INDUSTRY 4.0

กรมโรงงานอุตสาหกรรม
DEPARTMENT OF INDUSTRIAL WORKS

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมโรงงานอุตสาหกรรม (ฉบับปรับปรุงครั้งที่ 2)
พ.ศ. 2561

จัดทำโดย : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม

สารบัญ

หน้า

ประกาศกรมโรงงานอุตสาหกรรม
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

.....

คำนำ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจัดทำขึ้นเพื่อให้ระบบสารสนเทศของกรมโรงงานอุตสาหกรรมมีความมั่นคงปลอดภัยและมิให้ผู้ใดกระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จหรือมีลักษณะอันลามกอนาจารซึ่งอาจก่อให้เกิดความเสียหายแก่กรมโรงงานอุตสาหกรรม และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

คำนิยามศัพท์ที่ใช้ในนโยบายฉบับนี้

๑. “กระทรวง” หมายถึง กระทรวงอุตสาหกรรม

๒. “กรม” หมายถึง กรมโรงงานอุตสาหกรรม

๓. “ศูนย์สารสนเทศ” หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔. “สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของกรมโรงงานอุตสาหกรรมภายใต้การกำกับดูแลของศูนย์สารสนเทศ

๕. “ระบบเครือข่าย” หมายถึง เครือข่ายคอมพิวเตอร์ของกรมโรงงานอุตสาหกรรมภายใต้การกำกับดูแลของศูนย์สารสนเทศ

๖. “คณะกรรมการบริหาร” หมายถึง คณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารกรมโรงงานอุตสาหกรรม (Steering Committee)

๗. “ผู้บริหารระดับสูงด้านสารสนเทศ” หมายถึง รองอธิบดีกรมโรงงานอุตสาหกรรมที่ได้รับมอบหมายให้ทำหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer, CIO)

๘. “ผู้บริหารระดับสูงสุด” หมายถึง อธิบดีกรมโรงงานอุตสาหกรรม

๙. “ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมาบริการ และเจ้าหน้าที่ประจำโครงการต่าง ๆ ของกรมโรงงานอุตสาหกรรม รวมถึงประชาชนที่เข้าใช้งานระบบสารสนเทศของกรมโรงงานอุตสาหกรรม และผู้รับจ้างที่กรมโรงงานอุตสาหกรรมมอบหมายให้ปฏิบัติงานตามสัญญา

๑๐. “สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ

๑๑. “การเข้าถึง...

๑๑. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ การเข้าถึงระบบปฏิบัติการ รวมถึงการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๑๒. “ผู้ดูแลระบบ” หมายถึง ข้าราชการ หรือบุคคลที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศต่าง ๆ ที่ติดตั้งอยู่ภายในกรม

๑๓. “เจ้าหน้าที่กรม” หมายถึง เจ้าหน้าที่ของกรมที่มีสิทธิ์ในการเข้าออกสถานที่ อาคาร ห้อง ตามที่กำหนดในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

๑๔. “ผู้มาติดต่อจากหน่วยงานภายนอก” หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อกับกรมในการติดตั้ง (Implement) บำรุงรักษา (Maintenance) หรือให้คำปรึกษาที่เกี่ยวข้องกับเครื่องแม่ข่าย (Server) ระบบเครือข่าย (Network) โปรแกรม (Software) ฐานข้อมูล (Database) หรืออุปกรณ์อื่นใดที่ติดตั้งอยู่ภายในห้องเครื่องคอมพิวเตอร์แม่ข่ายศูนย์สารสนเทศ

๑๕. “ผู้พัฒนาระบบ” หมายถึง ข้าราชการหรือบุคคลที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาระบบสารสนเทศและบำรุงรักษาระบบสารสนเทศให้กับหน่วยงานต่างๆ ภายในกรม

๑๖. “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๑๗. “ระบบสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงาน สามารถนำมาใช้ประโยชน์ในตารางวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

๑๘. “เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายถึง

กรณีที่ ๑ คือ เหตุการณ์ที่เกิดขึ้นแล้วกับระบบคอมพิวเตอร์และระบบเครือข่ายของกรม

กรณีที่ ๒ คือ เหตุการณ์ที่เป็นจุดอ่อนหรือสงสัยว่าจะเป็นจุดอ่อนทั้งสองกรณี สามารถสร้างความเสียหายให้กับองค์กรได้ในลักษณะใดลักษณะหนึ่ง ซึ่งอาจส่งผลให้

- เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ เช่น ระบบการรับแจ้ง วอ./อก.๖ เกิดการหยุดชะงัก เป็นต้น
- เป็นการละเมิดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กรมกำหนดไว้
- เกิดภาพลักษณ์ที่ไม่ดีต่อกรม หรือทำให้สูญเสียชื่อเสียง เช่น การโพสต์ข้อความพาดพิงถึงกรมในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกรม

๑๙. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของกรมถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

วัตถุประสงค์...

วัตถุประสงค์

๑. ประกาศกรมโรงงานอุตสาหกรรม เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้จัดทำขึ้นเพื่อกำหนดนโยบายและแนวทางให้เกิดความมั่นคงปลอดภัยในระบบสารสนเทศ โดยมีขอบเขตครอบคลุมระบบสารสนเทศของกรม และมีวัตถุประสงค์เพื่อ

๑.๑ ระบบสารสนเทศเกิดความมั่นคงปลอดภัย ป้องกันการบุกรุก และความเสียหายที่มีข้อมูลในระบบสารสนเทศ

๑.๒ ผู้ใช้งานระบบสารสนเทศเกิดความมั่นใจเมื่อระบบมีปัญหา และระบบสามารถกู้คืนกลับใช้งานได้อย่างรวดเร็ว

๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้จัดทำขึ้นเป็นลายลักษณ์อักษร และได้รับการอนุมัติจากอธิบดีกรมโรงงานอุตสาหกรรมและได้เผยแพร่ให้บุคลากรทุกคนที่เกี่ยวข้องทราบและปฏิบัติ

ความรับผิดชอบของผู้บริหาร

๑. อธิบดีกรมโรงงานอุตสาหกรรม เป็นผู้ลงนามอนุมัตินโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. คณะกรรมการบริหาร มีอำนาจหน้าที่ดังนี้

๒.๑ กำหนดและทบทวนนโยบาย ตลอดจนทิศทางงานด้านสารสนเทศของกรม

๒.๒ ผลักดันให้บุคลากรทุกคนตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบสารสนเทศและปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

๒.๓ พิจารณาสนับสนุนการจัดหาทรัพย์สินต่าง ๆ เพื่อให้การบริหารจัดการและให้บริการระบบสารสนเทศมีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายตามประกาศฉบับนี้

๓. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ดูแล ควบคุม การให้บริการด้านระบบสารสนเทศให้สอดคล้องตามนโยบายและรายงานผลการปฏิบัติงานต่อคณะกรรมการบริหารตามวาระที่กำหนด

ขอบเขตของนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมโรงงานอุตสาหกรรม ดังนี้

๑. กำหนดนโยบาย แผนงาน และโครงการด้านสารสนเทศของกรม
๒. ดำเนินการเกี่ยวกับข้อมูล และสารสนเทศเกี่ยวกับโรงงานอุตสาหกรรม
๓. การปฏิบัติงาน หรือสนับสนุนการปฏิบัติงานร่วมกับหน่วยงานอื่นที่เกี่ยวข้อง
๔. จัดสร้างระบบเครือข่ายเชื่อมโยงระหว่างหน่วยงานภายในและภายนอก
๕. พัฒนาระบบการทำงานภายในให้เข้าสู่ระบบบริหารงานรัฐอิเล็กทรอนิกส์
๖. รักษามาตรฐานข้อมูลและเสถียรภาพการให้บริการสารสนเทศ
๗. ฝึกอบรมและเผยแพร่สารสนเทศอุตสาหกรรม
๘. อื่น ๆ ตามที่ได้รับมอบหมาย

การทบทวนและปรับปรุงระบบและข้อปฏิบัติต่อไปนี้ให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๑ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) อย่างน้อยดังนี้

๑.๑ ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงาน

๑.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศที่มีเนื้อหาอย่างน้อยดังนี้

๒.๑ การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๒.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๒.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๒.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๓ การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๓.๑ ให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๓.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๓.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๓.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มบริการอุปกรณ์และระบบเครือข่าย กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ

๓.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างเครือข่ายให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๓.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๔.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๔.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๔.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๔.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๔.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๔.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๕ ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๕.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๕.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

๕.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๖ จัดทำระบบ...

ข้อ ๖ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

๖.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๖.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๖.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๖.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๖.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๗.๑ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) จากผู้ตรวจสอบภายในของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

๗.๒ การประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๘ กำหนดให้มีการทบทวนปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ทันสมัยอย่างน้อยปีละครั้งหรือเมื่อระบบสารสนเทศมีการเปลี่ยนแปลงที่สำคัญ

ข้อ ๙ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๑๐ ให้ทุกหน่วยงานในกรมโรงงานอุตสาหกรรมถือปฏิบัติตามแนวปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศที่แนบท้ายประกาศฉบับนี้

ข้อ ๑๑ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบขับเคลื่อนการปฏิบัติตามนโยบายนี้

จึงประกาศมาเพื่อทราบและถือปฏิบัติ

ประกาศ ณ วันที่ ๒๙ ธันวาคม พ.ศ. ๒๕๖๑

(นายทองชัย ชวลิตพิเชฐ)
อธิบดีกรมโรงงานอุตสาหกรรม

ส่วนที่ ๑

แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของกรมได้ถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๒.๑ สถานที่ตั้งของระบบสารสนเทศที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูล ให้เหมาะสมกับการใช้งานของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๒.๔ ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของกรม และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๒.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งที่ผู้ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓. การควบคุมการเข้าถึงระบบสารสนเทศ

๓.๑ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

๓.๒ เจ้าของข้อมูลและ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

๔. การบริหารจัดการการเข้าถึงของผู้ใช้

๔.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของกรม ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้ง ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เจ้าหน้าที่ที่ลาออกจากราชการแล้ว ต้องทำการยกเลิกสิทธิภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายใน ต้องทำการยกเลิกสิทธิภายใน ๗ วัน

๔.๒ การลงทะเบียนสำหรับผู้ใช้งานระบบสารสนเทศจากภายนอกกรม
ได้กำหนดขั้นตอนการปฏิบัติอย่างเป็นทางการ สำหรับการเข้าใช้งานระบบที่เปิดให้บริการแก่ผู้ประกอบการกิจการโรงงาน แยกออกเป็น ๒ กรณี ดังนี้

๔.๒.๑ ผู้สมัครใช้ระบบใหม่ โดยมีขั้นตอนการลงทะเบียนผ่านระบบสารสนเทศและต้องแนบไฟล์เอกสารที่สำคัญซึ่งใช้ยืนยันตัวตนที่แท้จริง ประกอบด้วย ใบอนุญาตประกอบกิจการโรงงาน หนังสือรับรองบริษัท หนังสือมอบอำนาจ (ถ้ามี) บัตรประจำตัวประชาชนผู้มอบอำนาจ บัตรประชาชนผู้รับมอบอำนาจ ซึ่งเอกสารทุกฉบับต้องประทับตราบริษัทและผู้มีอำนาจลงนามกำกับทุกฉบับ

๔.๒.๒ ผู้ใช้ระบบงานเดิม เมื่อต้องการที่จะขอรหัสประจำตัวผู้ใช้หรือต้องการขอเปลี่ยนรหัสผ่านใหม่ ผู้ใช้ต้องทำหนังสือเป็นลายลักษณ์อักษรแจ้งปัญหาและความต้องการ โดยระบุเลขทะเบียนโรงงาน ชื่อโรงงาน และชื่อผู้ประสานงาน (ผู้รับมอบอำนาจ) พร้อมแจ้งเบอร์โทรศัพท์ และอีเมล์ (สำหรับการแจ้งรหัสประจำตัวหรือเลข ๑๓ หลักและรหัสผ่าน) ลงนามโดยผู้มีอำนาจลงนาม พร้อมเอกสาร คือ หนังสือมอบอำนาจ สำเนาบัตรประชาชนของผู้มอบอำนาจ สำเนาบัตรประชาชนของผู้รับมอบอำนาจ หนังสือรับรองบริษัท และกรณีอยู่นอกนิคมอุตสาหกรรมให้ส่งใบอนุญาตประกอบกิจการโรงงาน (รง. ๔) หรือหากอยู่ในนิคมอุตสาหกรรมให้ส่งใบอนุญาตใช้ที่ดินหรือใบรับแจ้งประกอบอุตสาหกรรม ฉบับล่าสุด และส่งเอกสารทางไปรษณีย์และเอกสารทุกฉบับต้องประทับตราบริษัท

๔.๓ การกำหนดสิทธิ์การใช้เทคโนโลยีสารสนเทศของ กรอ. ต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ โดยกำหนดการเข้าถึงและการใช้งานระบบสารสนเทศ ดังนี้

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไขข้อมูล

๔.๔ ผู้ใช้ต้องลงนามรับทราบสิทธิ์ และหน้าที่เกี่ยวกับการใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๔.๕ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๔.๕.๑ ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบสารสนเทศ แต่ละระบบทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในคู่มือความปลอดภัยในระบบสารสนเทศ เรื่อง “การบริหารสิทธิผู้เข้าถึงระบบ”

๔.๕.๒ การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ในคู่มือความปลอดภัยในระบบสารสนเทศ เรื่อง “การบริหารสิทธิผู้เข้าถึงระบบ”

๔.๕.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๑) ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

๒) ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๔) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่นทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก ๖ เดือน เป็นต้น

๔.๖ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๖.๑ ผู้ดูและระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๖.๒ เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๖.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๔.๖.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๔.๖.๕ ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่กำหนดไว้ในคู่มือความปลอดภัยในระบบสารสนเทศ เรื่อง “การบริหารสิทธิผู้เข้าถึงระบบ”

๔.๖.๖ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรม เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๕. การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๕.๑ การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายขององค์กร ต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๕.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๕.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๕.๔ มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๕.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๖. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๖.๑ ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร ดังนี้

๖.๑.๑ แสดงชื่อผู้ใช้งาน (Username)

๖.๑.๒ ใส่รหัสผ่าน (Password)

๗. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๗.๑ การใช้งานรหัสผ่าน (Password Use)

๗.๑.๑ ให้ผู้ใช้เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับแจ้งจากผู้ดูแลระบบทันทีที่เข้าใช้งานเป็นครั้งแรก

๗.๑.๒ ตั้งรหัสผ่านให้มีความยาวไม่น้อยกว่า ๘ ตัวอักษร ที่ยากต่อการเดา มีการผสมกันระหว่างตัวเลข ตัวอักษรและสัญลักษณ์เข้าด้วยกัน และเปลี่ยนรหัสผ่านทุก ๖ เดือน

๗.๑.๓ ไม่ควรจดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำ

๗.๑.๔ หากมีความจำเป็นบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติแทนตนเองได้ หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านทันที

๗.๑.๕ ผู้ใช้ที่มีสิทธิตามบัญชีผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้ของตนเองเพื่อเข้าใช้ระบบคอมพิวเตอร์และเครือข่ายของกรม และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากบัญชีผู้ใช้งานของตน

๗.๑.๖ กลุ่มผู้ใช้งานที่มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านเดียวกันจะต้องร่วมกันรับผิดชอบหากมีความเสียหาย หรือมีปัญหาเกิดขึ้นกับระบบที่เข้าถึง

๗.๒ ให้ปิดเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เมื่อใช้งานเสร็จสิ้น หรือเมื่อยุติการใช้งานนานเกินกว่า ๓ ชั่วโมง

๗.๓ เมื่อไม่มีการใช้งานระบบเป็นระยะเวลาหนึ่ง ได้แก่ ๓๐ นาที ให้ระบบทำการ Logout ผู้ใช้ออกจากระบบโดยอัตโนมัติ

๗.๔ ให้ทำการตั้งค่า Screen Server ของเครื่องคอมพิวเตอร์ที่รับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานนานเกินกว่า ๑๕ นาที และมีการป้องกันด้วยรหัสผ่านด้วย

๗.๕ ให้ Logout ออกจากระบบทันทีที่ใช้งานเสร็จ

๗.๖ เครื่องโทรสาร เครื่องถ่ายเอกสาร ควรได้รับการป้องกันจากการใช้งานที่ไม่ได้รับอนุญาตด้วยการล็อคกุญแจ หรือรหัสผ่าน

๗.๗ ให้แต่ละฝ่ายมีผู้รับผิดชอบจัดทำทะเบียนสินทรัพย์ และปรับปรุงให้ถูกต้องเป็นปัจจุบันอยู่เสมอ

๗.๘ ให้จัดเก็บสื่อบันทึกข้อมูล ข้อมูล เอกสารสำคัญไว้ในตู้นิรภัยและล็อคกุญแจ ไม่วางทิ้งไว้ในที่เปิดเผย

๗.๙ เอกสารข้อมูลที่มีความสำคัญควรนำออกจากเครื่องพิมพ์ทันที

๗.๑๐ ในกรณีที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ไปใช้งานนอกกรม จะต้องขออนุญาตจากกรมอย่างเป็นลายลักษณ์อักษรก่อน และให้ระมัดระวังรักษาเครื่องคอมพิวเตอร์

และอุปกรณ์ ที่นำไปใช้งานนอกสถานที่มิให้เกิดความเสียหาย หรือสูญหาย รวมทั้งให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ป้องกันไม่ให้บุคคลอื่นเข้าถึงข้อมูลภายในเครื่องได้ เพื่อป้องกันมิให้ข้อมูลที่อยู่ในคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวรั่วไหล

๘. ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๘.๑ ประเภทข้อมูลขององค์กร แบ่งได้ดังนี้

๘.๑.๑ ข้อมูลสารสนเทศด้านการบริหาร

๑) นโยบาย

๒) ข้อมูลยุทธศาสตร์

๓) ข้อมูลคำรับรองการปฏิบัติราชการ

๔) ข้อมูลบุคลากร

๕) ข้อมูลงบประมาณการเงินและบัญชี

๘.๑.๒ ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน

๑) ข้อมูลกฎ ระเบียบ กฎหมาย

๒) ข้อมูลการติดต่อสื่อสารภายในกรม

๓) ข้อมูลการรายงานผลการปฏิบัติราชการ

๔) ข้อมูลการดำเนินงานตามภารกิจของกรมโรงงาน

๘.๑.๓ ข้อมูลสารสนเทศด้านการให้บริการ (หน้าWeb)

๑) ข้อมูลทั่วไปของโรงงาน

๒) ข้อมูลทั่วไปเกี่ยวกับการประกอบการวัตถุอันตราย

๓) ข้อมูลทั่วไปเกี่ยวกับการจดทะเบียนเครื่องจักร

๔) ข้อมูลสถิติโรงงาน

๘.๒ ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

ในแนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๘.๒.๑ การกำหนดชั้นความลับ ตามความสำคัญของข้อมูลในเอกสาร กำหนดไว้ ๓ ระดับ ได้แก่ ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบ ให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณาแหล่งที่มาของเครื่องจักรกำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

๘.๒.๒ การควบคุมเอกสาร โดยกำหนดให้มาตรการควบคุมต่างๆ คือ การจัดทำทะเบียน การตรวจสอบ การจัดทำเอกสาร การทำสำเนาและการแปล การโอน การส่งและการรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉิน เวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

๘.๓ เวลาที่ได้เข้าถึง

๘.๓.๑ การเข้าถึงสารสนเทศในเวลาราชการ (เวลา ๐๘.๓๐ – ๑๖.๓๐ น.)

๘.๓.๒ การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ – ๑๖.๓๐ น.)

๘.๓.๓ การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

๘.๓.๔ การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาและจำนวนระยะเวลาการเข้าถึง ระยะเวลาการเข้าถึง ได้แก่

๑) ๑ - ๓ วัน

๒) ๑ สัปดาห์

๓) ๑ เดือน

๔) ครึ่งปีงบประมาณ

๕) ตามเวลาที่ร้องขอ

๘.๔ ช่องทางการเข้าถึง

๘.๔.๑ ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

๘.๔.๒ เคาน์เตอร์บริการ (เข้าถึงได้ในเวลาราชการ)

๘.๔.๓ โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

๘.๔.๔ หนังสือหรือบันทึกข้อความ

๘.๔.๕ ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

๘.๔.๖ ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

๘.๔.๗ ระบบอินเตอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

๘.๔.๘ ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

๘.๔.๙ เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือในช่วงเวลาพิเศษที่กำหนด)

๘.๔.๑๐ การประชุมทางไกล (เข้าได้ในเวลาราชการและช่วงเวลาพิเศษเป็นรายครั้ง)

๘.๕ ระดับชั้นการเข้าถึงแบ่งตามกลุ่มผู้ใช้งาน ดังนี้

๘.๕.๑ ระดับชั้นสำหรับผู้บริหาร

- ดูข้อมูลได้ทุกระบบ

๘.๕.๒ ระดับชั้นสำหรับผู้ใช้งานภายใน

- เข้าถึงข้อมูลได้ตามสิทธิที่ได้รับ

๘.๕.๓ ระดับชั้นสำหรับผู้ใช้ภายนอก

- ดูข้อมูลที่เปิดเผยได้

๘.๕.๔ ระดับชั้นสำหรับผู้ประกอบการ

- เข้าถึงข้อมูลได้ตามสิทธิที่ได้รับ

๘.๕.๕ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

- บริหารจัดการข้อมูลในระบบที่ได้รับมอบหมาย
- กำหนดสิทธิ์ในการเข้าถึงข้อมูลให้แก่ผู้ใช้ทุกระดับตามที่ได้รับมอบหมาย

ส่วนที่ ๒

แนวปฏิบัติในการควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server)

(Security Control of Server Room)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้อง Server) ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบสารสนเทศ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของกรม จึงได้มีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย

๒.บทบาทและหน้าที่ความรับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

- อนุมัติสิทธิเข้าออกพื้นที่ใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย
- อนุมัติกระบวนการควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย

๒.๒ ผู้ดูแลระบบห้องเครื่องคอมพิวเตอร์แม่ข่าย

- ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องเครื่องคอมพิวเตอร์แม่ข่ายให้ปฏิบัติตามระเบียบ และกฎเกณฑ์ของห้องเครื่องคอมพิวเตอร์แม่ข่ายอย่างเคร่งครัด
- ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องติดบัตรผู้มาติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กรนั้น ๆ แล้ว เท่านั้น

๓. กระบวนการควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑ ผู้ดูแลระบบห้องเครื่องคอมพิวเตอร์แม่ข่าย และเจ้าหน้าที่กรม มีแนวทางปฏิบัติ ดังนี้

๓.๑.๑ ผู้ดูแลระบบห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๓.๑.๒ สิทธิในการเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่ความรับผิดชอบ ในการปฏิบัติงานภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑.๓ ต้องจัดทำระบบการจัดเก็บบันทึกการเข้าออก ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออก ห้อง Server”

๓.๑.๔ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่ายต้องมีการควบคุมอย่างรัดกุม

๓.๑.๕ การเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออก ห้อง Server”

๓.๒ ผู้มาติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๓.๒.๑ ผู้มาติดต่อจากหน่วยงานภายนอกทุกคน ต้องกรอกข้อมูลในเอกสาร “แบบฟอร์มการเข้า-ออก ห้อง SERVER” ให้เรียบร้อยและส่งมายังเจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบล่วงหน้าอย่างน้อย ๑ ชั่วโมง หรือ ในกรณีที่เจ้าหน้าที่ของกรมที่รับผิดชอบในงานนั้น ๆ ไม่สามารถมาด้วยตนเองได้ ให้ลงลายมือชื่อและลงนามรับรองกำกับในเอกสาร “แบบฟอร์มการเข้า-ออก ห้อง SERVER” ตามปกติและมอบหมายให้เจ้าหน้าที่ในกลุ่มงานที่เกี่ยวข้องเป็นผู้ทำหน้าที่พาบุคคลภายนอกเข้าห้องเครื่องคอมพิวเตอร์แม่ข่าย

๓.๒.๒ เมื่อได้รับการอนุมัติแล้วเอกสารจะถูกส่งกลับไปยังผู้ขอเข้าใช้งาน และผู้ขอเข้าใช้งานต้องนำเอกสารที่ลงลายมือรับรองการอนุมัติแล้ว มาแสดงต่อเจ้าหน้าที่ที่รับผิดชอบ พร้อมทั้งทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออก ห้อง Server” ทั้งก่อนและหลังการเข้าใช้งานห้องทุกครั้ง

๓.๒.๓ ผู้มาติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร มาปฏิบัติงานที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออก ห้อง Server”

๓.๒.๔ ผู้มาติดต่อจากหน่วยงานภายนอกต้องแลกบัตร ณ จุดที่กำหนดแลกบัตรของกรม และต้องติดบัตรผ่านตรงจุดที่สามารถมองเห็นได้ชัดเจนตลอดเวลาที่อยู่ในกรม

๓.๒.๕ ผู้มาติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อ “Visitor” กับเจ้าหน้าที่ที่รับผิดชอบ ซึ่งเจ้าหน้าที่ผู้รับผิดชอบต้องตรวจสอบการคืนบัตร

๓.๒.๖ เจ้าหน้าที่ผู้รับผิดชอบ ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้าออกเป็นประจำทุกเดือน

ส่วนที่ ๓

แนวปฏิบัติในการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

(Network Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงล่วงรู้ แก้ไขเปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรม โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

๒. กระบวนการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๒.๑ การใช้งานบริการเครือข่าย

๒.๑.๑ การควบคุมการเข้าถึงเครือข่าย (Network Control) ผู้ดูแลระบบจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๑.๒ การใช้งานบริการเครือข่ายห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของกรม

๒.๑.๓ กรมไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเตอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๒.๑.๔ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว กรมไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๒.๑.๕ ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๒.๑.๖ กรมให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๒.๑.๗ บัญชีผู้ใช้งาน (User Account) ที่กรมให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่า ผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒.๑.๘ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๒.๑.๙ ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิงในระหว่างปฏิบัติงาน

๒.๒ ผู้ดูแลระบบเครือข่ายและเจ้าหน้าที่กรมมีแนวทางปฏิบัติ ดังนี้

๒.๒.๑ ผู้ดูแลระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออก ห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๒.๒.๒ สิทธิการเข้า-ออกห้องต่าง ๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มบริการอุปกรณ์และระบบเครือข่ายเป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

๒.๒.๓ ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกกรมตามกระบวนการที่ระบุไว้ในเอกสาร “แบบบันทึกการเข้า-ออกห้อง Sever”

๒.๒.๔ กรณีเจ้าหน้าที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๒.๒.๕ การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบบันทึกการเข้า-ออกห้อง Sever”

๒.๓ ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติ ดังนี้

๒.๓.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “แบบบันทึกการเข้า-ออกห้อง Sever”

๒.๓.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน ภายในกรมมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่ายต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกห้อง Sever” ให้ถูกต้องชัดเจน

๒.๓.๓ เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำทุกเดือน

๒.๓.๔ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่นอกองค์กร (User Authentication for External Conductions) การเข้าใช้งานระบบเครือข่าย และระบบสารสนเทศของกรม จากภายนอก ต้องมีการระบุตัวตนของผู้ใช้งานและการพิสูจน์ยืนยันตัวตน ด้วยชื่อผู้ใช้ และรหัสผ่านเพื่อยืนยัน และตรวจสอบความถูกต้องก่อนเข้าใช้งาน

๒.๔ การระบุอุปกรณ์บนเครือข่าย

๒.๔.๑ ผู้ดูแลระบบต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อบนเครือข่ายมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว เพื่อจำกัดสิทธิในการใช้ งานระบบสารสนเทศของกรม

๒.๔.๒ ให้ใช้หมายเลข IP address เป็นการระบุตัวตนของอุปกรณ์ที่เชื่อมต่อเข้ากับเครือข่าย

๒.๔.๓ กำหนดให้เครื่องคอมพิวเตอร์ของผู้ดูแลระบบเท่านั้นที่สามารถเชื่อมต่อไปยังเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายของกรม โดยมีการยืนยันตัวบุคคลด้วยชื่อผู้ใช้และการใช้รหัสผ่าน

๒.๔.๔ จัดทำตารางการใช้งาน IP address ภายในระบบเครือข่ายคอมพิวเตอร์ของสถาบัน โดยต้องมีการทบทวนและปรับปรุงตารางดังกล่าว อย่างน้อยปีละ ๑ ครั้ง

๒.๔.๕ ป้องกัน IP address ภายในของระบบเครือข่ายของกรม มิให้หน่วยงานภายนอกรับรู้

๒.๔.๖ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๒.๔.๗ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

๒.๔.๘ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๒.๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๒.๕.๑. ผู้ดูแลระบบต้องกำหนดการเปิด – ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๒.๕.๒. บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องควบคุมระบบคอมพิวเตอร์จะต้องลงชื่ออนุญาตการเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากผู้อำนวยการกลุ่มบริการอุปกรณ์และระบบเครือข่ายก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่เข้ามาติดต่อตลอดเวลา

๒.๕.๓. บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาบริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

๒.๕.๔. ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๒.๖ การแบ่งแยกเครือข่าย

๒.๖.๑ ผู้ดูแลระบบต้องจัดแบ่งเครือข่ายตามกลุ่มของผู้ใช้งาน เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๒.๖.๒ จัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ ซึ่งมีการควบคุมและป้องกันการบุกรุกอย่างเป็นระบบ

๒.๖.๓ ติดตั้ง Fire Wall เพื่อป้องกันทางเข้าเครือข่ายของกรมจากผู้ไม่หวังดี

๒.๗ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

ผู้ดูแลระบบต้องทำการแบ่งแยกเครือข่ายตามความจำเป็นของหน่วยงาน และสอดคล้องกับนโยบายควบคุมการเข้าถึงหรือความต้องการในการเข้าถึงเครือข่าย และระบบงาน อาทิ ความต้องการของผู้ใช้งานกลุ่มต่าง ๆ หรือของผู้บริหาร รวมไปถึงคุณค่าและชั้นความลับของข้อมูลที่ใช้งานอยู่ภายในเครือข่ายของหน่วยงานตลอดจนการแบ่งตามโครงสร้างองค์กร โครงสร้างกายภาพตามพื้นที่ หรือตามกลุ่มของบริการสารสนเทศกลาง กลุ่มผู้ใช้งาน และกลุ่มบริการอุปกรณ์และระบบเครือข่าย ฯลฯ โดยการใช้ขีดความสามารถของอุปกรณ์เครือข่าย ทำการแยกเครือข่ายและควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

๒.๗.๑ มีการประเมินความเสี่ยงสำหรับการจัดแบ่งเครือข่ายภายในหน่วยงาน และกำหนดมาตรการป้องกันสำหรับเครือข่ายย่อยที่ได้มีการจัดแบ่ง

๒.๗.๒ มีการจัดแบ่งเครือข่ายภายในหน่วยงานออกเป็นเครือข่ายภายในและเครือข่ายภายนอก

๒.๗.๓ ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการผู้ใช้งาน และระบบงานต่าง ๆ ของหน่วยงาน

๒.๗.๔ ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่งจะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้

๒.๗.๕ มีการควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยและป้องกันการเปลี่ยนแปลงแก้ไขสัญญาณ ดักแอบดูข้อมูลบนเครือข่าย หรืออื่นโดยไม่ได้รับอนุญาต

๒.๗.๖ มีการใช้ไฟร์วอลล์กั้น หรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๒.๗.๗ มีการกรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย

๒.๗.๘ มีการใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๒.๗.๙ ทำการแบ่งแยกเครือข่ายออกเป็นส่วนๆ รวมทั้งควบคุมการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น ด้วยวิธีการทำ IP Switching

๒.๗.๑๐ มีการแยกวงของเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของหน่วยงาน มีการแยกกลุ่มเครือข่ายเป็น ๓ ประเภทใหญ่ๆ คือ (๑) ระบบเครือข่ายภายใน (๒) ระบบเครือข่ายภายนอก และ (๓) ส่วนที่มีความสำคัญสูง (DMZ Zone ZDemilitarized Zone) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

๒.๗.๑๒ ผู้ดูแลระบบต้องมีการทบทวน ปรับปรุงสิทธิ์ในการเข้าถึงและการใช้งานของผู้ใช้ให้เหมาะสมกับลักษณะงาน

๒.๘ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๒.๘.๑ ระบบเครือข่ายทั้งหมดของกรม ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกกรม ต้องจัดให้มีอุปกรณ์ป้องกันการบุกรุกติดตั้งประจำทุกเส้นทางที่มีการเชื่อมต่อ

๒.๘.๒ ให้ผู้ดูแลระบบควบคุมจำกัดสิทธิ์การเข้าถึงไฟล์วอลล์ และ IPS ของกรม ทั้งทางกายภาพและการกำหนดบัญชีผู้ใช้งานบนไฟล์วอลล์ให้มีน้อยที่สุดเท่าที่จำเป็น

๒.๘.๓ ผู้ดูแลระบบจำกัดการเข้าถึงระบบสารสนเทศของกรม โดยกำหนดกฎของไฟล์วอลล์ให้เหมาะสมและสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งทบทวนกฎไฟล์วอลล์อย่างสม่ำเสมอ เพื่อป้องกันกฎในไฟล์วอลล์ที่ขัดแย้งกันและทำให้ไฟล์วอลล์ทำงานไม่ถูกต้อง

๒.๘.๔ ให้มีการตรวจสอบการแจ้งเตือน ปรับปรุงฐานข้อมูลการโจมตีใหม่ๆ ของ IPS สม่ำเสมอเพื่อป้องกันกรณีเกิดเหตุบุกรุกขึ้นจริง

ส่วนที่ ๔

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

(Operating System Access Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๒.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

๒.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๒.๓ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and Authentication) ผู้ดูแลระบบจัดให้ผู้ใช้งานมีชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ที่ไม่ซ้ำซ้อนกันในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ และต้องให้มีการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๒.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๕ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๒.๗ ซอฟต์แวร์ที่กรมใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟแวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๒.๘ ซอฟท์แวร์ที่กรมจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๒.๙ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรม เพื่อประโยชน์ทางการค้า

๒.๑๐ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อมูลความ รูปภาพที่พบไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๒.๑๑ ผู้ดูแลระบบจะต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุ ดังนี้

๓.๑ มีการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกัน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบบัญชีของเจ้าหน้าที่ทางเทคนิคอื่น ๆ เป็นต้น

๓.๒ ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานแยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

๓.๓ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศโดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓.๔ ผู้ใช้งานสำหรับระบบงานที่มีความสำคัญสูง ต้องทำการพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูง เช่น ใช้การเข้ารหัสข้อมูล สมาร์ทการ์ด token วิธีการทางชีวภาพ (อาทิ การใช้ลายนิ้วมือ เรตินา ฝ่ามือ เสียง)

๓.๕ ผู้ใช้งานที่สามารถเข้าถึงระบบปฏิบัติการได้ จะต้องได้รับการอนุมัติสิทธิ์การเข้าถึงระบบปฏิบัติการจากผู้บังคับบัญชาของหน่วยงานหรือเจ้าของระบบงานเท่านั้น

๓.๖ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๗ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่าย หรือจ่ายแจกให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๘ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๓.๙ กำหนดให้มีช่องทางสำหรับให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านการเข้าใช้ระบบสารสนเทศได้ด้วยตนเอง

๓.๑๐ กรณีผู้ใช้ภายนอกลืมรหัสผ่าน กำหนดให้ผู้ใช้ทำหนังสือขอรับรหัสผ่านใหม่พร้อมแนบเอกสารหลักฐานที่ใช้ในขั้นตอนการลงทะเบียนขอรหัสผู้ใช้

๔. การบริหารจัดการรหัสผ่าน

ผู้ดูแลระบบต้องมีกระบวนการบริหารรหัสผ่าน รวมทั้งจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๔.๑ มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้งานป้อนรหัสผ่านผิดเกิน ๕ ครั้ง ระบบจะทำการล็อคสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีก จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้

๔.๒ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการเข้าพยายามเดารหัสผ่านจากเครื่องปลายทาง

๔.๓ อนุญาตให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง และต้องยืนยันรหัสผ่านใหม่ที่ตั้งอีกครั้ง

๔.๔ ไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตน เช่น ให้แสดงเป็นเครื่องหมายจุด หรือดอกจันบนหน้าจอแทน

๔.๕ จัดเก็บรหัสผ่านเดิมของผู้ใช้งานไว้จำนวนหนึ่งเพื่อป้องกันการกลับไปใช้รหัสเดิมที่ได้เคยตั้งไปแล้ว

๔.๖ จัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๔.๗ ป้องกันข้อมูลรหัสผ่านที่ได้มีการจัดเก็บไว้ในระบบ และ/หรือ ที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น โดยการเข้ารหัสข้อมูล การคำนวณค่าผลรวม (Hash) เพื่อซ่อนข้อมูลรหัสผ่านไว้

๕. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

๕.๑ กำหนดให้ศูนย์สารสนเทศ เป็นผู้ควบคุมและติดตั้งโปรแกรมประเภทยูทิลิตี้ในกรม

๕.๒ โปรแกรมประเภทยูทิลิตี้ที่ติดตั้งใช้งานในกรม ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

๕.๓ ถ้าผู้ใช้งานกระทำการติดตั้งหรือใช้งานโปรแกรมยูทิลิตี้นอกเหนือจากที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ติดตั้งให้และเป็นโปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย หากมี ความเสียหายใด ๆ ที่เกิดขึ้นจากการละเมิดลิขสิทธิ์ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น หากผู้ใช้งานมีความจำเป็นต้องใช้งานโปรแกรมประเภทยูทิลิตี้เพิ่มเติม ต้องกรอกแบบฟอร์มการขอใช้งานโปรแกรมประเภทยูทิลิตี้ ตามที่ศูนย์สารสนเทศ

๖. การหมดเวลาใช้งานระบบสารสนเทศ (Session time-out)

๖.๑ ต้องกำหนดให้ระบบสารสนเทศ เช่น **ระ**บบงานอุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๓๐ นาที

๖.๒ ให้ผู้ดูแลระบบกำหนดให้ระบบสารสนเทศยุติการใช้งานที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๓๐ นาที

๖.๓ กำหนดให้ระบบสารสนเทศ ที่มีความสำคัญสูงหรือระบบสารสนเทศที่มีความเสี่ยงสูง มีการตัดและหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๒๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ส่วนที่ ๕

แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(Application Information Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของกรม และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของกรม ได้อย่างถูกต้อง

๒. การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๒.๑ ผู้ดูแลระบบกำหนดสิทธิ์ และควบคุมการใช้งานของผู้ใช้งานตามฟังก์ชั่นการใช้งานที่ได้กำหนดให้สอดคล้องกับมาตรการการควบคุมการเข้าถึงสารสนเทศ

๒.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรมควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่ สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงาน ในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๔ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าระบบสารสนเทศอีกครั้ง

๒.๕ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบ และรหัสผ่านของบุคลากร ดังต่อไปนี้

๒.๕.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๕.๒ กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

๒.๕.๓ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๕.๔ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๕.๕ ในกรณีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๕.๖ กรณีที่มีการจ้างเหมาดำเนินงาน (Outsource) ด้านสารสนเทศศูนย์สารสนเทศต้องเป็นผู้กำหนดรหัสการเข้าใช้งานระบบสารสนเทศตามระยะเวลาของการจ้างเหมาดำเนินงาน และต้องปฏิบัติตามที่กำหนดไว้ในคู่มือความปลอดภัยในระบบสารสนเทศ เรื่อง “การบริหารสิทธิ ผู้เข้าถึงระบบ”

๒.๖ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ กรมได้กำหนดช่องทางการเข้าถึงระบบสารสนเทศที่สำคัญที่กรมพัฒนาในรูปแบบของ Web base Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายในของกระทรวงอุตสาหกรรม ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว

๒.๗ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๗.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับรวมทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๗.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๗.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๗.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ และการจัดเก็บข้อมูลที่เป็นความลับต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๒.๗.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๗.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๘ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ค โทรศัพท์มือถือสมาร์ทโฟน และแท็บเล็ต อย่างเป็นทางการ รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยที่เหมาะสมต่าง ๆ ดังนี้

(๑) มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๒) สร้างความตระหนักเพื่อให้พนักงานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น การใช้งานในที่สาธารณะ ห้องประชุม นอกสถานที่ซึ่งรวมถึงการเชื่อมต่อโดยผ่านทางเครือข่ายสาธารณะภายนอกหน่วยงาน เป็นต้น

(๓) ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสข้อมูล

(๔) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์ฯ

(๕) สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์ฯ อย่างสม่ำเสมอ

(๖) ควบคุมการเชื่อมต่อและเข้าถึงระบบงานของหน่วยงานจากระยะไกลโดยผ่านทางอุปกรณ์คอมพิวเตอร์ประเภทพกพาซึ่งเชื่อมต่อเข้ามาโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต

(๗) มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงระบบงานของหน่วยงานจากระยะไกลโดยผ่านทางอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๘) ควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของหน่วยงาน

(๙) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในหน่วยงานมาปฏิบัติที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย ต้องลงบันทึกในรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

(๑๐) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกัน เช่น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless area) เป็นต้น

๒.๙ การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัยเพียงพอ ดังนี้

(๑) มีแผนการปฏิบัติงานและขั้นตอนปฏิบัติสำหรับบุคลากรของหน่วยงานที่จำเป็นต้องปฏิบัติงานของหน่วยงานจากภายนอกสำนักงานหรือระยะไกล

(๒) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

(๓) ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการและต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

(๔) ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

(๕) มีข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้
- ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
- ระบบงานหรือบริการต่างๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล
- ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน
- ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

(๖) มีการควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ที่มีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

(๗) มีการป้องกันข้อมูลสำหรับการสื่อสารระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลกับระบบงานต่างๆ ภายในหน่วยงาน

(๘) มีการกำหนดระดับความสำคัญของข้อมูลที่จะมีการรับส่งหรือสื่อสารกันระหว่างหน่วยงานกับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

(๙) ไม่อนุญาตให้ครอบครัวหรือเพื่อนของผู้ปฏิบัติงานจากระยะไกลเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลของหน่วยงาน

(๑๐) มีการควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล รวบทั้งมาตรการการควบคุมการใช้บริการเครือข่ายไร้สายจากที่บ้าน ทั้งนี้เพื่อป้องกันการเข้าถึงระบบ หรือข้อมูลของหน่วยงานโดยไม่ได้รับอนุญาต

(๑๑) มีการป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากระยะไกล เพื่อป้องกันการโต้แย้งกันว่าใครเป็นเจ้าของทรัพย์สินทางปัญญานั้น

(๑๒) มีการสงวนสิทธิ์ในการเข้าถึงอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล เช่น เพื่อทำการตรวจสอบโปรแกรมไม่พึงประสงค์ในอุปกรณ์นั้น เพื่อทำการตรวจสอบข้อมูลในอุปกรณ์สำหรับการดำเนินการสอบสวนกรณีที่มีเหตุเกิดขึ้น

(๑๓) มีการตรวจสอบว่าซอฟต์แวร์ที่ใช้งานบนอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้งานในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล มีใบอนุญาตการใช้งานที่ถูกต้องและครบถ้วน

(๑๔) มีการติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็น เช่น ซอฟต์แวร์ป้องกันไวรัส ไฟร์วอลล์ ในอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล

(๑๕) มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูล

(๑๖) ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยหน่วยงาน

(๑๗) มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานระยะไกล

(๑๘) มีการทำประกันภัยสำหรับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลตามความจำเป็น

(๑๙) มีการสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

(๒๐) มีแผนการสร้างความต่อเนื่องทางธุรกิจในกรณีที่เกิดเหตุฉุกเฉินขึ้นกับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

๒.๑๐ การจ้างเหมาดำเนินงานด้านสารสนเทศ กำหนดให้บุคคลหรือนิติบุคคลหรือพนักงานลูกจ้างที่เป็นคู่สัญญา ต้องมีการลงนามในสัญญารักษาความลับและรักษาข้อมูลไม่เปิดเผยข้อมูลขององค์กร ก่อนการปฏิบัติหน้าที่

๓. การจัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

๓.๑ ต้องกำหนดให้ระบบสารสนเทศจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๑ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของกรมตามปกติเท่านั้น

๓.๒ ต้องกำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์กร) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๓.๓ ต้องกำหนดให้ระบบสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ ทุก ๆ ๑ ชั่วโมง

๔. การจัดการกับระบบซึ่งไวต่อการรบกวน

๔.๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมให้แยกออกจากระบบงานอื่น ๆ ของกรม ที่มีการดูแลสภาพแวดล้อมโดยเฉพาะ ควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๔.๒ กรมกำหนดหลักเกณฑ์และวิธีปฏิบัติเกี่ยวกับบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) ให้ส่วนราชการถือปฏิบัติ ดังนี้

๔.๒.๑ ให้หัวหน้าส่วนราชการเจ้าของงบประมาณแต่งตั้งบุคคลผู้มีสิทธิถือบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) รหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) เพื่อเข้าใช้งานในระบบบริหารการเงินการคลังภาครัฐเข้าสู่ระบบอิเล็กทรอนิกส์ (GFMIS) ซึ่งจะมีอำนาจหน้าที่ใน การบันทึกข้อมูลหรือควบคุมดูแลกลุ่มระบบงานต่าง ๆ เกี่ยวกับงานงบประมาณ บัญชี การเงิน ต้นทุน ตรวจสอบภายใน จัดซื้อจัดจ้าง และทะเบียนสินทรัพย์ โดยให้แจ้งรายชื่อพร้อมทั้งข้อมูลส่วนบุคคลของผู้มีสิทธิใช้งานในระบบดังกล่าว ส่งให้กรมบัญชีกลางเพื่อดำเนินการจัดทำบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) รหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) สำหรับ

เข้าใช้งานในระบบโดยเร็ว ตามแบบลงทะเบียนผู้มีสิทธิถือบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) ที่ส่งมาด้วย

๔.๒.๒ เมื่อกรมบัญชีกลางได้บันทึกข้อมูลที่ได้รับลงในบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) กำหนดรหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) ให้ส่วนราชการเรียบร้อยแล้วกรมบัญชีกลางจะแจ้งให้ส่วนราชการมารับ โดยส่วนราชการในส่วนกลางรับที่กรมบัญชีกลาง (สำนักบริหารการรับ-จ่ายเงินภาครัฐ) สำหรับส่วนราชการในส่วนภูมิภาครัฐที่สำนักงานคลังจังหวัดหรือสำนักงานคลังจังหวัด ณ อำเภอ

๔.๒.๓ เมื่อส่วนราชการได้รับบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) กำหนดรหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) แล้ว ก่อนเริ่มใช้งานในครั้งแรก ให้ผู้มีสิทธิถือบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) โทรศัพท์ติดต่อกรมบัญชีกลาง เพื่อขอให้ดำเนินการเชื่อมต่อกับระบบให้ปฏิบัติงานได้ (Activate)

๔.๒.๔ ส่วนราชการเจ้าของงบประมาณสามารถกำหนดวิธีการปฏิบัติงานและมอบหมายการปฏิบัติงานในการบันทึกข้อมูลและการอนุมัติให้ส่งข้อมูลเพื่อถือปฏิบัติได้ตามความเหมาะสมทั้งนี้ ส่วนราชการจะต้องจัดทำคำสั่ง เพื่อกำหนดบุคคลที่จะได้รับมอบหมาย หน้าที่ความรับผิดชอบและมาตรการในการควบคุมภายในของส่วนราชการขึ้น เพื่อเป็นหลักปฏิบัติสำหรับเจ้าหน้าที่ผู้รับผิดชอบและผู้ที่ได้รับมอบหมายในการเข้าใช้งานในระบบ

๔.๒.๕ ให้ส่วนราชการเจ้าของงบประมาณกำหนดวิธีการเก็บรักษาบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) รหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) ให้เหมาะสมแก่การปฏิบัติงานและความปลอดภัย เพื่อเป็นแนวทางให้ผู้มีสิทธิถือบัตรถือปฏิบัติ

๔.๒.๖ กรณีบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) สูญหาย หากกรมบัญชีกลางไม่ได้รับแจ้ง และมีผู้อื่นนำสิทธิการใช้งานดังกล่าวไปใช้ ผู้มีสิทธิถือบัตรต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นตามแต่กรณี ดังนั้น เพื่อป้องกันปัญหาดังกล่าว ผู้มีสิทธิถือบัตรจะต้องโทรศัพท์แจ้งให้กรมบัญชีกลาง (สำนักบริหารการรับ-จ่ายเงินภาครัฐ ส่วนบริหารการรับ-จ่ายเงิน ทราบทันที ซึ่งกรมบัญชีกลางจะระงับการใช้งานของบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) รหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) โดยทันที

๔.๒.๗ ทั้งนี้ ให้หัวหน้าส่วนราชการมีหนังสือแจ้งกรมบัญชีกลางทราบภายใน ๓ วันทำการนับจากวันที่ผู้มีสิทธิถือบัตรแจ้งด้วยวาจา เพื่อให้กรมบัญชีกลางออกบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) กำหนดรหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) ใหม่ ให้แก่ผู้มีสิทธิถือบัตร โดยในกรณีที่เป็นผู้มีสิทธิถือบัตรคนเดิม ไม่ต้องแจ้งข้อมูลส่วนตัวอีก

๔.๒.๘ กรณีบัตรชำรุดให้หัวหน้าส่วนราชการมีหนังสือแจ้งให้กรมบัญชีกลางออกบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) กำหนดรหัสผู้ใช้งาน (User Log-In) และรหัสผ่าน (Password) ใหม่ ให้แก่ผู้มีสิทธิถือบัตร

๔.๒.๙ กรณีมีการย้ายหรือเปลี่ยนแปลงผู้ดำรงตำแหน่ง ทำให้ต้องมีการเปลี่ยนแปลงผู้มีสิทธิถือบัตร กำหนดสิทธิ์การใช้ (GFMIS Smart Card) ให้ส่วนราชการเจ้าของงบประมาณมีหนังสือแจ้งพร้อมแบบลงทะเบียนผู้มีสิทธิถือบัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) และแนบคำสั่งแต่งตั้งให้ดำรงตำแหน่งของผู้มีสิทธิถือบัตรใหม่ ให้กรมบัญชีกลางทราบเพื่อออกบัตร โดยส่วนราชการสามารถใช้บัตรกำหนดสิทธิ์การใช้ (GFMIS Smart Card) เดิม ใช้งานในระบบต่อไปได้ภายในระยะเวลาไม่เกิน ๑๕ วัน นับจากมีคำสั่งย้ายหรือเปลี่ยนตัวผู้ดำรงตำแหน่ง

๔.๓ การควบคุมการปฏิบัติงานจากภายนอกกรมบัญชีกลาง ได้กำหนดหลักเกณฑ์และวิธีปฏิบัติการใช้ GFMIS Token Key ในการนำส่งข้อมูลผ่านเครือข่าย Internet เพื่อเป็นการเพิ่มช่องทางสำหรับส่วนราชการในการนำส่งข้อมูลเข้าระบบ GFMIS ผ่าน Excel Loader ให้มีความคล่องตัวและสะดวกรวดเร็วขึ้นโดยสามารถปฏิบัติงานที่หน่วยงานได้ โดยกำหนดให้ส่วนราชการดำเนินการ ดังนี้

๔.๓.๑ ให้ใช้ GFMIS Token Key และรหัสผ่าน (password) ในการนำส่งข้อมูลเข้าระบบ GFMIS ผ่านเครือข่าย Internet

๔.๓.๒ ให้จัดทำคำสั่งหรือการมอบหมายไว้เป็นลายลักษณ์อักษร เพื่อกำหนดตัวบุคคลผู้มีสิทธิใช้ GFMIS Token Key และรหัสผ่าน (password) หน้าที่ความรับผิดชอบ มาตรการในการควบคุมตรวจสอบวิธีปฏิบัติในการเก็บรักษา GFMIS Token Key และ รหัสผ่าน (password) พร้อมทั้งต้องดำเนินการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๓.๓ ในกรณี GFMIS Token Key และรหัสผ่าน (password) เกิดการสูญหาย ต้องดำเนินการร้องทุกข์ต่อพนักงานสอบสวนและโทรศัพท์แจ้งการสูญหาย พร้อมทั้งส่งสำเนาบันทึกประจำวันทางโทรสารให้กรมบัญชีกลาง (สำนักบริหารรับ–จ่ายเงินภาครัฐ กลุ่มลูกค้าสัมพันธ์) ทราบทันทีและให้มีหนังสือแจ้งกรมบัญชีกลางภายใน ๓ วันทำการ เพื่อให้กรมบัญชีกลางจัดส่ง GFMIS Token Key และรหัสผ่าน (password) ให้ใหม่ หากกรมบัญชีกลางไม่ได้รับแจ้งและมีผู้อื่นนำสิทธิการใช้งานดังกล่าวไปใช้ ผู้มีสิทธิ์ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นตามแต่กรณี

๔.๓.๔ กรณี GFMIS Token Key เกิดการชำรุดหรือถูกล็อค ให้ปฏิบัติตามคู่มือใช้งาน GFMIS Token Key

ส่วนที่ ๖

แนวปฏิบัติในการจัดทำระบบสำรองข้อมูล

(Backup System)

๑. วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๑. ศูนย์สารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

๔. แนวปฏิบัติ

๔.๑ ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๔.๑.๑ ทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง ตามคู่มือความปลอดภัยในระบบสารสนเทศ เรื่อง การสำรองข้อมูล

๔.๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูล Configuration ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๔.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อม กรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทาง ต่อไปนี้

๔.๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๔.๒.๒ ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๔.๓ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔.๔ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔.๕ ต้องทบทวนทดสอบสภาพการพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๗

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยง

(Risk Management)

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๒. แนวปฏิบัติการประเมินความเสี่ยง

๒.๑ กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ให้ปฏิบัติตามกระบวนการ PDCA ดังต่อไปนี้

๒.๑.๑ การกำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

- กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาจากลักษณะการดำเนินงานกรม สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยีที่กรมใช้งาน
- กำหนดนโยบายความมั่นคงปลอดภัยเพื่อให้ครอบคลุมตามขอบเขตที่กำหนดไว้
- กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศของกรม
- ประเมินความเสี่ยง กำหนดทางเลือกในการจัดการกับความเสี่ยง และกำหนดมาตรการลดความเสี่ยง (ซึ่งสามารถนำมาตรการต่างๆ ในมาตรฐาน ISO/IEC 27001 มาใช้ในการลดความเสี่ยง)
- นำเสนอภาพความเสี่ยงโดยรวม และขออนุมัติสำหรับความเสี่ยงที่ยังหลงเหลืออยู่
- จัดทำเอกสาร Statement of Applicability

๒.๑.๒ การดำเนินการกับระบบบริหารจัดการความมั่นคงปลอดภัย (Do)

- จัดทำแผนการลดความเสี่ยง
- ปฏิบัติตามแผนการลดความเสี่ยงที่ได้กำหนดไว้
- กำหนดแผนการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย เพื่อใช้ในการติดตามภาพรวมของการบริหารจัดการความมั่นคงปลอดภัยของกรม
- จัดทำและดำเนินการตามแผนการอบรม และสร้างความตระหนักเพื่อให้ความรู้และสร้างความตระหนักแก่บุคลากรทั้งหมดที่อยู่ในขอบเขตเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ ประสิทธิผล รวมทั้งมีความมั่นคงปลอดภัย

- บริหารจัดการการดำเนินงานและการใช้ทรัพยากรต่างๆ ภายในขอบเขต เพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของกรม

- จัดทำขั้นตอนปฏิบัติ และ/หรือ กำหนดมาตรการที่จำเป็นสำหรับการติดตามและบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security incident management procedures and controls) รวมทั้งกำหนดให้ผู้ที่เกี่ยวข้องให้ปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยเคร่งครัด

๒.๑.๓ การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย (Check)

- ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ตามนโยบายความมั่นคงปลอดภัย) เพื่อตรวจหาข้อผิดพลาดจากการประมวลผล ตรวจหา การละเมิดหรือความพยายามในการละเมิดความมั่นคงปลอดภัย ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น ตรวจสอบว่าการดำเนินการจัดการกับเหตุการณ์การละเมิดความมั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผลหรือไม่ เป็นต้น

- ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยอย่างน้อยนำสิ่งต่าง ๆ ดังนี้ มาทบทวนด้วย เช่น ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย เหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น ผลจากการวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย คำแนะนำและผลตอบกลับ (Feedback) จากผู้ที่เกี่ยวข้อง

- ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย อย่างสม่ำเสมอโดยดูว่าแผนการวัดความสัมฤทธิ์ผลฯ เป็นไปตามเป้าหมายหรือตัวชี้วัดที่กำหนดไว้ในแผนหรือไม่

- ทบทวนผลการประเมินความเสี่ยงอย่างเป็นระยะๆ (เช่น ทุก ๆ ๓ - ๖ เดือน) ทบทวนระดับความเสี่ยงที่ยังเหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ตามการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับกรม เทคโนโลยีที่กรมใช้งาน วัตถุประสงค์ และกระบวนการทางธุรกิจของกรม ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลง ความสัมฤทธิ์ผลของมาตรการต่าง ๆ ที่กรมใช้งาน เหตุการณ์ภายนอกต่าง ๆ เช่น การเปลี่ยนแปลงด้านกฎหมาย ระเบียบข้อบังคับ หรือ สิ่งที่อยู่ในสัญญาจ้าง และการเปลี่ยนแปลงด้านสังคม เป็นต้น

- ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่ได้กำหนดไว้

- บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่างๆ ซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งประกอบด้วย การประชุมทบทวนด้านความมั่นคงปลอดภัยโดยผู้บริหาร ให้จัดทำรายงานการประชุมและแจ้งเวียนมติให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตามการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่าง ๆ ในนโยบายความมั่นคงปลอดภัยของกรมให้ผู้รับผิดชอบบันทึกหลักฐานการ

ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเหล่านั้นไว้เพื่อให้สามารถตรวจสอบได้ในภายหลัง

๒.๑.๔ การทบทวนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (Act)

- ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามผลของการเฝ้าระวังติดตามและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย เช่น การปฏิบัติตามมติการประชุมทบทวนโดยผู้บริหาร การปรับปรุงนโยบายความมั่งคงปลอดภัย การจัดการหรือแก้ไขความไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัย การกำหนดมาตรการเพิ่มเติมการเกิดขึ้นของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เคยเกิดขึ้นแล้ว การปฏิบัติตามแผนการลดความเสี่ยง การปฏิบัติตามแผนด้านความมั่นคงปลอดภัย การปฏิบัติตามคำแนะนำและผลตอบกลับจากผู้ที่เกี่ยวข้อง เป็นต้น
- แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้องทราบ โดยให้รายละเอียดที่เพียงพอและเหมาะสมตรวจสอบว่าการปรับปรุงที่ได้ดำเนินการไปแล้วนั้น บรรลุผลตามที่ต้องการหรือไม่

๒.๒ การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศต้องดำเนินการดังต่อไปนี้

๒.๒.๑ มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศ การสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒.๒.๒ มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๒.๒.๓ มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น

๒.๒.๔ มีการกำหนดสิทธิ์ให้ผู้ใช้ในแต่ละระดับ (Access rights)

๒.๓ ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อยปีละ ๑ ครั้ง

๒.๔ ต้องมีการตรวจสอบและประเมินความเสี่ยงของระบบฐานข้อมูลและสารสนเทศโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) เป็นประจำทุกปี ตามเกณฑ์คุณภาพการบริหารจัดการภาครัฐ (PMQA) ของสำนักงาน กพร. ในส่วนของ หมวด ๔ การวิเคราะห์และการจัดการความรู้ หัวข้อ IT ๖ ส่วนราชการต้องมีระบบบริหารความเสี่ยงของ ระบบฐานข้อมูลและสารสนเทศ กำหนดให้กรมต้องดำเนินการ ดังนี้

๒.๔.๑ แสดงการทบทวนนโยบายความมั่นคง

๒.๔.๒ แสดงผลการจัดทำนโยบายความมั่นคงปลอดภัยขององค์การอย่างเป็นลายลักษณ์อักษรโดย CIO หรือ CEO เป็นผู้อนุมัติ

๒.๔.๓ แสดงผลการกำหนดหน้าที่ความรับผิดชอบของข้าราชการในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศองค์การ

๒.๔.๔ แสดงระบบสารสนเทศที่มีทั้งหมดในองค์การ

๒.๔.๕ แสดงระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูลและสารสนเทศ

๒.๔.๖ แสดงรายละเอียดแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๒.๔.๗ แสดงผลการปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๒.๔.๘ แสดง Access Rights ที่ถูกต้องและทันสมัยได้อย่างน้อย ๑ ระบบ

ส่วนที่ ๘

แนวปฏิบัติในนโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ต

(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของกรมถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการขออนุญาตจากกลุ่มบริการอุปกรณ์และระบบเครือข่าย ศูนย์สารสนเทศ เป็นลายลักษณ์อักษร

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

๒.๓ ผู้ใช้หมั่น Update Patch และ Hotfix อย่างสม่ำเสมอ โดยสามารถ Download patch และ Hotfix ต่างๆ จาก Microsoft website เพื่อแก้ปัญหาช่องโหว่

๒.๔ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๒.๕ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกรมเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๖ ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรม

๒.๗ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับกรม

๒.๘ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๒.๙ ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑๐ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๙

แนวปฏิบัติในข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์

(Terms of Use and Disclaimer)

๑. วัตถุประสงค์

๑.๑ เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของกรม สามารถสนับสนุนการปฏิบัติงานของกรมเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์มีประสิทธิภาพ

๑.๒ เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับบุคลากรของกรม และหน่วยงานเป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของกรม

๒. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม

๒.๑ ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของกรม จะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้

๒.๑.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

๒.๑.๓ พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐

๒.๑.๔ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๒.๑.๕ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

๒.๑.๖ ข้อตกลง เงื่อนไขการใช้บริการที่กรมกำหนด

๓. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ของกรม

๓.๑ หน่วยงาน/บุคคลผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของกรม จะต้องใช้จดหมายอิเล็กทรอนิกส์ของกรม เพื่อผลประโยชน์ของทางราชการ

๓.๒ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการประกอบธุรกิจ หรือแสวงหาผลประโยชน์ส่วนตน

๓.๓ ห้ามใช้บริการนี้ ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใดๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

๓.๔ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม ในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารความลับของทางราชการ

๓.๕ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรม เพื่อการเผยแพร่ข้อมูลข่าวสาร ภาพ เสียง ข้อความที่ไม่เหมาะสม หรือสร้างความเสื่อมเสียให้กับผู้อื่น

๓.๖ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือกรมตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมโรงงานอุตสาหกรรม

๓.๗ ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

๓.๘ ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

(๑) การสร้างจดหมายลูกโซ่ (Chain mail)

(๒) การส่งจดหมายจำนวนมาก (Spam mail)

(๓) การส่งจดหมายต่อเนื่อง (Letter bomb)

(๔) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

๓.๙ ห้ามผู้ใช้บริการกระทำการใดๆ ที่อาจจะนำมาซึ่งความเสื่อมเสีย หรือก่อให้เกิดความเสียหายแก่ระบบเครื่องแม่ข่ายจดหมายอิเล็กทรอนิกส์ของกรม

๓.๑๐ ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคล หรือหน่วยงานของจดหมายอิเล็กทรอนิกส์ไว้เป็นความลับ

๓.๑๑ ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของกรม

๓.๑๒ การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกกรมจะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารตามที่กรมกำหนด

๓.๑๓ ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน (Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

๓.๑๔ ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ กรมหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจเพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของกรม ได้อย่างถูกต้อง

๓.๑๕ กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับบริการแก่สมาชิกนั้นๆ เป็นการชั่วคราวเพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุนั้น ๆ

ส่วนที่ ๑๐

แนวปฏิบัติในการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

(Third party access control)

๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบสารสนเทศขององค์กรให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบสารสนเทศของที่ปรึกษาการใช้บริการด้านระบบสารสนเทศจากหน่วยงานภายนอก เป็นต้น

๒. แนวทางปฏิบัติ

๒.๑ ผู้อำนวยการกลุ่มบริการระบบสารสนเทศ ๑ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศได้

๒.๒ การควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายนอก

๒.๒.๑ บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของกรม จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบสารสนเทศ ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๒.๒.๓ หน่วยงานภายนอกที่ทำงานให้กับกรม ทุกหน่วยงานไม่ว่าจะทำงานอยู่ภายในกรมหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของกรม โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศ

๒.๒.๔ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๒.๒.๕ สำหรับโครงการขนาดใหญ่หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรม ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๒.๒.๖ กรมมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบสารสนเทศ เพื่อให้มั่นใจได้ว่ากรมสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๒.๒.๗ ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงานคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้องรวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ในแนวปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศ

ส่วนที่ ๑๑

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

(User access management)

๑.วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ มีการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่เจ้าหน้าที่กรม อย่างน้อย ๑ ครั้ง หลังจากมีการประกาศใช้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๓ หากมีการปรับปรุงเปลี่ยนแปลงนโยบายหรือแนวปฏิบัติฯ จะต้องมีการประชาสัมพันธ์ให้เจ้าหน้าที่กรมรับทราบ

๒.๔ จัดฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ข้าราชการบรรจุใหม่ โดยกำหนดไว้ในหลักสูตรการอบรมข้าราชการบรรจุใหม่ของกรมทุกปี

๒.๕ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๖ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๗ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password)

๑. กำหนดรหัสผ่าน (Password) ต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยกำหนดให้มีการผสมกันระหว่างตัวเลข ตัวอักษร ตัวอักขระพิเศษ และสัญลักษณ์ต่าง ๆ และกำหนดให้มีการเปลี่ยนรหัสผ่านทุก ๖ เดือน

๒. จัดให้การบริหารจัดการการจัดส่งรหัสผ่านให้กับผู้ใช้งาน และกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีที่ใช้งานครั้งแรก

๒.๘ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบ ทบทวนสิทธิ์ในการใช้งานของผู้ใช้งาน ให้ถูกต้องเป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง รวมถึงการยกเลิกสิทธิ์การใช้งานเมื่อผู้ใช้งานลาออก โอนย้ายงานหรือพ้นสภาพการเป็นข้าราชการพนักงานราชการ ลูกจ้างประจำของกรม

ส่วนที่ ๑๒

แนวปฏิบัติในการติดตั้งและกำหนดค่าของระบบ

(System Installation and Configuration)

๑. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

๑.๑. ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

๑.๒. ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

๑.๓. กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator) และชื่อผู้ใช้ (User)

๑.๔. กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address

๑.๕. ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

๑.๖. ติดตั้งโปรแกรม Antivirus / ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

๒. การบริหารบัญชีผู้ใช้/สิทธิการเข้าถึงและการใช้งานระบบ (User Account Management)

๒.๑. กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

๒.๒. กำหนดชื่อผู้ใช้ (User) และรหัสผ่าน (Password)

๒.๓. บันทึกบัญชีผู้ใช้และสิทธิการเข้าใช้ระบบ

๓. การปรับปรุงการรักษาความปลอดภัย/Antivirus (System Security & Antivirus Update)

๓.๑. ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ เช่น Log File หรือตรวจสอบ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

๓.๒. ปรับปรุง/กำหนดค่าระบบความปลอดภัย ให้เหมาะสมกับปัญหา

๓.๓. ปรับปรุงโปรแกรม Antivirus และ definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

๓.๔. ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

๔. ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

๔.๑. ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่หน่วยงานใช้หรือรองรับงานบริการ

๔.๒. กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพตามระบบฐานข้อมูลนั้นกำหนด

๔.๓. สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้อื่นและสิทธิการใช้

๔.๔. ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

๕. ติดตั้งฐานข้อมูล โปรแกรมบริการ/โปรแกรมระบบงานต่างๆ/กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้ และสิทธิการเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

๕.๑. ติดตั้งโปรแกรมการให้บริการ หรือโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

๕.๒. กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมบริการหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

๕.๓. ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด

๕.๔. แจ้งผู้ใช้ หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อ รหัสผ่านและสิทธิการเข้าใช้ระบบ และฐานข้อมูลตามระบบกำหนด

๕.๕. ระบุเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน (Restore Test)

๕.๖. บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้แต่ละระดับของระบบทุกครั้งที่มีการสร้าง/ปรับปรุง

๖. ปฏิบัติการระบบฐานข้อมูล การสำรอง/สำเนาฐานข้อมูล (Database Backup) และการกู้คืนฐานข้อมูล (Database Restore)

๖.๑. ตรวจสอบการทำงานโปรแกรมการให้บริการ / โปรแกรมระบบงานที่ใช้ฐานข้อมูล

๖.๒. ตรวจสอบการทำงานของฐานข้อมูลในระบบ Database System และขนาดความจุตามระยะเวลาที่กำหนดแต่ละระบบ (ทุกวันหรือรายสัปดาห์)

๖.๓. ตรวจสอบการทำงานและขนาดของ Device ที่จัดเก็บฐานข้อมูลด้านการทำงานและรองรับบริการได้ปกติหรือไม่

๖.๔. ทำการสำรองข้อมูล Backup ฐานข้อมูลบันทึกลงสื่อที่กำหนดไว้

๖.๕. ระบุชื่อ Backup โดยระบุชื่อฐานข้อมูล และวันที่ Backup

๖.๖. ทำการสำเนา Backup ฐานข้อมูลตามระบบกำหนด และส่งให้หน่วยงานจัดเก็บสำเนาที่ระบุ

๖.๗. ทดสอบการกู้คืนฐานข้อมูลจาก Backup ตามกำหนด

๖.๘. ปฏิบัติการกู้คืนจาก Backup ล่าสุด ในกรณีมีความเสียหายของระบบฐานข้อมูล

๖.๙. บันทึกการปฏิบัติการทุกครั้ง ตามชื่อฐานข้อมูล (ชื่อ Backup /Restore Test หรือ การกู้คืน)/ระดับปฏิบัติการ/วันที่ปฏิบัติการ/ปัญหาหรือผลสำเร็จ/ชื่อผู้ปฏิบัติการ/การทำสำเนาระบบ/ Destination Area

๖.๑๐. แจ้งผู้ควบคุม กำกับ ผู้รับผิดชอบระบบ และผู้ใช้ระบบฐานข้อมูลถึงความเสียหาย การแก้ไข การกู้คืนและการใช้งาน

๗. การตรวจสอบและดูแลบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบ

๗.๑. ตรวจสอบการทำงานส่วนประกอบของเครื่องแม่ข่าย ได้แก่ สถานภาพการทำงานของเครื่อง โดยรวม Hard disk / System Fan / System Led / จอภาพและอุปกรณ์อื่นๆ

๗.๒. ทำความสะอาดเครื่องอุปกรณ์เป็นระยะตามกำหนด

๗.๓. ตรวจสอบการทำงานของอุปกรณ์สำรองไฟฟ้าหากมีการติดตั้ง

๗.๔. ตรวจสอบสถานการณ์ทำงาน ประสิทธิภาพของระบบ จาก Device Monitor และ Performance Monitor ของ Operating System ได้แก่ สถานการณ์ทำงานของ CPU/ Memory / หน่วย Hard drive ขนาดความจุที่เหลือ

๗.๕. แจ้งผลตรวจสอบ/ปัญหา ให้ผู้บริหารระบบ System Administrator ทราบ

๗.๖. บันทึกการตรวจสอบ/แก้ไข และดูแลบำรุงรักษาทุกครั้ง

ส่วนที่ ๑๓

แนวปฏิบัติในการกำหนดแบ่งอำนาจหน้าที่ผู้รับผิดชอบ

(The Responsible authority)

วัตถุประสงค์

การกำหนดแบ่งอำนาจหน้าที่ มีวัตถุประสงค์เพื่อลดความเสี่ยงด้านโครงสร้างพื้นฐาน ซึ่งมีแนวทางปฏิบัติดังนี้ คือ ต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละกลุ่มภายในศูนย์สารสนเทศ อย่างชัดเจนเป็นลายลักษณ์อักษรซึ่งมีการจัดให้มีบุคลากรสำรองภายในกลุ่มในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น โดยกำหนดหน้าที่ ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบสารสนเทศ รายละเอียด ดังนี้

๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

- ผู้บริหารระดับสูงสุด (CEO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ระดับปฏิบัติ

๒.๑ ผู้รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและสารสนเทศผู้รับผิดชอบ ได้แก่ กลุ่มบริการระบบสารสนเทศ ๒

๒.๒ ผู้รับผิดชอบ ควบคุม ดูแล การใช้ระบบสารสนเทศต่าง ๆ มีรายละเอียดตามแผนป้องกัน แก้ไขและสำรองฉุกเฉินด้านระบบฐานข้อมูลและสารสนเทศ (IT Prevention, Recovery and Contingency Plan)

ส่วนที่ ๑๔

แนวปฏิบัติเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ใช้งาน

(Responsibility of the user)

๑. วัตถุประสงค์

การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและทรัพย์สินอื่น ๆ ดังนี้

๑.๑ เจ้าหน้าที่ทุกคนต้องปฏิบัติการป้องกันทรัพย์สิน

๑.๒ เจ้าหน้าที่ต้องออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๑.๓ ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล๊อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของราชการ

๑.๔ ต้องป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน และป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสาร ไปรษณีย์ เพื่อความปลอดภัยของข้อมูล

๑.๕ ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ กล้องดิจิตอล เครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น โดยไม่ได้รับอนุญาต

๑.๖ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒. กำหนดมาตรการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการเข้าถึงข้อมูลสำคัญที่ยังคงค้างอยู่บนสื่อบันทึกข้อมูลนั้น โดยต้องปฏิบัติตามแนวทาง ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การตัดด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ใช้การตัดด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีทำลายข้อมูลตามมาตรฐานการทำข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M (ซึ่งมีการฟอร์แมทเป็นจำนวนหลายรอบ)
แฟ้มข้อมูลลับ	ใช้การลบแฟ้มข้อมูลลับอย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานบนเครื่องคอมพิวเตอร์เมื่อหมดความจำเป็นในการใช้งานด้วยวิธีการตามมาตรฐานการทำข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๒๒-M (ลบแล้วไม่สามารถกู้ไฟล์กลับคืนมาได้)

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๓.๑ เครื่องคอมพิวเตอร์ที่จะนำมาใช้งานภายในกรมจะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส

๓.๒ การนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เชื่อมต่อเข้ากับระบบเครือข่ายของกรม จะต้องมีการลงทะเบียนการใช้งานอย่างเป็นลายลักษณ์อักษร และให้ผู้ดูแลระบบแบ่งกลุ่มผู้ใช้งาน กำหนดระยะเวลา และสิทธิ์ในการใช้งานตามกลุ่มผู้ใช้งาน รวมทั้งให้ยกเลิกสิทธิ์เมื่อสิ้นสุดการใช้งาน

๔. การปฏิบัติงานจากภายนอกกรม (Teleworking)

๔.๑ การควบคุมการเข้าใช้งานระบบจากภายนอก ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในกรม เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ดังนี้

๔.๑.๑ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกรม จะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๔.๑.๒ ต้องไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๔.๑.๓ การให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อย่างเป็นทางการและผู้ใช้ ต้องปฏิบัติตามข้อกำหนดของกรมในการเข้าสู่ระบบจากระยะไกลโดยเคร่งครัด

๔.๑.๔ ในกรณีนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ไปใช้งานนอกกรม ให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันมิให้ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวรั่วไหล

ส่วนที่ ๑๕
แนวปฏิบัติในการจัดหาระบบเทคโนโลยีสารสนเทศ
(Procurement for Information Technology System)

กำหนดแนวปฏิบัติในการจัดหาระบบเทคโนโลยีสารสนเทศ ให้ดำเนินการตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม ให้ครอบคลุมอย่างเคร่งครัด ดังนี้

๑. การเสนอของบประมาณ

๑.๑ ในการจัดหาระบบเทคโนโลยีสารสนเทศ โดยใช้งบประมาณรายจ่ายประจำปีของกรม ให้ทุกหน่วยงานในกรม ดำเนินการจัดทำรายละเอียดประกอบคำของบประมาณ เสนอคณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสาร (IT Steering Committee) พิจารณาเพื่อขอความเห็นชอบก่อนเสนอร่างคำของบประมาณของกรม (ปฏิทินคำของบประมาณในแต่ละปี) และให้เป็นไปตาม แนวทางการปฏิบัติในการจัดหาระบบคอมพิวเตอร์ของกระทรวง

๑.๒ ในการจัดหาระบบเทคโนโลยีสารสนเทศ โดยใช้งบอื่นใดที่นอกเหนือจากงบประมาณรายจ่ายประจำปีของกรม ให้ทุกหน่วยงานในกรม ดำเนินการตามแนวทางการปฏิบัติในการจัดหาระบบคอมพิวเตอร์ของกระทรวง <u>โดยไม่ต้องเสนอขอความเห็นชอบต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสาร (IT Steering Committee)</u>

๒. การจัดทำรายละเอียดของโครงการควรมีองค์ประกอบที่เกี่ยวข้อง ดังนี้

๒.๑ ใช้ระบบตรวจสอบการเข้าใช้งาน Single Sign On ของกรม

๒.๒ มีระบบกำหนดสิทธิการใช้งานในระดับผู้ใช้งาน หรือ จากรหัสหน่วยงานที่รับมาจากระบบ Single Sign On หรือมีการสร้างกลุ่ม (Group Objects) ที่สามารถบริหารจัดการได้

๒.๓ สามารถเชื่อมโยงข้อมูลกับระบบงานอื่นๆด้วยคีย์หลัก เช่น เลขทะเบียนโรงงาน เลข ร.๒/๑ รหัสสถานประกอบการวัตถุอันตราย เลขประจำตัวผู้เสียภาษี และจัดทำเป็นเว็บเซอร์วิส ในรูปแบบของ SOAP (Simple Object Access Protocol) หรือ RESTful (Representational state transfer) หรือวิธีอื่นใดที่คณะกรรมการบริหารเห็นชอบ

๒.๔ การจัดเก็บข้อมูล ควรจัดเก็บข้อมูลเท่าที่จำเป็นและอ้างอิงกับคีย์หลัก และหากมีไฟล์แนบในระบบสารสนเทศ ควรมีการกำหนดขนาดแต่ละไฟล์ไม่เกิน ๑๐ เมกะไบต์ และกำหนดประเภทของไฟล์ให้ชัดเจน

๒.๕ กรณีที่มีการบันทึกข้อมูลการติดต่อจากผู้ประกอบการหรือประชาชน จะต้องมีระบบสารสนเทศที่เชื่อมโยงข้อมูลกับกรม และกระทรวง โดยระบุเลขทะเบียนพาณิชย์ หรือเลขบัตรประชาชน

๒.๖ ระบบฐานข้อมูลที่ใช้ควรพิจารณาใช้งานตามความเหมาะสม โดยลำดับดังนี้ MS SQL Server, Postgres, Mysql, Access โดยหลีกเลี่ยงการใช้ Oracle โดยไม่จำเป็น

๒.๗ การพัฒนาระบบควรนำระบบลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) มาป้องกันการแก้ไขเอกสาร

๒.๘ ข้อมูลที่นำเข้าโดยผู้ประกอบการหรือประชาชน ควรให้บันทึกเท่าที่จำเป็น หากมีข้อมูลเพียงเล็กน้อย (น้อยกว่า ๕๐ ฟิลด์) ให้จัดทำหน้าจอนำเข้าข้อมูล (Input) ผ่านหน้าเว็บ หรือโมบาย

แอพพลิเคชั่น โดยผู้ประกอบการหรือประชาชน จะต้องทำการเข้าระบบ (Login) ก่อน แต่ถ้ามีข้อมูลจำนวนมากควรจัดทำในรูปแบบเอกสารออฟไลน์ และนำเอกสารดังกล่าวเข้าสู่ระบบ

๒.๙ หน้าจอบันทึกข้อมูล ควรมีการตรวจสอบความถูกต้อง (Validate) ทุกๆการนำเข้าข้อมูล (Input) ว่าค่าที่มีความเป็นไปได้

๒.๑๐ ข้อมูลการอนุญาต/ใบอนุญาต และเอกสารอื่นใด ให้จัดทำในรูปแบบอิเล็กทรอนิกส์ที่เป็นมาตรฐาน และให้บริการผ่านเว็บไซต์ โดยมีรหัสคิวอาร์โค้ด (QR Code) ที่อ้างอิงถึงข้อมูลพิมพ์ลงในเอกสาร

๒.๑๑ การวิเคราะห์ ออกแบบ และพัฒนาระบบควรมีองค์ประกอบที่เกี่ยวข้อง ดังนี้

๒.๑๑.๑ วิเคราะห์และออกแบบระบบโดยใช้เครื่องมือภาษา Unified Modeling Language (UML) ได้แก่ Use Case Diagrams, Class Diagrams, Activity Diagram การออกแบบส่วนติดต่อผู้ใช้ (User Interface Design) การออกแบบฐานข้อมูล (Database Design) และ/หรืออื่น ๆ ที่เกี่ยวข้อง โดยระบุ Framework และ/หรือ Design Pattern

๒.๑๑.๒ พัฒนาระบบที่สอดคล้องตาม Framework และระบุ Platform ของเครื่องแม่ข่ายและเครื่องลูกข่าย

๒.๑๑.๓ จัดทำคู่มือผู้ใช้งาน (User Manual)

๒.๑๑.๔ จัดทำคู่มือผู้ดูแลระบบ (System Manual) โดยมีเนื้อหาอย่างน้อย

- ข้อกำหนดสภาพแวดล้อมของเครื่องแม่ข่าย และขั้นตอนการติดตั้งระบบบนเครื่องแม่ข่าย
- Use Case, Class Diagram, Activity Diagram (แบบ Swimlan), Data Dictionary
- รายละเอียดของโปรแกรม (Program Specification) ที่อธิบายการทำงานของโปรแกรมทุกกระบวนงานครอบคลุมทุกโปรเซสงานที่สอดคล้องกับ Framework/Design Pattern
- รายละเอียดอื่น ๆ ที่จำเป็นสำหรับใช้การอ้างอิงเพื่อปรับปรุงแก้ไขระบบในอนาคต

๒.๑๒ ต้องมีการจัดทำแผนค่าใช้จ่ายในการบำรุงรักษา (Budget Plan) หลังหมดการรับประกันจากผู้พัฒนาระบบ และหากมีค่าใช้จ่ายเพิ่มเติม เช่น ค่าเช่าอินเตอร์เน็ต ค่าบริการอื่นๆรายเดือน/รายปี จะต้องแจ้งราคาให้ทราบโดยละเอียด

๒.๑๓ อุปกรณ์คอมพิวเตอร์ที่จัดหาจะต้องเป็นไปตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย ให้พิจารณาใช้ทรัพยากรจากระบบ Cloud ของกรม หรือกระทรวงก่อน

๒.๑๔ การเชื่อมโยงระหว่างระบบสารสนเทศ หรือการทำงานร่วมกับระบบงานเดิมต่าง ๆ ที่กรมใช้งานอยู่ ต้องได้รับความเห็นชอบจากศูนย์สารสนเทศ

๒.๑๕ ควรมีการฝึกอบรม แนะนำการใช้งาน หรือ มีบทเรียนออนไลน์ (E-learning)

๓.การติดตั้งและการทดสอบ

๓.๑.๑ กำหนดแผนการติดตั้ง ระยะเวลาที่จะดำเนินการ และแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่นๆ

๓.๓.๒ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๓.๓.๓ ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน (Configuration) หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งไม่สำเร็จ ต้องกลับมาใช้สถานะเดิมได้

๓.๓.๔ ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือเปลี่ยนแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๓.๓.๕ สำหรับซอฟต์แวร์ที่จะทำการติดตั้งให้ปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมโรงงานอุตสาหกรรม ส่วนที่ ๕ แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๓.๓.๖ การอบรมเจ้าหน้าที่และผู้ใช้งาน

๔. การส่งมอบระบบสารสนเทศเพื่อให้ศูนย์สารสนเทศดำเนินการจะต้องจัดส่ง

๔.๑ คู่มือผู้ดูแลระบบ

๔.๒ ส่งมอบโปรแกรม (Source Code) ของระบบทั้งหมดในรูปแบบ CD

๑. การจัดสรรหรือการจัดหาอุปกรณ์เพื่อรองรับระบบสารสนเทศใหม่ ให้รวมอยู่ในการจัดหาด้วย รวมทั้งการดูแลระบบ การดูแลข้อมูล การสำรองข้อมูล และการ update ระบบต่าง ๆ ให้เป็นหน้าที่ของผู้พัฒนาระบบ และอยู่ในการกำกับดูแลของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. กำหนดให้ผู้ดูแลระบบของหน่วยงานเจ้าของเรื่อง ที่ได้รับการอบรมและมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานนั้นๆ

๓. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๔. กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบงาน เป็นต้น

บันทึก

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....