ ระบบเครือข่ายสื่อสาร

๑.๓ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า - ออกพื้นที่ของศูนย์ฯทั้งหมด และกำหนดพื้นที่ที่มีความเสี่ยง ห้ามบุคคลภายนอกหรือผู้มีส่วนเกี่ยวข้องเข้าถึงได้ ดังนี้

๑) ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

- กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี
- ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า – ออก ของบุคคลเป็นจำนวนมาก
- จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว
- จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่าง หรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่
- หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสารให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว
- ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด
- จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๒) การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

- มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๓) การควบคุมการเข้าออก อาคารสถานที่

- กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า - ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

- การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตร ประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและ รับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

- ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

- ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

- บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

- จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

- ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับ อนุญาต

- มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

- สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

- มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

- ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

- มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า –ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

- จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

- จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

๑.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑.๕ จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งานดังนี้

๑) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

๒) ติดตั้ง ระบบน้ำ และเครื่องดับเพลิง

๓) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

๔) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๕) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

๒. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงให้ติดตั้งระบบป้องกันที่ปลอดภัย

๒.๒ ให้มีการร้อยท่อสายสัญญาณ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒.๔ ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๒.๕ จัดทำแผนผังสายสัญญาณสื่อสาร ให้ครบถ้วนและถูกต้อง

๒.๖ ห้องที่มีสายสัญญาณสื่อสาร ให้ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่นสายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๓. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๓.๑ วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

๓.๒ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๓.๓ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๓.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ทุกครั้ง

๓.๕ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๔.๑ ต้องขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอกหรือนำไปซ่อมบำรุงภายนอก

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 เป็นผู้อนุมัติในการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

๖.๒ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

๗. การควบคุมอุปกรณ์แบบพกพา หรือ สื่อบันทึกข้อมูลที่ถอดแยกได้

๗.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยก/เคลื่อนย้ายได้ (Management of Removable Media)

๑) ให้เจ้าของระบบสารสนเทศเป็นผู้พิจารณาอนุญาตให้ใช้งานสื่อบันทึกข้อมูลที่ถอดแยกได้บนเครื่องคอมพิวเตอร์ที่ตนดูแลรับผิดชอบ

๒) ในกรณีที่เจ้าของระบบสารสนเทศอนุญาตให้ใช้งานสื่อบันทึกข้อมูลที่ถอดแยกได้ก่อนการใช้งานต้องได้รับการสแกนไวรัสจากโปรแกรมป้องกันไวรัสที่ได้รับการอัพเดทอยู่เสมอ

๓) ห้ามใช้งานสื่อบันทึกข้อมูลที่ถอดแยกได้ที่ไม่สามารถระบุเจ้าของหรือแหล่งที่มาได้และให้ส่งมอบแก่ผู้ดูแลระบบสารสนเทศเพื่อทำการตรวจสอบความมั่นคงปลอดภัย

๒. การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

๒.๑ ผู้ดูแลระบบ/เจ้าของข้อมูลเป็นผู้ทำลายข้อมูลที่เป็นความลับ หรือ มีสำคัญ ที่บันทึกในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบ หรือ เขียนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนาอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันการรั่วไหลของข้อมูล หรือป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ให้ทำลายด้วยเครื่องทำลายเอกสาร
Flash Drive/Memory Stick/Memory Card	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบ หรือ บดให้เสียหาย
แผ่น CD/DVD	- ให้ทำลายด้วยเครื่องทำลายแผ่น CD/DVD
เทป	- ให้ทุบ หรือ บดให้เสียหาย หรือ เผาทาลาย
ฮาร์ดดิสก์	- ให้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบ หรือ บดให้เสียหาย

๒.๒ กรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพรวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่

๒.๓ เจ้าของข้อมูลต้องจัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูล และสื่อบรรทุกข้อมูลสำคัญและมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๒.๔ เจ้าของข้อมูลต้องจัดทำบันทึกรายละเอียดการปฏิบัติงานในการทำลายข้อมูล เพื่อให้สามารถตรวจสอบได้ภายหลัง

๓. การขนย้ายสื่อบันทึก (Physical Media Transfer)

๓.๑ ผู้ที่มีหน้าที่ให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการ จะต้องดูแลรักษาความปลอดภัย จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือทำให้เสียหายระหว่างการขนย้าย

๓.๒ ผู้ที่มีหน้าที่ให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการ ต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าของทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ที่มีหน้าที่ให้เคลื่อนย้ายสื่อบันทึก

ส่วนที่ ๑๑
ระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อให้กรมทางหลวงมีแนวทางปฏิบัติหรือมาตรการในการจัดทำระบบสำรองข้อมูล (Backup System) และแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อป้องกันข้อมูลสูญหายเพิ่มความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศ ของกรมทางหลวง ในกรณีฉุกเฉินหรือสถานการณ์ ไม่ปกติหรือมีภัยพิบัติเกิดขึ้น และสามารถกู้คืนระบบสารสนเทศ ภายในระยะเวลาที่เหมาะสม

แนวปฏิบัติ

๑. การสำรองข้อมูล

๑.๑ ศูนย์เทคโนโลยีสารสนเทศต้องทำการคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑.๒ จัดทำบัญชีระบบสารสนเทศทั้งหมดที่มีความสำคัญของกรมทางหลวง พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง

๑.๓ มีการวางแผนสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ กำหนดชนิดการสำรองข้อมูล สื่อบันทึกที่ใช้ในการสำรองข้อมูลตามความเหมาะสม ช่วงเวลาในการสำรองข้อมูลโดยพิจารณาจากความสำคัญของข้อมูล ความถี่ในการเปลี่ยนแปลงข้อมูล

๑.๔ ผู้ดูแลระบบต้องทำการบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่สำรอง สื่อบันทึกที่ได้สำรองข้อมูล โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย

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

๑.๖ หากเกิดข้อผิดพลาดในการสำรองข้อมูล ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูล รวมทั้งวิธีการแก้ไข

๑.๗ ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

๑.๘ ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยเลือกใช้วิธีการที่เหมาะสม เพื่อป้องกันการรั่วไหลของข้อมูล

๑.๙ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติต่าง ๆ

๑.๑๐ ให้มีการมอบหมายเจ้าหน้าที่สำรองในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๑.๑๑ ผู้ดูแลระบบต้องมีการสำรองข้อมูลและทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอเพื่อตรวจสอบว่ายังสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้และให้เป็นไปตามนโยบายการสำรองข้อมูล ของกรมทางหลวง

๒. การกู้คืนระบบ

๒.๑ ผู้ดูแลระบบต้องทำการบันทึกการกู้คืนระบบทุกครั้งที่มีการกู้คืนระบบ แล้วรายงานให้ผู้บังคับบัญชาทราบ

๒.๒ ผู้ดูแลระบบต้องทำการแก้ไขหากเกิดปัญหารวมถึงรายงานผู้บังคับบัญชาถึงปัญหาและวิธีการแก้ไขในการกู้คืนระบบ

๒.๓ ผู้ดูแลระบบต้องทำการกู้คืนระบบโดยใช้ข้อมูลสำรองที่ทันสมัยที่สุดที่ได้สำรองไว้

๒.๔ ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยระบบละ ๑ ครั้งต่อปี

๓. แผนเตรียมพร้อมกรณีฉุกเฉิน

ให้ศูนย์เทคโนโลยีสารสนเทศจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และแผนเตรียมความพร้อมในกรณีที่ไม่สามารถดำเนินการได้ด้วยวิธีการทางอิเล็กทรอนิกส์ และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวปีละ ๑ ครั้ง โดยมีรายละเอียดอย่างน้อย ดังนี้

๓.๑ ศูนย์เทคโนโลยีสารสนเทศต้องมีการกำหนดให้มีกระบวนการรับมือสำหรับกรณีฉุกเฉิน และแผนฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ได้

๓.๒ ศูนย์เทคโนโลยีสารสนเทศต้องมีการกำหนดชนิดของภัยพิบัติที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ

๓.๓ ศูนย์เทคโนโลยีสารสนเทศต้องมีการประเมินความเสี่ยงที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ทำให้ไม่สามารถเข้าใช้งานระบบสารสนเทศได้

๓.๔ กำหนดขั้นตอนปฏิบัติในกู้คืนระบบ และการทดสอบแผนฉุกเฉิน

๓.๕ กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในหน่วยงานและผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ

๓.๖ สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๓.๗ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓.๘ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

๓.๙ ศูนย์เทคโนโลยีสารสนเทศต้องจัดให้มีการซักซ้อม และทบทวนแผนเตรียมพร้อมในกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๔. การกำหนดหน้าที่ความรับผิดชอบ

๔.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer: DCIO)

๑) กำกับดูแลให้เจ้าหน้าที่ทุกหน่วยงานในกรมทางหลวงปฏิบัติตามนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศอย่างถูกต้อง เพื่อให้มั่นใจได้ว่าการใช้ระบบสารสนเทศมีความมั่นคงปลอดภัย

๒) ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศในฐานะประธานศูนย์ฯ

๓) เป็นผู้รับผิดชอบในการทบทวนนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศ

๔.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒) มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๓) มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

๔) ประชุมหารือกับผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่ายและคณะกรรมการอื่นที่เกี่ยวข้องในการจัดการกรณีฉุกเฉิน

๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯตามความเหมาะสม

๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ทราบ

๔.๓ ผู้อำนวยการกลุ่มบริหารคอมพิวเตอร์และเครือข่าย

๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ จะมาถึงที่เกิดเหตุ

๓) ดำเนินการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

๔) ทำหน้าที่แทนผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศตามที่ได้รับมอบหมาย หรือขณะที่ท่านผู้อำนวยการศูนย์สารสนเทศไม่อยู่

๕) ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง ได้แก่ ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

๖) รายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

๗) กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

๘) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔.๔ ผู้ดูแลระบบเครือข่าย

๑) หากมีเหตุการณ์ฉุกเฉินหลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้บังคับบัญชาทราบ

๒) เตรียมพร้อมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบหากเกิดเหตุการณ์ฉุกเฉิน

๓) ทำการเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหาก จากห้องควบคุมระบบ โปรแกรมและแฟ้มข้อมูล, Tape backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

๔) ทำการสำรองข้อมูลตามแผนการสำรองข้อมูล

ส่วนที่ ๑๒
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Information Security Audit and Assessment)

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ กรมทางหลวง จึงจัดให้มีระบบบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศขึ้น 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) เพื่อให้กรมทางหลวง ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีการทดสอบเจาะระบบ (Penetration Testing) ประกอบด้วย

๒.๑ การทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology : IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับความเสี่ยง และพิจารณาผลกระทบ หรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๒.๒ การทดสอบเจาะระบบต้องดำเนินการโดยผู้ทดสอบเจาะระบบ (Penetration Testers) ภายในองค์กร หรือผู้ทดสอบเจาะระบบอิสระ ที่มีคุณสมบัติเป็นผู้ทดสอบเจาะระบบตามที่กฎหมายกำหนด

๓. กำหนดแนวทางในการประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อยดังนี้

๓.๑ ระบุความเสี่ยง สาเหตุของความเสี่ยงและผลกระทบที่เกิดขึ้นจากความเสี่ยง

๓.๒ จัดลำดับความสำคัญของความเสี่ยง

๓.๓ จัดทำมาตรการในการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน และมาตรการในภาวะฉุกเฉิน

๓.๔ ให้จัดทำรายงานการควบคุมความเสี่ยงประจำปี

๓.๕ หากมีความเสี่ยงที่เกิดขึ้นใหม่ ให้มีการจัดทำรายงานและวิเคราะห์การแก้ไขความเสี่ยงเพื่อไม่ให้เกิดขึ้นซ้ำอีก เป็นการดำเนินการต่อเนื่องว่าแผนบริหารความเสี่ยงมีความเหมาะสมกับสถานการณ์ที่มีการเปลี่ยนแปลงไปหรือไม่ รวมถึงทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอนและพัฒนาระบบให้ดียิ่งขึ้น

๓.๖ ให้มีการทบทวนประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๔. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๔.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อค (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๑๓
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 หรือผู้หนึ่งผู้ใดอัน เนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Department Chief Information Officer : DCIO) กรมทางหลวง เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแลและควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศของกรมทางหลวง ผู้รับผิดชอบ ดังนี้

๑) กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูล และเทคโนโลยีสารสนเทศ

๒) ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๓) วางแผน จัดทำ ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

๒. ระดับปฏิบัติงาน

ระดับปฏิบัติงาน ประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจ ดังนี้

๒.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ ดังนี้

๑) ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและ ภัยพิบัติ

๓) ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ระบบเครือข่ายระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๖) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมทางหลวง

๒.๒ ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด

ภาคผนวก
เอกสาร/แบบฟอร์ม ที่เกี่ยวข้อง

กรมทางหลวง
สัญญารักษาความลับของข้อมูล (NDA)

สัญญาฉบับนี้ทำขึ้น.....และมีผลบังคับใช้ เมื่อวันที่.....

ระหว่าง :

๑. **กรมทางหลวง** ตั้งอยู่ ณ ๒/๔๘๖ ถนนศรีอยุธยา แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐ ซึ่งต่อไปนี้ในสัญญาฉบับนี้เรียกว่า “ผู้ว่าจ้าง” ฝ่ายหนึ่ง กับ

๒. ..... ตั้งอยู่ ณ ..... ซึ่งต่อไปในสัญญาฉบับนี้ เรียกว่า “.....” หรือ “ผู้รับจ้าง” อีกฝ่ายหนึ่ง

คู่สัญญาทั้งสองฝ่ายตกลงกันข้อความดังต่อไปนี้

๑. วัตถุประสงค์

โดยที่กรมทางหลวงได้ติดต่อ และ /หรือ ว่าจ้าง บริษัทฯ เพื่อ .....นั่น คู่สัญญาแต่ละฝ่ายอาจมีความจำเป็นต้องเปิดเผยข้อมูลที่เป็นความลับของตนอันเกี่ยวข้องกับการดำเนินงาน ตามวัตุประสงค์ ให้แก่คู่สัญญาฝ่ายหนึ่ง โดยคู่สัญญาฝ่ายผู้ให้ข้อมูลประสงค์ให้คู่สัญญาฝ่ายผู้รับข้อมูล เก็บรักษาข้อมูลดังกล่าวไว้เป็นความลับ

๒. “ข้อมูลที่เป็นความลับ”

“ข้อมูลที่เป็นความลับ” หมายความถึง ข้อมูลใดๆ รวมทั้งข้อมูลของบุคคลที่สาม ซึ่งคู่สัญญา ฝ่ายผู้ให้ข้อมูลได้เปิดเผยแก่คู่สัญญาฝ่ายผู้รับข้อมูล และ คู่สัญญาฝ่ายผู้ให้ข้อมูลประสงค์ให้คู่สัญญาฝ่ายผู้รับข้อมูลเก็บรักษาข้อมูลดังกล่าวไว้เป็นความลับและ/หรือความลับทางการค้าของคู่สัญญาฝ่ายผู้ให้ข้อมูล โดยข้อมูลดังกล่าวจะเกี่ยวข้องกับการดำเนินงานตามวัตถุประสงค์ ซึ่งรวมถึง แต่ไม่จำกัดเพียงแค่ กระบวนการ ขั้นตอน วิธี การดำเนินโครงการ โปรแกรมคอมพิวเตอร์ (อาทิเช่น Source Code โปรแกรมปฏิบัติการ และฐานข้อมูลที่ ใช้เชื่อมต่อโปรแกรมคอมพิวเตอร์) แบบ ต้นแบบ ภาพวาด สูตร เทคนิค การพัฒนาผลิตภัณฑ์ ข้อมูลการทดลอง ข้อมูลทางธุรกิจ ได้แก่ ข้อมูลเกี่ยวกับการตลอด การบริหาร การเงิน เป็นต้น ข้อมูลลูกค้า ข้อมูลลูกจ้าง และ ข้อมูลอื่นใด ที่เกี่ยวข้องกับการดำเนินงานตามวัตถุประสงค์

๓. การรักษาข้อมูลที่เป็นความลับ

คู่สัญญาฝ่ายผู้รับข้อมูลตกลงว่าจะเก็บรักษาข้อมูลที่เป็นความลับที่คู่สัญญาฝ่ายผู้ให้ข้อมูลได้ เปิดเผยให้แก่คู่สัญญาฝ่ายผู้รับข้อมูลภายใต้ข้อตกลงฉบับนี้ เป็นระยะเวลานานตราบเท่าที่ข้อมูลที่เป็น ความลับนั้นยังมีนัยสำคัญต่อผู้ให้ข้อมูล แต่ไม่น้อยกว่าระยะเวลา ..... ปี โดยมีข้อปฏิบัติดังนี้

๓.๑ รักษาข้อมูลที่เป็นความลับได้รับมาอย่างเคร่งครัดและไม่เปิดเผยข้อมูลที่เป็นความลับไม่ว่าทั้งหมดหรือแต่บางส่วน ให้แก่บุคคลใดหรือองค์กรใดทราบ เว้นแต่จะเป็นการเปิดเผยข้อมูลที่เป็น

ความลับให้แก่ลูกจ้างหรือพนักงานของคู่สัญญาฝ่ายผู้รับข้อมูลที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลที่เป็นความลับเท่านั้น และคู่สัญญาฝ่ายผู้รับข้อมูลจะต้องจัดให้ลูกจ้างหรือพนักงานของคู่สัญญาฝ่ายผู้รับข้อมูลได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับด้วย

๓.๒ ใช้ข้อมูลที่เป็นความลับเพียงเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ในข้อ ๑ เท่านั้น

๓.๓ เก็บรักษาเอกสาร บันทึก หรือ วัตถุอื่นใดที่บรรจุข้อมูลที่เป็นความลับที่ได้รับมาไว้ในสถานที่ที่ปลอดภัยที่บุคคลทั่วไปไม่สามารถเข้าถึงได้โดยง่าย และรักษาข้อมูลที่เป็นความลับที่ได้มาในลักษณะและระดับเดียวกันกับการรักษาข้อมูลที่เป็นความลับของตนเอง แต่ทั้งนี้ จะต้องไม่น้อยกว่าระดับที่วิญญูชนพึงรักษาข้อมูลที่เป็นความลับของตนเอง

๓.๔ ไม่ทำซ้ำข้อมูลที่เป็นความลับแม้แต่เพียงส่วนหนึ่งส่วนใดหรือทั้งหมด เว้นแต่การทำซ้ำเพื่อการใช้ข้อมูลที่เป็นความลับให้บรรลุผลตามวัตถุประสงค์ที่กำหนดไว้ในข้อ ๑ เท่านั้น และไม่ทำวิศวกรรมย้อนกลับ หรือถอดรหัสข้อมูลที่เป็นความลับ ต้นแบบ หรือสิ่งอื่นใดที่บรรจุข้อมูลที่เป็นความลับ รวมทั้งไม่เคลื่อนย้าย พิมพ์ทับ หรือทำให้เสียรูปซึ่งสัญลักษณ์ที่แสดงเครื่องหมายสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า ตราสัญลักษณ์และเครื่องหมายอื่นใดที่แสดงกรรมสิทธิ์ของต้นแบบหรือสำเนาข้อมูลที่เป็นความลับที่ได้รับมาจากคู่สัญญาฝ่ายผู้ให้ข้อมูล

๔. การรักษาข้อมูลที่เป็นความลับ

หน้าที่ในการรักษาข้อมูลที่เป็นความลับตามสัญญาข้อ ๓ จะไม่ใช้บังคับกับคู่สัญญาฝ่ายผู้รับข้อมูล หากคู่สัญญาฝ่ายผู้รับข้อมูลสามารถแสดงพยานหลักฐานได้ว่า

๔.๑ ข้อมูลดังกล่าวเป็นข้อมูลที่คู่สัญญาฝ่ายผู้รับข้อมูลได้รับทราบอยู่ก่อนที่คู่สัญญาฝ่ายผู้ให้ข้อมูลจะได้เปิดเผยข้อมูลนั้น

๔.๒ คู่สัญญาฝ่ายผู้รับข้อมูลได้รับข้อมูลที่เป็นความลับจากบุคคลที่สามที่ไม่อยู่ภายใต้ข้อกำหนดในเรื่องการรักษาความลับ หรือ ข้อจำกัดในเรื่องสิทธิ

๔.๓ ข้อมูลดังกล่าวเป้นข้อมูลที่รู้กันโดยทั่วไปก่อนหรือขณะเวลาที่คู่สัญญาฝ่ายผู้ให้ข้อมูลเปิดเผยข้อมูลที่เป็นความลับแก่คู่สัญญาฝ่ายผู้รับข้อมูล หรือเป็นข้อมูลที่ความลับที่ได้เปิดเผยต่อสาธารณะหลังจากที่คู่สัญญาฝ่ายผู้ให้ข้อมูลได้เปิดเผยข้อมูลที่เป็นความลับให้แก่คู่สัญญาฝ่ายข้อมูล

๔.๔ ข้อมูลดังกล่าวเป็นข้อมูลที่มาจากการพัฒนาโดยอิสระของคู่สัญญาฝ่ายผู้รับข้อมูลเอง

๔.๕ ข้อมูลดังกล่าวเป็นข้อมูลที่กำหนดให้ต้องเปิดเผยโดยกฎหมายหรือตามคำสั่งศาล ทั้งนี้คู่สัญญาฝ่ายผู้รับข้อมูลจะต้องแจ้งเป็นหนังสือให้คู่สัญญาฝ่ายผู้ให้ข้อมูลได้รับทราบถึงข้อกำหนดหรือคำสั่งดังกล่าวก่อนที่จะดำเนินการเปิดเผยข้อมูลดังกล่าว และในการเปิดเผยข้อมูลดังกล่าวคู่สัญญาฝ่ายข้อมูลจะต้องดำเนินการตามขั้นตอนทางกฎหมายเพื่อข้อให้คุ้มครองข้อมูลดังกล่าวไม่ให้ถูกเปิดเผยต่อสาธารณะด้วย

๔.๖ผู้รับข้อมูลได้รับความยินยอมเป็นหนังสือจากผู้ให้ก่อนเปิดเผยข้อมูลนั้น

๕. การชดใช้ค่าเสียหาย

๕.๑กรณีที่คู่สัญญาฝ่ายผู้รับข้อมูล และ/หรือพนักงาน และ/หรือลูกจ้างของคู่สัญญาฝ่ายผู้รับข้อมูลฝ่าฝืน ข้อกำหนดจามสัญญาฉบับนี้และก่อให้เปิดความเสียหายแก่ผู้ให้ข้อมูลและ/หรือบุคคล ที่มีอำนาจในการใช้ข้อมูลที่เป็นความลับของคู่สัญญาฝ่ายผู้ให้ข้อมูล คู่สัญญาฝ่ายผู้รับข้อมูลจะต้องชดใช้ค่าเสียหายให้แก่คู่สัญญาฝ่ายผู้ให้ข้อมูลแล/หรือบุคคลที่ได้รับความเสียหายสำหรับความเสียหายเช่นว่านั้น

๕.๒คู่สัญญาฝ่ายผู้รับข้อมูลรับทราบการเปิดเผยหรือการใช้ข้อมูลที่เป็นความลับโดยฝ่าฝืนข้อกำหนดตามสัญญาฉบับนี้จะก่อให้เกิดความเสียหายแก่คู่สัญญาฝ่ายผู้ให้ข้อมูลในจำนวนที่ไม่สามารถประเมินได้ ดังนั้นคู่สัญญาฝ่ายผู้รับข้อมูลยินยอมให้คู่สัญญาฝ่ายผู้ให้ข้อมูลใช้สิทธิ์ที่จะต้องขอต่อศาลเพื่อให้มีคำสั่งให้คู่สัญญาฝ่ายผู้รับข้อมูลหยุดการกระทำใดๆ ที่เป็นการฝ่าฝืนข้อกำหนดตามสัญญาฉบับนี้ และ/หรือใช้วิธีคุ้มครองชั่วคราวใดๆ ตามที่คู่สัญญาฝ่ายผู้ให้ข้อมูลเห็นว่าเหมาะสมได้ โดยคู่สัญญาฝ่ายผู้รับข้อมูลจะเป็นผู้รับผิดชอบในค่าใช้จ่ายต่าง ทั้งหมดในการดำเนินการดังกล่าว

๕.๓กรณีที่คู่สัญญาฝ่ายผู้ให้ข้อมูลสงสัยว่าคู่สัญญาฝ่ายผู้รับข้อมูลฝ่าฝืนข้อตกลงตามสัญญาฉบับนี้ คู่สัญญาฝ่ายผู้รับข้อมูลจะต้องเป็นฝ่ายพิสูจน์ว่าคู่สัญญาฝ่ายผู้รับข้อมูลไม่ได้ฝ่าฝืนข้อตกลงตามสัญญาฉบับนี้

๖. ข้อตกลงอื่นๆ

๖.๑การแก้ไขเปลี่ยนแปลงสัญญาฉบับนี้จะกระทำได้ก็ต่อเมื่อได้ทำเป็นหนังสือและลงนามโดยคู่สัญญาทั้งสองฝ่าย

๖.๒การเปิดเผยข้อมูลที่เป็นความลับของคู่สัญญาฝ่ายผู้ให้ข้อมูลตามสัญญาฉบับนี้ ไม่ถือว่าคู่สัญญาฝ่ายผู้ให้ข้อมูลได้อนุญสตให้คู่สัญญาฝ่ายผู้รับข้อมูลใช้ผลงานซึ่งมีสิทธิบัตร ลิขสิทธิ์เครื่องหมายการค้า หรือข้อมูลทางการค้า อื่นของคู่สัญญา ฝ่ายผู้ให้ข้อมูล เว้นแต่คู่สัญญาฝ่ายผู้ให้ข้อมูลจะมีหนังสือแสดงความตกลงเป็นอย่างอื่น

๖.๓กรณีที่คู่สัญญาฝ่ายผู้รับข้อมูลได้โอนกิจการ รวมกิจการ หรือควบคุมกิจการ หรือดำเนินการอื่นๆ ในลักษณะที่มีการเปลี่ยนแปลงอำนาจในการดำเนินกิจการของคู่สัญญาฝ่ายผู้รับข้อมูล คู่สัญญาฝ่ายผู้รับข้อมูลจะต้องแจ้งให้คู่สัญญาฝ่ายผู้ให้ข้อมูลทราบโดยทันที

กรมทางหลวง
สัญญารักษาความลับของข้อมูล (NDA)

สัญญาฉบับนี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญาละเอียด แล้วจึงได้ลงลายมือชื่อพร้อมประทับตรา (ถ้ามี) ไว้เป็นสำคัญ และต่างเก็บรักษาไว้ฝ่ายละหนึ่งฉบับ

ลงชื่อ ..... (ผู้ว่าจ้าง)
(.....)
กรมทางหลวง

ลงชื่อ ..... (ผู้รับจ้าง)
(.....)
บริษัทฯ

ลงชื่อ .....พยาน
(.....)
ประทับตรา

ลงชื่อ .....พยาน
(.....)
ประทับตรา

ตารางจัดเก็บค่าการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

รายงาน : ☐ : ไตรมาส ที่ ๑ ☐ : ไตรมาส ที่ ๒ ☐ : ไตรมาส ที่ ๓ ☐ : ไตรมาส ที่ ๔

Rack	ลำดับ	ยี่ห้อ	โมเดล	CPU	MEMORY	DISK