ประกาศกรมศุลกากร

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล อธิบดีกรมศุลกากรโดยความเห็นชอบของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมศุลกากร เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕”

ข้อ ๒ ในประกาศนี้

(๑) “ผู้ใช้งาน” หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของกรมศุลกากร รวมถึงบุคคลภายนอกที่เป็นหน่วยงานราชการ รัฐวิสาหกิจ นักศึกษา และผู้ประกอบการที่เกี่ยวข้องกับกรมศุลกากร ทั้งภายใน และภายนอกประเทศ

(๒) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรมศุลกากร

(๓) “เครื่องคอมพิวเตอร์ส่วนบุคคล” หมายความว่า เครื่องคำนวณอิเล็กทรอนิกส์ที่มีการทำงานแบบอัตโนมัติ ซึ่งทำหน้าที่เหมือนสมองกล สามารถแก้ปัญหาต่างๆ ทั้งที่ง่ายและซับซ้อนตามคำสั่งของโปรแกรม โดยการทำงานจะประกอบด้วยขั้นตอนการรับโปรแกรมและข้อมูลในรูปแบบที่เครื่องสามารถรับได้ แล้วทำการคำนวณ เคลื่อนย้ายข้อมูล เปรียบเทียบ จนกระทั่งได้ผลลัพธ์ตามที่ต้องการ ได้แก่ Desktop Computer เป็นต้น ทั้งนี้ ให้รวมถึงอุปกรณ์ที่มีการทำงานในลักษณะเหมือนหรือคล้ายกับอุปกรณ์ที่กล่าวมาข้างต้น

(๔) “เครื่องคอมพิวเตอร์แบบพกพา” และ “อุปกรณ์สื่อสารเคลื่อนที่” หมายความว่า เครื่องคำนวณอิเล็กทรอนิกส์ที่มีการทำงานแบบอัตโนมัติ ซึ่งทำหน้าที่เหมือนสมองกล สามารถแก้ปัญหาต่างๆ ทั้งที่ง่ายและซับซ้อนตามคำสั่งของโปรแกรม โดยการทำงานจะประกอบด้วยขั้นตอนการรับโปรแกรมและข้อมูลในรูปแบบที่เครื่องสามารถรับได้ แล้วทำการคำนวณ เคลื่อนย้ายข้อมูล เปรียบเทียบ จนกระทั่งได้ผลลัพธ์ตามที่ต้องการ สามารถพกพาได้ เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) แท็บเล็ต (Tablet) คอมพิวเตอร์พกพาขนาดเล็ก (Personal Digital Assistant (PDA)) และโทรศัพท์มือถือ (Smart Phone) เป็นต้น ทั้งนี้ ให้รวมถึงอุปกรณ์ที่มีการทำงานในลักษณะเหมือนหรือคล้ายกับอุปกรณ์ที่กล่าวมาข้างต้น

(๕) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

(๖) “ความมั่นคงปลอดภัยด้านสารสนเทศ” (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(๗) “เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๘) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

(๙) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๑๐) “ผู้บริหาร” หมายความว่า อธิบดี ที่ปรึกษาฯ รองอธิบดี หรือ ผู้ซึ่งอธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านสารสนเทศของกรมศุลกากร

(๑๑) “ผู้บริหารระดับสูงสุด” หมายความว่า อธิบดีกรมศุลกากร

(๑๒) “กรม/สำนักงาน” หมายความว่า กรมศุลกากร

(๑๓) “โปรแกรมสำเร็จรูป” (software package) คือ ซอฟต์แวร์หรือโปรแกรมประยุกต์ที่มีผู้จัดทำไว้ เพื่อใช้ในการทำงานประเภทต่างๆ แต่จะไม่สามารถทำการดัดแปลงหรือแก้ไขโปรแกรมภายในได้

(๑๔) “ระบบคอมพิวเตอร์” หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรมชุดคำสั่ง (Software) ระบบเครือข่ายสื่อสาร (Communication Network System) ระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ระบบงาน (Application) ระบบสารสนเทศ (Information System) บุคลากร (People) รวมถึงอุปกรณ์ต่าง ๆ ที่สามารถกำหนด IP Address ได้

ข้อ ๓ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ประกอบด้วยเนื้อหาหลัก ๓ ส่วน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๔ ข้อปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศของกรมศุลกากรให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรมศุลกากรที่แนบท้ายประกาศนี้

ข้อ ๕ ให้ประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

ข้อ ๖ ต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๗ ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ โดยให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติอย่างน้อยปีละครั้ง

ข้อ ๘ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมศุลกากร ให้มีการควบคุมหลักในเรื่องต่อไปนี้

(๑) การใช้งานสารสนเทศ

(๒) การเข้าถึงระบบเครือข่าย

(๓) การเข้าถึงระบบปฏิบัติการ

(๔) การเข้าถึงโปรแกรมประยุกต์ (Application) และสารสนเทศ

ข้อ ๙ ในการเข้าถึงและควบคุมการใช้งานสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ซึ่งเป็นไปตามวัตถุประสงค์การใช้งานและความมั่นคงปลอดภัยที่เหมาะสม

(๒) การอนุญาตให้เข้าถึง ซึ่งเป็นไปตามข้อปฏิบัติที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ

(๓) การกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๑๐ การจัดทำข้อปฏิบัติ สำหรับการใช้งานสารสนเทศตามภารกิจ ให้คำนึงถึงเรื่องต่อไปนี้

(๑) การควบคุมการเข้าถึงสารสนเทศ

(๒) ความสอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๑๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่อง ดังนี้

(๑) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User registration)

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User management)

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

ข้อ ๑๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลัก

ขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่อง ดังนี้

(๑) การใช้รหัสผ่าน (Password use)

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

(๔) ผู้ใช้งานข้อมูลที่เป็นความลับ

ข้อ ๑๓ ในการควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่อง ดังนี้

(๑) การใช้งานบริการเครือข่าย

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks)

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

(๕) การแบ่งแยกเครือข่าย (Segregation in networks)

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control)

ข้อ ๑๔ ในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อให้การเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

(๓) การบริหารจัดการรหัสผ่าน (Password management system)

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

(๕) การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

ข้อ ๑๕ ในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and information access control) ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

(๒) การบริหารจัดการกับระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๑๖ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) การคัดเลือกและการจัดทำระบบสำรอง

(๒) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

(๓) การกำหนดหน้าที่และความรับผิดชอบของบุคลากร

(๔) การทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน

(๕) ระยะความถี่ของการปฏิบัติ

ข้อ ๑๗ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) ระยะความถี่การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๒) ตรวจสอบและประเมินความเสี่ยง

ข้อ ๑๘ การจัดหา หรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) การจัดหาระบบคอมพิวเตอร์ ระบบเครือข่าย และการพัฒนาระบบที่เกี่ยวข้องกับด้านสารสนเทศ

(๒) แนวปฏิบัติในการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม

ข้อ ๑๙ การบริหารจัดการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsource) ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) ข้อตกลงในการจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(๒) แนวปฏิบัติสำหรับผู้ให้บริการภายนอกที่กรมศุลกากรทำสัญญาว่าจ้างด้านสารสนเทศ

(๓) การกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอก

(๔) แนวทางการบริหารจัดการผู้ให้บริการภายนอก

ข้อ ๒๐ การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมศุลกากร แนบท้ายประกาศ

ข้อ ๒๑ การบริหารจัดการทรัพย์สินด้านสารสนเทศ (Asset Control)

(๑) การกำหนดอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) ของทรัพย์สินด้านสารสนเทศ

(๒) การจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศ

(๓) การดูแลรักษาพื้นที่รอบนอกศูนย์คอมพิวเตอร์ และตัวอาคารศูนย์คอมพิวเตอร์ให้มีความมั่นคงปลอดภัย

ข้อ ๒๒ ให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒๓ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้บังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม

ข้อ ๒๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ มิถุนายน พ.ศ. ๒๕๖๔ เป็นต้นไป

ประกาศ ณ วันที่ มิถุนายน พ.ศ. ๒๕๖๔

(ลงชื่อ) พชร อนันตศิลป์
(นายพชร อนันตศิลป์)
อธิบดีกรมศุลกากร

สำเนาถูกต้อง

(นายธีรยุทธ์ อารยรุ่งโรจน์)
นักวิชาการคอมพิวเตอร์ชำนาญการ

(ร่าง)
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ
กรมศุลกากร

คำนำ

การจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมศุลกากรฉบับนี้ จัดทำขึ้นตามมาตรฐานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นมาตรการและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมศุลกากรและหน่วยงานภายนอก เพื่อช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของกรมศุลกากรและหน่วยงานภายนอก ให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

กรมศุลกากร

วัตถุประสงค์

ระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูลของกรมศุลกากร เป็นระบบที่มีความสำคัญต่อการให้บริการประชาชน หน่วยงานทั้งภาครัฐและเอกชน รวมทั้งการใช้งานภายในกรมศุลกากร จึงได้มีการจัดทำแนวทางปฏิบัติ เพื่อให้ระบบสามารถใช้งานได้อย่างเหมาะสม มีประสิทธิภาพและเกิดความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ

เอกสารแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมศุลกากร จึงเป็นเอกสารที่จัดทำขึ้นเพื่อเป็นกรอบสำหรับแนวทางปฏิบัติ ที่สามารถกำหนดขั้นตอนดำเนินการในรายละเอียดได้ตลอดจนเป็นแผนการปรับปรุงที่สามารถให้ กรมศุลกากรดำเนินการให้ครอบคลุมด้านความปลอดภัยต่อไปข้างหน้า ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่น ความน่าเชื่อถือของระบบการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศภายในเครือข่ายคอมพิวเตอร์ของกรมศุลกากร ให้สามารถดำเนินงานไปได้อย่างมีประสิทธิภาพ และประสิทธิผล

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมศุลกากร เป็นไปอย่างเคร่งครัด และตะหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของกรมศุลกากร

๓. เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมศุลกากร ในการยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัย

ส่วนที่ ๑ การประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมศุลกากรต้องทำการประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้ ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

๑.๑ หนังสือเวียนภายในองค์กร

๑.๒ หนังสือเวียนภายนอกองค์กร

๑.๓ เว็บไซต์ของกรมศุลกากร

ส่วนที่ ๒ ผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมศุลกากร กำหนดให้ผู้ใช้งานเป็นผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๒.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

๒.๑.๑ ที่ปรึกษาฯ หรือ รองอธิบดี ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม

๒.๑.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ระดับบริหาร

รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

๒.๒.๑ ผู้อำนวยการสำนักงาน/กลุ่ม/กอง/ศูนย์ หรือเทียบเท่า

๒.๒.๒ นายด่านศุลกากร หรือเทียบเท่า

๒.๓ ระดับปฏิบัติ

๒.๓.๑ รับผิดชอบดูแลบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายและความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่าง ๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งการทำสำเนาข้อมูล (Back up) และกู้คืนฐานข้อมูล (Recovery) ของระบบฐานข้อมูลสารสนเทศ ข้อมูลสำหรับตัวระบบและโปรแกรมระบบ ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการส่วนพัฒนาระบบนำเข้า

(๒) ผู้อำนวยการส่วนพัฒนาระบบส่งออกและสิทธิประโยชน์

(๓) ผู้อำนวยการส่วนนวัตกรรมและคลังข้อมูล

(๔) ผู้อำนวยการส่วนแผนงานและมาตรฐาน

(๕) ผู้อำนวยการส่วนพัฒนาคอมพิวเตอร์และเครือข่าย

(๖) เจ้าหน้าที่ที่เกี่ยวข้อง

๒.๓.๒ รับผิดชอบในการอนุมัติสิทธิการเข้าใช้ระบบงาน (Applications) รวมถึงการรักษาความปลอดภัยของแต่ละระบบงานสารสนเทศ ผู้รับผิดชอบ ได้แก่

(๑) ผู้อำนวยการส่วนพัฒนาระบบนำเข้า

(๒) ผู้อำนวยการส่วนพัฒนาระบบส่งออกและสิทธิประโยชน์

(๓) ผู้อำนวยการส่วนนวัตกรรมและคลังข้อมูล

(๔) ผู้อำนวยการส่วนแผนงานและมาตรฐาน

(๕) ผู้อำนวยการส่วนพัฒนาคอมพิวเตอร์และเครือข่าย

(๖) เจ้าหน้าที่ที่เกี่ยวข้อง

ส่วนที่ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

๓.๑ กรมศุลกากรต้องระบุวัตถุประสงค์การใช้งานสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัยที่เหมาะสม โดยมีข้อปฏิบัติการเข้าถึงและการใช้งานสารสนเทศ ดังนี้

๓.๑.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๑.๒ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบฟอร์มที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนดเพื่อขอสิทธิในการเข้าระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้อำนวยการสำนักงาน/กลุ่ม/กอง/ศูนย์ หรือเทียบเท่า เพื่อการจัดเก็บไว้เป็นหลักฐาน

๓.๑.๓ เจ้าของข้อมูล และ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๑.๔ เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะต้องดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติของข้อมูล และ/หรือระบบงานที่รับผิดชอบ เพื่อให้ผู้ใช้งานสามารถนำข้อมูล หรือใช้ระบบงานได้อย่างถูกต้อง มีประสิทธิภาพ และเป็นมาตรฐานเดียวกัน

๓.๑.๕ เจ้าของข้อมูล และ เจ้าของระบบงาน ต้องบริหารจัดการข้อมูล ตั้งแต่การจัดเก็บ รวบรวมข้อมูล การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูล ต้องมีการกำหนดสิทธิ หน้าที่ ความรับผิดชอบ เพื่อควบคุมให้อยู่ในขอบเขตที่สามารถกระทำได้โดยไม่ขัดต่อกฎหมาย ระเบียบ ความลับของทางราชการ และความเป็นส่วนบุคคล อย่างเคร่งครัด

๓.๒ กรมศุลกากรต้องกำหนดสิทธิ หรือการมอบอำนาจการใช้งานสารสนเทศแต่ละชนิดเพื่อควบคุมการอนุญาตให้เข้าถึงสารสนเทศที่สำคัญ โดยมีการแบ่งแยกอำนาจหน้าที่ของบุคลากรในส่วนของงานคอมพิวเตอร์

๓.๒.๑ มีหน่วยงานควบคุมการให้สิทธิการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

๓.๒.๒ แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System administrator) ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์

๓.๒.๓ กำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

๓.๒.๔ มีบุคลากรสำรองในงานที่สำคัญเพื่อทำงานทดแทนในกรณีจำเป็น เช่น ผู้บริหารระบบ เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator) เป็นต้น

๓.๒.๕ ให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักงาน/กลุ่ม/กอง/ศูนย์/ด่าน หรือเทียบเท่า เป็นลายลักษณ์อักษร

๓.๒.๖ มีการตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที

๓.๒.๗ จัดให้มีการอนุมัติสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบเครือ และอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๒.๘ ต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ โดยมีระบบสารสนเทศที่สำคัญ ดังนี้

(๑) โปรแกรมประยุกต์ (Application)

(๒) ระบบอินเทอร์เน็ต

๓.๓ กรมศุลกากรต้องกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับสารสนเทศแต่ละชนิดอย่างเหมาะสม ดังนี้

๓.๓.๑ ประเภทของข้อมูล เช่น

(๑) ข้อมูลประเภทตัวอักษร

(๒) ข้อมูลประเภทตัวเลข

(๓) วันที่และเวลา

(๔) ข้อมูลประเภทค่าตรรกะ

๓.๓.๒ ลำดับความสำคัญ เป็นการลำดับความสำคัญของสารสนเทศตามที่หน่วยงานกำหนด ดังนี้

(๑) ความสำคัญระดับเคร่งครัด

(๒) ความสำคัญระดับกลาง

(๓) ความสำคัญระดับพื้นฐาน

๓.๓.๓ ลำดับชั้นความลับของข้อมูล ดังนี้

(๑) ลับที่สุด – หากถูกเปิดเผยจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

(๒) ลับมาก – หากเปิดเผยจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

(๓) ลับ – หากเปิดเผยจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๓.๓.๔ ระดับชั้นการเข้าถึง เช่น

(๑) การเข้าถึงเพื่อการอ่าน (Read)

(๒) การเข้าถึงเพื่อการเขียน (Write)

(๓) การเข้าถึงเพื่อแก้ไข (Edit)

(๔) การเข้าถึงเพื่อลบ (Delete)

๓.๓.๕ เวลาที่สามารถเข้าถึงได้ เช่น

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน เป็นต้น

๓.๓.๖ ช่องทางการเข้าถึงสำหรับสารสนเทศ เช่น

(๑) ผู้บริหารระบบ (Administrator) ต้องได้รับสิทธิในการเข้าใช้งานจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการกำหนด user และ password ในการเข้าใช้งานผ่านทาง Secure Shell หรือเทียบเท่าเป็นอย่างน้อย ซึ่งแยกประเภทตามความรับผิดชอบ เช่น Network Admin , System Admin , Database Admin เป็นต้น

(๒) ผู้ใช้งาน (User) ต้องมีการยืนยันตัวตน โดยต้องใส่รหัสผู้ใช้ (Username) ตามที่กำหนดและรหัสผ่าน (Password) ทุกครั้งที่มีการเปิดใช้เครื่องคอมพิวเตอร์ส่วนบุคคล หรือเครื่องคอมพิวเตอร์แบบพกพา หรือเมื่อมีการเริ่มใช้ระบบงานหรืออาจมีระบบความปลอดภัยอื่น ๆ เช่น Smart Card, Finger Print และ/หรือเทียบเท่า เป็นต้น ที่นำมาใช้ร่วมกัน เพื่อพิสูจน์ตัวตนของผู้ใช้งาน (Multi Factors Authentication)

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

๓.๔.๑ ไม่ควรกำหนดรหัสผ่านในส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

๓.๔.๒ กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน) หากระบบใด มีความจำเป็นต้องกำหนดรูปแบบรหัสผ่านเป็นอย่างอื่น จะต้องออกแบบและทดสอบให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศนั้น ๆ ทั้งนี้ต้องรายงานให้ศูนย์เทคโนโลยีสารสนเทศรับทราบด้วย

๓.๔.๓ ผู้ใช้สามารถเปลี่ยนรหัสผ่านได้ตลอดเวลา รหัสผ่านที่กำหนดใหม่แต่ละครั้ง ต้องไม่ซ้ำกับรหัสผ่านที่เคยกำหนดมาแล้วใน ๕ ครั้งล่าสุด

๓.๔.๔ กำหนดให้รหัสผ่านมีอายุการใช้งาน ๙๐ วัน นับแต่วันที่เปลี่ยนรหัสผ่านครั้งล่าสุด

๓.๔.๕ การกำหนดรหัสผ่าน การเปลี่ยนรหัสผ่าน เป็นไปตามรูปแบบที่กรมศุลกากรกำหนด เพื่อให้การเข้าใช้ระบบสารสนเทศกรมศุลกากรมีความมั่นคงปลอดภัย

๓.๕ การบริหารจัดการรหัสผ่านสำหรับผู้บริหารระบบ (Administrator password management)

๓.๕.๑ ผู้บริหารระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านที่ยากต่อการคาดเดาจากผู้อื่น

๓.๕.๒ ผู้บริหารระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๓.๕.๓ ผู้บริหารระบบต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน โดยลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วยงาน

๓.๕.๔ การส่งมอบรหัสผ่านของผู้บริหารระบบ ให้แก่ผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๓.๖ กรมศุลกากรต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยมีการแจ้งเตือนอย่างน้อยดังนี้

๓.๖.๑ มีการแจ้งเตือนให้ผู้ใช้งานทราบอย่างอัตโนมัติเมื่อเข้าสู่ระบบสำเร็จหรือเข้าสู่ระบบไม่สำเร็จ

๓.๖.๒ มีการแจ้งเตือนเมื่อผู้ใช้ระบุ รหัสผู้ใช้ หรือ รหัสผ่านไม่ถูกต้อง

๓.๖.๓ มีการแจ้งเตือนให้ผู้ใช้งานเปลี่ยนรหัส ก่อนถึงรอบระยะเวลาการเปลี่ยนรหัสผ่านที่กำหนดไว้

ส่วนที่ ๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

๔.๑ การสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยมีข้อปฏิบัติ ดังนี้

๔.๑.๑ มีคู่มือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑.๒ มีการฝึกอบรมให้ผู้ใช้งานตระหนักและเข้าใจในเรื่องภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ถูกต้องหรือไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งมาตรการการป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

๔.๒ การลงทะเบียนผู้ใช้งานและการยกเลิกสิทธิการใช้งาน (User Registration and De-Registration)

๔.๒.๑ แจ้งศูนย์งานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอรับสิทธิในการเข้าถึงระบบสารสนเทศที่เกี่ยวข้อง

๔.๒.๒ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อเกษียณอายุราชการ ลาออก หรือเมื่อเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๔.๒.๓ ผู้ใช้สามารถตั้งรหัสผ่านได้ด้วยตนเอง

๔.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๔.๓.๑ ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับ

๔.๓.๒ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา และต้องได้รับความเห็นชอบและอนุมัติจาก ผู้อำนวยการสำนักงาน/กลุ่ม/กอง/ศูนย์/นายด่าน หรือเทียบเท่า นั้นๆ

(๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น เป็นต้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๙๐ วัน เป็นต้น

๔.๓.๓ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๔ การกำหนดรหัสผ่านให้ปฏิบัติตามที่ระบุไว้ส่วนที่ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) ข้อ ๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

๔.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๕.๑ การใช้งานรหัสผ่าน (Password use)

๕.๑.๑ ต้องเก็บรักษารหัสผ่านไว้เป็นความลับ

๕.๑.๒ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๕.๑.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์หรือเครื่องมือช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

๕.๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๕.๑.๕ เมื่อเจ้าหน้าที่ของสำนักงาน/กลุ่ม/กอง/ศูนย์/ด่าน ลาออก/ไล่ออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้ผู้อำนวยการสำนักงาน/กลุ่ม/กอง/ศูนย์/นายด่าน หรือเทียบเท่า แจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทันที เพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ที่ลาออก/ไล่ออก ออกจากระบบทันทีที่ได้รับแจ้ง

๕.๑.๖ การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ส่วนที่ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) ข้อ ๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

๕.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๕.๒.๑ ผู้ใช้ต้องทำการล็อคหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพา หรือไม่อยู่ที่หน้าจอ

๕.๒.๒ ผู้ใช้ต้องทำการ Log out ออกจากระบบทันที เมื่อเลิกใช้ระบบสารสนเทศ

๕.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๕.๓.๑ การจัดการบริเวณโดยรอบ (Physical security management)

(๑) กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

(๒) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center) ให้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

(๓) มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

(๔) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้ได้ตามปกติ

(๕) บุคลากรของกรมศุลกากรต้องล็อคและปิดประตูหน้าต่างอยู่เสมอ หากไม่มีผู้ดูแล เพื่อป้องกันทรัพย์สินของกรมศุลกากร

๕.๓.๒ การควบคุมการเข้า – ออก (Physical entry controls)

(๑) ให้มีการบันทึกวันและเวลาเข้า – ออก พื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

(๒) ควบคุมสอดส่องดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) **มีกลไกการอนุญาตให้บุคคลภายนอก** ในการเข้าถึงพื้นที่ หรือบริเวณที่มีความสำคัญ

(๔) สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนด ต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๕) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๖) ไม่ให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๗) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า – ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เป็นต้น

(๘) จัดเก็บบันทึกการเข้า – ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังได้

(๙) เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้างต้องติดบัตรที่ออกโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ให้เห็นชัดตลอดระยะเวลาการทำงาน

(๑๐) ผู้ที่มาเยือนต้องติดบัตรให้เห็นชัดตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๑๑) ต้องจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๒) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๕.๓.๓ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, Delivery, and Loading areas)

(๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

(๓) จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายใน กรมศุลกากร

(๔) ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

(๕) ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สิน ของกรมศุลกากร

๕.๓.๔ การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้อง Data Center ให้น้อยที่สุด

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

(๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center)

(๔) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มี ระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่ เป็นต้น

(๕) ปิดประตูตู้ RACK สำหรับติดตั้งอุปกรณ์เครือข่ายและสัญญาณสื่อสารให้สนิท รวมถึงการล็อคประตูเพื่อป้องกันการเข้าถึงข้อมูลของบุคคลที่ไม่เกี่ยวข้อง ในกรณีไม่สามารถปิดได้ต้องดำเนินการแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

๕.๓.๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

(๑) มีการสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของกรมศุลกากรที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบต่าง ๆ เช่น

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น
- ระบบตรวจจับอัคคีไฟ
- ระบบดับเพลิง เป็นต้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้อง เครื่องทำงานผิดปกติหรือหยุดการทำงาน

๕.๓.๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling security)

(๑) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย หรือป้องกันสัตว์ต่าง ๆ กัดสาย

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๓) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๔) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๕.๓.๗ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมสอดส่องดูแลการปฏิบัติงานของผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในกรมศุลกากร

(๖) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕.๓.๘ การนำทรัพย์สินของกรมศุลกากร ออกนอกสำนักงาน (Removal of property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกกรมศุลกากร

(๒) บันทึกข้อมูลการนำอุปกรณ์ของกรมศุลกากรออกนอกกรมศุลกากรเพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๓) ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม

๕.๓.๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงกรณีการนำอุปกรณ์หรือทรัพย์สินของกรมศุลกากรออกไปใช้งานข้างนอก

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของกรมศุลกากรไว้โดยลำพังในที่สาธารณะ

(๓) จัดให้มีเจ้าหน้าที่รับผิดชอบในการควบคุมดูแลอุปกรณ์หรือทรัพย์สินที่นำออกไปใช้งานข้างนอก

๕.๓.๑๐ การจำหน่ายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะมีการจำหน่ายอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบ หรือเขียนข้อมูลทับบนข้อมูลในอุปกรณ์ก่อนที่จะอนุญาตให้จำหน่ายหรือให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลนั้นได้

๕.๔ ผู้ใช้งานข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เก็บความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย (Network access control)

๖.๑ การใช้งานบริการเครือข่ายอินเทอร์เน็ต (Use of the Internet)

๖.๑.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ที่มาใช้ระบบเครือข่ายของกรมศุลกากรต้องมีการติดตั้งโปรแกรมป้องกันไวรัส หรือทำการอุดช่องโหว่ หรือ Update ระบบปฏิบัติการของ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ให้ทันสมัยอยู่ตลอดเวลา

๖.๑.๒ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของกรมศุลกากร ไปในทางที่ไม่ถูกต้อง และผิดกฎหมาย หรือทำการเข้าเว็บไซต์ที่เป็นภัยต่อสังคม

๖.๑.๓ ผู้ใช้จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรมศุลกากร โดยผ่านความเห็นชอบจาก ผู้อำนวยการสำนักงาน/กลุ่ม/กอง/ศูนย์/นายด่าน หรือเทียบเท่า

๖.๑.๔ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมศุลกากร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๖.๑.๕ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท(Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๖.๑.๖ ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๖.๑.๗ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๖.๑.๘ การใช้งานเว็บบอร์ด (Web Board) ของกรมศุลกากรผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับของกรมศุลกากร

๖.๑.๙ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบหรือปิดเว็บบราวเซอร์ (Web Browser) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๖.๑.๑๐ผู้ใช้ต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และที่แก้ไขเพิ่มเติมอย่างเคร่งครัด

๖.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections) ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของกรมศุลกากร โดยมีแนวทางปฏิบัติ ดังนี้

๖.๒.๑ กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๖.๒.๒ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๖.๒.๓ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน

๖.๒.๔ การเข้าสู่ระบบสารเทศของกรมศุลกากรจากอินเทอร์เน็ตนั้น ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๖.๒.๕ การใช้งานอินเทอร์เน็ตเข้ามายังระบบสารเทศของกรมศุลกากร ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

๖.๒.๖ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ (เช่น เครือข่ายอินเทอร์เน็ต เป็นต้น) หรือเครือข่ายไร้สาย

๖.๒.๗ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๖.๒.๘ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๖.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks)

๖.๓.๑ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖.๓.๒ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับอนุมัติจากกรมศุลกากร และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๖.๓.๓ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๖.๓.๔ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๖.๓.๕ การบริหารจัดการ การบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๖.๓.๖ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๖.๓.๗ มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (เก็บ log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๖.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and Configuration port protection)

๖.๔.๑ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมศุลกากร ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุก

รุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๖.๔.๒ IP address ภายในของระบบงานเครือข่ายภายในของกรมศุลกากร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

๖.๔.๓ หากผู้บริหารระบบ (Administrator) จำเป็นต้องใช้งานผ่านพอร์ต ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๖.๕ การแบ่งแยกเครือข่าย (Segregation in networks)

กรมศุลกากร มีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่อสะดวกในการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ ดังนี้

๖.๕.๑ เครือข่ายภายนอก

๖.๕.๒ เครือข่ายสาธารณะ

๖.๕.๓ เครือข่ายภายในกรมศุลกากร

๖.๕.๔ เครือข่ายไร้สาย

๖.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

๖.๖.๑ ระบบเครือข่ายทั้งหมดของกรมศุลกากร ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกกรมศุลกากร ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ เป็นต้น

๖.๖.๒ ให้ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความมั่นคงปลอดภัย เช่น Proxy, Firewall, IPS/IDS เป็นต้น

๖.๖.๓ การควบคุมการเข้าถึงระบบเครือข่ายภายในของกรมศุลกากร

(๑) การเข้าสู่ระบบเครือข่ายภายในของกรมศุลกากร โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนที่จะสามารถใช้งานได้ทุกกรณี

(๒) การเข้าสู่ระบบเครือข่ายภายในกรมศุลกากร ผ่านทางอินเทอร์เน็ตต้องมีการ Login และ/หรือต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๖.๖.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

(๑) ผู้ใช้ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมศุลกากร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยแจ้งเหตุผลความจำเป็นในการใช้งาน และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๒) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบ ต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

(๔) ผู้ใช้งาน ต้องไม่ดำเนินการ ดังต่อไปนี้

(๔.๑) นำอุปกรณ์ไร้สาย มาติดตั้งหรือเปิดใช้งานเองในกรมศุลกากร เช่น Access Point, Wireless Routers, Wireless USB หรือ Wireless Card เป็นต้น

(๔.๒) เปิดระบบเครือข่ายไร้สายแบบจุดต่อจุด (Ad-Hoc) , Hotspot หรือ Peer-to-Peer Network

(๔.๓) นำรหัสผ่านที่ได้รับอนุญาตไปทำการเปิดเผยต่อผู้อื่นหรือสาธารณะ

(๔.๔) โอน จำหน่าย หรือแจกสิทธิที่ผู้ใช้งานที่ได้รับ ให้กับผู้อื่น

(๔.๕) ให้ผู้อื่นใช้งานผ่านบัญชีผู้ใช้ของตน หากเกิดปัญหาใด ๆ เจ้าของบัญชีจะต้องเป็นผู้รับผิดชอบทุกกรณี

๖.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control)

๖.๗.๑ ผู้ดูแลระบบ ต้องมีวิธีจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๖.๗.๒ ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน (Enforced Path)

๖.๗.๓ ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๖.๗.๔ กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

๗.๑ การควบคุมการเข้าถึงระบบปฏิบัติการ

๗.๑.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๗.๑.๒ ผู้ใช้ต้องกำหนดรหัสผ่านให้มีคุณภาพดี ตามปฏิบัติตามที่ระบุไว้ส่วนที่ ๔ ข้อ ๔.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๗.๑.๓ ผู้ใช้ต้องทำการล็อคหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ หรือไม่อยู่ที่หน้าจอ

๗.๑.๔ ผู้ใช้ต้องทำการ Logout ออกจากระบบสารสนเทศทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๗.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

๗.๒.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๗.๒.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

๗.๓ การบริหารจัดการรหัสผ่าน (Password management system)

ผู้ใช้สามารถกำหนดรหัสผ่านหรือเปลี่ยนรหัสผ่านได้ โดยผู้ใช้ต้องกำหนดรหัสผ่านให้มีคุณภาพตามที่ระบุไว้ในส่วนที่ ๔ ข้อ ๔.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๗.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

กำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันโปรแกรมไม่ประสงค์ดี ดังนี้

๗.๔.๑ ห้ามการติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก เว้นแต่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๗.๔.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๗.๔.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดี เช่น โปรแกรมป้องกันไวรัส เป็นต้นให้กับระบบเทคโนโลยีสารสนเทศของกรมศุลกากร

๗.๔.๔ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

๗.๔.๕ มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๗.๔.๖ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๗.๕ การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน (Session time-out)

๗.๕.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๗.๕.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

๗.๖.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งาน โดยให้ระบบยกเลิกการเชื่อมต่อ หากผู้ใช้งานไม่มีการใช้งานเกิน ๓๐ นาที

๗.๖.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกกรมศุลกากร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)

๘.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๘.๑.๑ ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ

(๑) กำหนดข้อมูลตามระดับชั้นความลับ เช่น ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน ข้อมูลความลับ เป็นต้น

(๒) ขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับต้องประกอบด้วยวิธีการประมวลผล การควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อบันทึกข้อมูล การทำป้ายบ่งชี้ และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย

(๓) ให้มีการจำกัดการเข้าถึงข้อมูลสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๔) มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

(๕) มีความตระหนัก และมาตรการป้องกันข้อมูลสำคัญที่มีการสั่งพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยผู้อื่น

(๖) จัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างน้อยปีละ ๑ ครั้ง

(๗) กรณีหน่วยงานของกรมศุลกากร มีการจ้างบุคคลภายนอก โดยทำสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงาน หรือบุคคลภายนอก ต้องส่งรายชื่อทีมงานตามสัญญาจ้าง หรือกำหนดหน้าที่ความรับผิดชอบไว้ในสัญญาจ้าง เพื่อใช้ในการกำหนดสิทธิและควบคุมการเข้าถึงระบบสารสนเทศกรมศุลกากร

๘.๑.๒ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเตอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

(๔) ให้ระมัดระวังในการนำสื่อบันทึกข้อมูล (Removable Media) ไปให้ผู้อื่นใช้งาน

๘.๑.๓ กำหนดขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

(๑) จัดทำแนวทางการใช้อย่างเหมาะสมสำหรับการใช้งานระบบหรืออุปกรณ์ที่ใช้ในการสื่อสารข้อมูลระหว่างกรมศุลกากร กับหน่วยงานภายนอก เช่น ห้ามใช้เพื่อก่อความรำคาญแก่ผู้อื่น ทำให้ผู้อื่นสูญเสียชื่อเสียง ปลอมเป็นบุคคลอื่น เป็นต้น

(๒) มีวิธีการทางเทคนิคป้องกันข้อมูลสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลงแก้ไข ถูกสวมรอยโดยผู้อื่น ถูกเปิดเผยความลับ โดยไม่ได้รับอนุญาต

(๓) จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่กรมศุลกากรต้องปฏิบัติตาม

๘.๑.๔ ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreement) จัดทำแนวทางข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างกรมศุลกากรกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูล ที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหาย หรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิการเข้าถึงข้อมูล

(๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

๘.๑.๕ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

พิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกรมศุลกากร หรือ หน่วยงานที่มาขอเชื่อมโยง มีดังต่อไปนี้

(๑) กำหนดมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๘.๑.๖ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging) จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลชื่อเทอมินัล

(๖) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๘) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (Configurations) ของระบบ

(๙) ข้อมูลแสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ

(๑๐) ข้อมูลแสดงการใช้งานแอปพลิเคชัน

(๑๑) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๒) ข้อมูลไอพีแอดเดรสที่เข้าถึง

(๑๓) ข้อมูลโปรโตคอลเครือข่ายที่ใช้

(๑๔) ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบ

(๑๕) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

(๑๖) ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญๆ

(๑๗) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๘.๒ การบริหารจัดการกับระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร

๘.๒.๑ จัดให้มีการบริหารจัดการสภาพแวดล้อมในส่วนของพื้นที่ศูนย์คอมพิวเตอร์ ดังนี้

(๑) มีกำหนดระเบียบหรือแนวการปฏิบัติในการเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์ เพื่อให้พื้นที่ศูนย์คอมพิวเตอร์มีความมั่นคงปลอดภัย

(๒) มีการควบคุมการเข้า-ออก ด้วยระบบ Hand Scan และระบบ Finger Print พร้อม ระบบ CCTV

(๓) ระบบสำรองกระแสไฟฟ้า (UPS)

(๔) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(๕) ระบบระบายอากาศ

(๖) ระบบปรับอากาศ และควบคุมความชื้น

(๗) ระบบดับเพลิง ระบบตรวจสอบควันไฟและน้ำรั่วซึม

๘.๒.๒ มีการสำรองข้อมูลและกู้คืนระบบคอมพิวเตอร์ (Backup and Recovery) ระบุไว้ในเอกสาร “แผนการสำรองข้อมูลและกู้คืนระบบคอมพิวเตอร์ (Backup and Recovery Plan) ”

๘.๒.๓ มีแผนฉุกเฉิน กรณีระบบคอมพิวเตอร์ขัดข้อง ระบุไว้ในเอกสาร “แผนฉุกเฉิน กรณีระบบเครื่องคอมพิวเตอร์ขัดข้อง”

๘.๒.๔ มีแผนฉุกเฉิน กรณีเกิดอุทกภัย หรือภัยพิบัติทางธรรมชาติ ระบุไว้ในเอกสาร “แผนฉุกเฉิน กรณีเกิดอุทกภัย หรือภัยพิบัติทางธรรมชาติ”

๘.๒.๕ ในระบบที่มีผลกระทบและความสำคัญสูงต่อกรมศุลกากร หากต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ ซึ่งมิใช่ของทรัพย์สินของกรมศุลกากรต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมศุลกากร

๘.๒.๖ มีการแยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ เช่น มีห้องปฏิบัติงานแยกเป็นสัดส่วน และกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว เป็นต้น

๘.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อดูแลรักษาความปลอดภัยในการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ดังนี้

๘.๓.๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(๑) แนวทางปฏิบัติในการใช้งานทั่วไป

(๑.๑) เครื่องคอมพิวเตอร์ที่กรมศุลกากร อนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินของ กรมศุลกากร ดังนั้น ผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่อการปฏิบัติงานในราชการของกรมศุลกากรเท่านั้น

(๑.๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของกรมศุลกากร ต้องเป็นโปรแกรมที่ กรมศุลกากร ได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๑.๓) ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งโปรแกรมและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของกรมศุลกากรเว้นแต่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(๑.๔) ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้ง ปรับปรุง ดัดแปลงอุปกรณ์ในเครื่องคอมพิวเตอร์ส่วนบุคคลของกรมศุลกากร

(๑.๕) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับ กรมศุลกากร เท่านั้น

(๑.๖) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๑.๗) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๑.๘) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๑.๙) ทำการล็อกหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๑.๑๐) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของกรมศุลกากร ยกเว้นจะได้รับการตรวจสอบจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนการใช้งาน

(๑.๑๑) ห้ามนำเครื่องคอมพิวเตอร์ที่ยังไม่ได้รับการติดตั้งโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ที่เป็นปัจจุบันเชื่อมต่อกับระบบเครือข่ายฯ ของกรมศุลกากร

(๑.๑๒) ห้ามดูภาพยนต์ ฟังเพลง เล่นเกมส์ และใช้บริการความบันเทิงต่าง ๆ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของกรมศุลกากร

(๒) แนวทางปฏิบัติในการใช้รหัสผ่าน

(๒.๑) ผู้ใช้สามารถกำหนดรหัสผ่านหรือเปลี่ยนรหัสผ่านได้ตลอดเวลา โดยผู้ใช้ต้องกำหนดรหัสผ่านให้มีคุณภาพตามที่ระบุไว้ในส่วนที่ ๔ ข้อ ๔.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

(๓) การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๓.๑) ผู้ใช้ ต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๓.๒) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

(๓.๓) ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๔) การสำรองข้อมูลและการกู้คืน

(๔.๑) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๔.๒) ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๘.๓.๒ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์สื่อสารเคลื่อนที่

(๑) แนวทางปฏิบัติการใช้งานทั่วไป

(๑.๑) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ที่กรมศุลกากรอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินของ กรมศุลกากร ดังนั้น ผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์ดังกล่าว อย่างมีประสิทธิภาพเพื่องานของกรมศุลกากร

(๑.๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ดังกล่าว ต้องเป็นโปรแกรมที่กรมศุลกากรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๑.๓) ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๑.๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรมศุลกากร เท่านั้น

(๑.๕) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๑.๖) ในกรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๑.๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๑.๘) การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๑.๙) หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินของกรมศุลกากรมาใช้กับระบบเครือข่ายของกรมศุลกากร ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนการใช้งาน

(๑.๑๐) หากมีการใช้งานโปรแกรมหรือ Web Application ที่มีลักษณะการใช้งาน Mobile Code หรือมี Script ซึ่งทำงานอัตโนมัติ เมื่อเรียกดูหรือใช้งาน ต้องมีการกำหนดค่า (Configuration) เพื่อให้การเข้าใช้ระบบสารสนเทศกรมศุลกากรมีความมั่นคงปลอดภัย

(๒) ความปลอดภัยทางด้านกายภาพ

(๒.๑) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒.๒) ผู้ใช้ต้องไม่เก็บ หรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

(๓) แนวทางปฏิบัติในการใช้งานรหัสผ่าน

(๓.๑) ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านได้ด้วยตนเอง โดยผู้ใช้ต้องกำหนดรหัสผ่านให้มีคุณภาพตามที่ระบุไว้ในส่วนที่ ๔ ข้อ ๔.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

(๔) การสำรองข้อมูลและการกู้คืน

(๔.๑) ผู้ใช้ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของกรมศุลกากร โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๔.๒) ผู้ใช้จะต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสียงต่อการรั่วไหลของข้อมูล

(๔.๓) แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔.๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๘.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในกรมศุลกากร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๘.๔.๑ ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

๘.๔.๒ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกรมศุลกากร การควบคุมบุคคลที่เข้าสู่ระบบของกรมศุลกากรจากระยะไกล จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๘.๔.๓ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๘.๔.๔ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมศุลกากร อย่างเพียงพอและต้องได้รับการอนุมัติจากกรมศุลกากร

ส่วนที่ ๙ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

กรมศุลกากร จัดให้มีระบบสำรองสำหรับระบบสารสนเทศ โดยมีข้อปฏิบัติดังนี้

๙.๑ การคัดเลือกและการจัดทำระบบสำรอง

๙.๑.๑ กำหนดระบบงานที่มีความสำคัญทั้งหมดของกรมศุลกากร

๙.๑.๒ กำหนดรายละเอียดของระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้อง เป็นต้น

๙.๑.๓ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง

๙.๑.๔ กำหนด วิธีการสำรอง (เช่น แบบ Full Backup หรือ Incremental Backup) ของระบบงานที่มีความสำคัญเหล่านั้น

๙.๑.๕ เตรียมอุปกรณ์ที่จำเป็นต่อการสำรองข้อมูล และการกู้คืนข้อมูล

๙.๑.๖ ทำการสำรองข้อมูลตามชนิด ความถี่ และ วิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

๙.๑.๗ ต้องนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่และ/หรือศูนย์คอมพิวเตอร์สำรองอย่างน้อย ๑ ชุด

๙.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๙.๒.๑ ระบุวัตถุประสงค์หลักของแผนเตรียมความพร้อมกรณีฉุกเฉิน

๙.๒.๒ จัดทำบัญชีรายชื่อของระบบงานที่มีความสำคัญ รวมทั้งปรับปรุงบัญชีรายชื่อดังกล่าวให้มีความทันสมัยอยู่เสมอ

๙.๒.๓ กำหนดปัจจัยเสี่ยงและภัยพิบัติที่อาจส่งผลกระทบกับระบบงานที่มีความสำคัญ และกำหนดมาตรการ เพื่อลดความเสี่ยงที่พบ เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๙.๒.๔ ประเมินสถานการณ์ความเสียงด้านสารสนเทศ

๙.๒.๕ จัดทำแผนกู้คืนเพื่อรับมือกับสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) การกำหนดหน้าที่ความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

(๒) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(๓) การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย

(๔) ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ เช่น ไฟไหม้

๙.๒.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๙.๒.๗ ให้ทำการปรับปรุงแผนกู้คืนอย่างน้อยปีละ ๑ ครั้ง

๙.๒.๘ ให้จัดประชุม และ แจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้งเมื่อมีการปรับปรุงแผนกู้คืนใหม่จะต้องจัดประชุมใหม่ และ แจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

๙.๓ การกำหนดหน้าที่และความรับผิดชอบของบุคลากร

กรมศุลกากรกำหนดหน้าที่ความรับผิดชอบในการสำรองและกู้คืนระบบคอมพิวเตอร์ ระบุไว้ในเอกสาร “แผนการสำรองและกู้คืนระบบคอมพิวเตอร์ (Backup and Recovery Plan)”

๙.๔ การทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมฉุกเฉิน

๙.๔.๑ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

๙.๔.๒ ให้ทำการตรวจสอบกู้คืนข้อมูลที่สำรองไว้นั้น ว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และ บันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีแก้ไขอย่างเป็นลายลักษณ์อักษร

๙.๕ ระยะความถี่ของการปฏิบัติ

๙.๕.๑ ระยะความถี่การสำรองข้อมูลของระบบงานขึ้นอยู่กับความสำคัญของระบบและสภาพความเปลี่ยนแปลงของระบบงานนั้น ๆ เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๙.๕.๒ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ และความพร้อมในการใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๙.๕.๓ ให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐ การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical Access and Environmental Security)

กรมศุลกากรจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล โดยกลุ่มตรวจสอบภายในของกรมศุลกากรอย่างน้อยปีละ ๑ ครั้ง และในการตรวจสอบและประเมินความเสี่ยง มีสิ่งที่ต้องคำนึงถึง ดังนี้

๑๐.๑ จัดลำดับความสำคัญของความเสี่ยง

๑๐.๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

๑๐.๓ ข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

๑๐.๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๑๐.๕ ในการตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยให้ครอบคลุมหัวข้ออย่างน้อยต่อไปนี้

๑๐.๕.๑ การตรวจสอบและประเมินด้านการบริหารสินทรัพย์ด้านสารสนเทศ

๑๐.๕.๒ การตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

๑๐.๕.๓ การตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการปฏิบัติการ

๑๐.๕.๔ การตรวจสอบและประเมินการควบคุมการเข้าถึง

๑๐.๕.๕ การตรวจสอบและประเมินด้านการพัฒนาระบบ จัดซื้อจัดหาระบบและการดูแลระบบ

๑๐.๕.๖ การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์

ส่วนที่ ๑๑ การจัดหา หรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

การจัดหาหรือการจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศของกรมศุลกากรให้ปฏิบัติดังนี้

๑๑.๑ การจัดหาระบบคอมพิวเตอร์ ระบบเครือข่าย และการพัฒนาระบบที่เกี่ยวข้องกับด้านสารสนเทศทั้งในส่วนการจัดหาใหม่และการปรับปรุงระบบเดิม ให้ทุกหน่วยงานต้องประสานงานหรือหารือกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนทุกครั้ง เพื่อพิจารณาให้ความเห็นเกี่ยวกับการดำเนินการ

ดังกล่าว ทั้งในด้านความมั่นคงปลอดภัย และความสอดคล้องกับโครงสร้างพื้นฐานและเครือข่ายของกรมศุลกากร ก่อนนำเสนอพิจารณาอนุมัติจัดหาและพัฒนา

๑๑.๒ ในการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้ปฏิบัติดังนี้

๑๑.๒.๑ มีข้อตกลงระดับการให้บริการ (Service-level Agreement : SLA) ที่เหมาะสมและเป็นประโยชน์ต่อกรมศุลกากร เพื่อให้ได้รายผู้รับจ้างที่มีความสามารถ และมีประสบการณ์

๑๑.๒.๒ ผู้รับจ้างต้องไม่เปิดเผยข้อมูลใด ๆ ไม่ว่าจะอยู่ในลักษณะ และรูปแบบใด รวมถึงจะต้องเก็บรักษาข้อความ และข้อมูลที่ได้จากการปฏิบัติงามตามสัญญาจ้าง โดยจะไม่เปิดเผยแก่บุคคลใด ๆ และจะไม่กระทำการ หรือร่วมกับบุคคลอื่นใดกระทำการคัดลอก เลียนแบบ สำเนาบันทึก แก้ไข ดัดแปลง ไม่ว่าโดยวิธีใด ๆ ตลอดระยะเวลาการปฏิบัติงานตามสัญญาจ้างและแม้ภายหลังสิ้นสุดระยะเวลาตามสัญญาจ้างแล้วก็ตามอย่าเคร่งครัด

๑๑.๒.๓ ต้องมีข้อกำหนดในการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน เพื่อป้องกันและสร้างความมั่นใจว่าข้อมูลที่ได้รับจากการแลกเปลี่ยนข้อมูลเป็นข้อมูลที่ถูกต้องแท้จริง มาจากผู้ส่งที่ถูกต้อง และไม่ถูกแก้ไขระหว่างทางหรือถูกแก้ไขโดยผู้ไม่มีสิทธิ์

๑๑.๒.๔ ต้องมีกระบวนการควบคุม ติดตามการเปลี่ยนแปลง ติดตั้ง แก้ไข ซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งาน (Software package) โดยคำขอให้แก้ไขต้องมาจากผู้ดูแลระบบและต้องเป็นการแก้ไขเท่าที่จำเป็น โดยต้องได้รับการอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และการขอแก้ไขนั้นต้องมีการทดสอบแล้วว่าผลของการเปลี่ยนแปลงดังกล่าว จะไม่ส่งผลกระทบใด ๆ ต่อความมั่นคงปลอดภัยของระบบสารสนเทศและการให้บริการของหน่วยงาน

๑๑.๒.๕ กรณีที่มีการจ้างพัฒนาซอฟต์แวร์กับผู้รับจ้าง และผู้รับจ้างมีการจ้างผู้รับจ้างช่วง (Subcontractor) ผู้รับจ้างช่วง จะต้องปฏิบัติตามข้อกำหนดเช่นเดียวกับที่ผู้รับจ้างได้ทำข้อตกลงไว้กับกรมศุลกากรทุกประการ

๑๑.๒.๖ การพัฒนาระบบงานที่ให้บริการผ่านอินเทอร์เน็ตต้องมีการเข้ารหัสข้อมูล หรือ มีการนำเทคนิคการบริหารจัดการกุญแจ (Key Management) เพื่อใช้ในการพิสูจน์ตัวตนสำหรับการเข้าใช้ระบบงาน ไม่อนุญาตให้นำข้อมูลสำคัญของกรมศุลกากร ไปใช้ในการทดสอบกับระบบงาน เว้นแต่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ เพื่อเป็นการป้องกันการรั่วไหลของข้อมูล

๑๑.๒.๗ มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของกรมศุลกากร โดยให้มีการควบคุม กำกับ ติดตาม ให้ครอบคลุมตลอดวงจรชีวิตของกุญแจ (Key Management) ได้แก่ การสร้างกุญแจรหัสลับ การจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ การเพิกถอนกุญแจรหัสลับหรือการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

๑๑.๒.๘ ต้องมีการจำกัดสิทธิการเข้าถึงชุดคำสั่งในการเขียนโปรแกรม (Source Code) ของระบบที่ใช้งานจริง และควรเก็บไว้ในที่ปลอดภัยเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๑.๒.๙ ต้องมีการตรวจสอบ (Validate) ข้อมูลใด ๆ ที่จะรับเข้าสู่แอปพลิเคชันก่อนเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม

๑๑.๒.๑๐ ต้องมีการดำเนินการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลมาจากการประมวลผลของแอปพลิเคชัน ร่วมกันระหว่างผู้พัฒนาระบบและผู้ใช้ เพื่อให้มั่นใจได้ว่าข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม

๑๑.๒.๑๑ ต้องมีการตรวจสอบ (Validate) การทำงานของแอปพลิเคชันเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด

๑๑.๒.๑๒ มีแนวทางในการเลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้สำหรับการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

ส่วนที่ ๑๒ การบริหารจัดการผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsource)

๑๒.๑ ผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsource) ที่กรมศุลกากรทำสัญญาว่าจ้าง ที่เข้ามาดำเนินงานภายในกรมศุลกากรในการจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ จะต้องไม่เปิดเผยข้อมูลใด ๆ (Non-Disclosure Agreement) ไม่ว่าจะอยู่ในลักษณะ และรูปแบบใด รวมถึงจะต้องเก็บรักษาข้อความ และข้อมูลที่ได้จากการปฏิบัติงามตามสัญญาจ้าง โดยจะไม่เปิดเผยแก่บุคคลใด ๆ และจะไม่กระทำการ หรือร่วมกับบุคคลอื่นใดกระทำการคัดลอก เลียนแบบ สำเนาบันทึก แก้ไข ดัดแปลง ไม่ว่าโดยวิธีใด ๆ ตลอดระยะเวลาการปฏิบัติงานตามสัญญาจ้างและแม้ภายหลังสิ้นสุดระยะเวลาตามสัญญาจ้างแล้วก็ตามอย่างเคร่งครัด

๑๒.๒ ผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsource) ที่กรมศุลกากรทำสัญญาว่าจ้างด้านสารสนเทศ ให้ดำเนินการดังนี้

๑๒.๒.๑ ในระดับองค์กร

(๑) ผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsource) ที่กรมศุลกากรทำสัญญาว่าจ้าง ให้เข้ามาดำเนินกิจกรรมภายในกรมศุลกากรในงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องผ่านการตรวจสอบคุณสมบัติของผู้ที่จะเข้ามาปฏิบัติงาน โดยมีการตรวจสอบประวัติอาชญากรรมของเจ้าหน้าที่ จากสำนักงานตำรวจแห่งชาติส่งผลการตรวจมาให้กรมศุลกากร

(๒) ให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่กรมศุลกากร ต้องปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะ การให้บริการ ระดับการให้บริการ ลิขสิทธิ์และกฎหมายที่เกี่ยวข้อง

(๓) ผู้ดูแลระบบหรือเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมาย ต้องกำกับดูแลการปฏิบัติงานของให้บริการภายนอกที่กรมศุลกากรทำสัญญาว่าจ้าง (Outsource) โดยเคร่งครัด

๑๒.๒.๒ ในระดับบุคคล

(๑) บุคคลภายนอกที่เข้ามาในศูนย์คอมพิวเตอร์ กรมศุลกากร ให้แสดงบัตรประจำตัวประชาชน หรือบัตรที่หน่วยงานราชการออกให้ เพื่อบันทึกการเข้า-ออกไว้เป็นหลักฐาน และแลกบัตรผู้มาติดต่อเพื่อผ่านเข้า-ออก ศูนย์คอมพิวเตอร์ กรมศุลกากร

(๒) บุคคลภายนอกต้องติดบัตรผู้มาติดต่อเพื่อเข้า-ออกศูนย์คอมพิวเตอร์ กรมศุลกากร ตลอดเวลาที่อยู่ในศูนย์คอมพิวเตอร์ กรมศุลกากร

๑๒.๓ ต้องมีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ

๑๒.๔ ต้องมีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอกระดับองค์กร โดยต้องมีการระบุข้อกำหนดในสัญญาจ้าง ว่าผู้ให้บริการภายนอกจะต้องไม่เปิดเผยข้อมูลใด ๆ (Non-Disclosure Agreement) ไม่ว่าจะอยู่ในลักษณะ และรูปแบบใด รวมถึงจะต้องเก็บรักษาข้อความ และข้อมูลที่ได้จากการปฏิบัติงามตามสัญญาจ้าง โดยจะไม่เปิดเผยแก่บุคคลใด ๆ และจะไม่กระทำการ หรือร่วมกับบุคคลอื่นใดกระทำการคัดลอก เลียนแบบ สำเนาบันทึก แก้ไข ดัดแปลง ไม่ว่าโดยวิธีใด ๆ ตลอดระยะเวลาการปฏิบัติงานตามสัญญาจ้างและแม้ภายหลังสิ้นสุดระยะเวลาตามสัญญาจ้างแล้วก็ตามอย่าเคร่งครัด

ส่วนที่ ๑๓ การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)

๑๓.๑ การร้องขอให้มีการเปลี่ยนแปลง

๑๓.๑.๑ ก่อนดำเนินการเปลี่ยนแปลงระบบสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือฐานข้อมูล โดยผู้ดูแลระบบ หรือผู้ให้บริการภายนอก ผู้ร้องขอต้องกรอกรายละเอียดลงในแบบคำขอเปลี่ยนแปลง (Change Request Form) โดยผ่านการอนุมัติจากผู้มีอำนาจตามขั้นตอนการปฏิบัติการบริหารจัดการการเปลี่ยนแปลง เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของบริการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

๑๓.๑.๒ การอนุมัติการเปลี่ยนแปลงต้องปฏิบัติตามขั้นตอนการปฏิบัติงานบริหารการเปลี่ยนแปลง

๑๓.๑.๓ การเปลี่ยนแปลงระบบงาน จะต้องปรับปรุงคู่มือในการใช้งานหรือคู่มือในการอบรมผู้ใช้งาน เมื่อการขอเปลี่ยนแปลงแก้ไขในครั้งนั้น ๆ มีผลต่อคู่มือฉบับเดิม

๑๓.๒ การกำหนดหน้าที่การเปลี่ยนแปลง

๑๓.๒.๑ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน

๑๓.๒.๒ ก่อนที่จะมีการอนุมัติต้องประเมินผลกระทบและความเสี่ยง รวมถึงทำการทดสอบเบื้องต้น

๑๓.๓ การเปลี่ยนแปลงฮาร์ดแวร์คอมพิวเตอร์และสื่อที่ใช้ในการจัดเก็บข้อมูล

๑๓.๓.๑ การเปลี่ยนแปลงฮาร์ดแวร์คอมพิวเตอร์ และสื่อที่ใช้ในการจัดเก็บข้อมูลจะต้องได้รับอนุมัติจากผู้มีอำนาจตามขั้นตอนการปฏิบัติการบริหารจัดการการเปลี่ยนแปลงเพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการให้บริการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๑๓.๓.๒ การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลตามระดับชั้นความลับของข้อมูล

๑๓.๔ การเปลี่ยนแปลงระบบเครือข่าย และระบบรักษาความปลอดภัย

๑๓.๔.๑ การเปลี่ยนแปลงระบบเครือข่าย และระบบรักษาความปลอดภัยจะต้องได้รับอนุมัติจากผู้มีอำนาจตามขั้นตอนการปฏิบัติการบริหารจัดการการเปลี่ยนแปลง เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการให้บริการ หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

๑๓.๔.๒ การเปลี่ยนแปลงใด ๆ ของระบบเครือข่าย และระบบรักษาความปลอดภัยของกรมศุลกากร ต้องปฏิบัติตามคู่มือที่กำหนดไว้

๑๓.๔.๓ ผู้ดูแลระบบจะต้องทำบันทึกข้อมูลของระบบเก่าเก็บไว้ เพื่อใช้แก้ปัญหาในการนำระบบเก่ามาใช้ในกรณีที่ระบบใหม่เกิดปัญหา

๑๓.๔.๔ ผู้ดูแลระบบจะต้องบันทึกข้อมูลที่มีการเปลี่ยนแปลงต่าง ๆ ไว้เป็นหลักฐาน

๑๓.๕ การเปลี่ยนแปลง Source Code

๑๓.๕.๑ Source Code ที่ใช้งานจริงต้องมีการจัดเก็บอย่างเป็นระบบตามขั้นตอนการปฏิบัติการจัดระดับชั้นความลับของข้อมูลและมีการควบคุมเวอร์ชัน

๑๓.๕.๒ การเปลี่ยนแปลงแก้ไข Source Code ต้องดำเนินการบนระบบทดสอบโดยแยกจากระบบที่ใช้งานจริงเท่านั้น

๑๓.๕.๓ Source Code ที่พร้อมใช้งาน หรือ Source Code ที่ได้รับจากระบบเครือข่ายภายนอกที่ไม่น่าเชื่อถือต้องผ่านการตรวจสอบจากหน่วยงานที่รับผิดชอบ ถึงจะสามารถโอนย้ายไปยังส่วนที่ใช้งานจริงโดยผู้ที่ได้รับอนุญาตเท่านั้น

๑๓.๖ การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์บริหารจัดการระบบฐานข้อมูล ซอฟต์แวร์สำเร็จรูป และซอฟต์แวร์ประยุกต์

๑๓.๖.๑ ไม่ดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์บริหารจัดการระบบฐานข้อมูล ซอฟต์แวร์สำเร็จรูป และซอฟต์แวร์ประยุกต์หากจำเป็นต้องดำเนินการเปลี่ยนแปลงแก้ไข ให้ขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลง แก้ไข หรือมอบหมายให้ผู้ขายดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์บริหารจัดการระบบฐานข้อมูล ซอฟต์แวร์สำเร็จรูป และซอฟต์แวร์ประยุกต์ให้

๑๓.๖.๒ ก่อนการเปลี่ยนแปลงซอฟต์แวร์บริหารจัดการระบบฐานข้อมูล ซอฟต์แวร์สำเร็จรูป และซอฟต์แวร์ประยุกต์ ให้หน่วยงานที่รับผิดชอบทำการสำรองซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง

๑๓.๖.๓ ซอฟต์แวร์บริหารจัดการระบบฐานข้อมูล ซอฟต์แวร์สำเร็จรูป และซอฟต์แวร์ประยุกต์ที่แก้ไขจะต้องได้รับการทดสอบและตรวจสอบถึงผลกระทบและความเสี่ยงที่อาจเกิดขึ้นก่อนการนำมาใช้งาน

๑๓.๗ การทดสอบ

๑๓.๗.๑ ผู้ที่ร้องขอและผู้ดูแลระบบ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

๑๓.๗.๒ ในระบบงานสำคัญควรมีการตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบก่อนที่จะโอนย้ายไปใช้งานจริง

๑๓.๗.๓ การทดสอบหลังการใช้งาน (post-implementation test) ต้องกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน

๑๓.๗.๔ ต้องมีการสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง เพื่อให้สามารถใช้งานได้อย่างถูกต้อง

ส่วนที่ ๑๔ การบริหารจัดการทรัพย์สินด้านสารสนเทศ (Asset Control)

๑๔.๑ ทรัพย์สินด้านสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) หรือไม่คุ้มค่าใช้จ่ายในการซ่อมแซมบำรุงรักษา ให้ปฏิบัติตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ หรือตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

๑๔.๒ มีการจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศของศูนย์เทคโนโลยีสารสนเทศให้ครอบคลุมทั้งอุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์ โดยอย่างน้อยต้องมีในเรื่องดังต่อไปนี้

๑๔.๒.๑ ชื่อเครื่องแม่ข่าย, ชื่อระบบปฏิบัติการ (operating system) และเวอร์ชัน หรือชื่อระบบงาน (application) และเวอร์ชัน

๑๔.๒.๒ เจ้าของทรัพย์สิน (owner)

๑๔.๒.๓ ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (specification)

๑๔.๒.๔ หมายเลขอ้างอิงของฮาร์ดแวร์ (serial number) และหมายเลขอ้างอิงของซอฟต์แวร์ (software license)

๑๔.๒.๕ สถานที่ตั้ง วันที่เริ่มติดตั้ง ประเภทการครอบครอง (ซื้อหรือเช่า)

๑๔.๒.๖ รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา วันที่บำรุงรักษาล่าสุด

๑๔.๒.๗ วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (support contract)

๑๔.๒.๘ วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

๑๔.๓ การจัดทำทะเบียนทรัพย์สินต้องมีการปรับปรุงทะเบียนทรัพย์สินเมื่อผู้ใช้งานพ้นสภาพการเป็นผู้ปฏิบัติงานภายในกรมศุลกากรหรือหากต้องการยกเลิกสิทธิการครอบครองทรัพย์สินจะต้องส่งคืนทรัพย์สินให้กรมศุลกากร

๑๔.๔ มีการติดตั้งระบบ CCTV เพื่อตรวจสอบ และดูแลรักษาพื้นที่รอบนอกศูนย์คอมพิวเตอร์ และตัวอาคารศูนย์คอมพิวเตอร์ให้มีความมั่นคงปลอดภัย เพื่อป้องกันการบุกรุก การลักขโมย เหตุการณ์ไฟไหม้ น้ำท่วม ลักลอบขโมยสายไฟฟ้า มิเตอร์ เพื่อทำลายสาธารณูปโภคให้มีปัญหา พร้อมกับกำหนดสิทธิผู้มีหน้าที่ปฏิบัติงานภายในอาคาร และสำหรับผู้ติดต่อประสานงาน การเข้า-ออก และมีการบันทึกข้อมูลไว้เป็นหลักฐาน สามารถตรวจสอบย้อนหลังได้ไม่น้อยกว่า ๓๐ วัน

๑๔.๕ สื่อบันทึกข้อมูลต่าง ๆ ในลักษณะ Removable media เช่น Thumb drive, External hard disk ที่มีข้อมูลสารสนเทศที่สำคัญ ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือ สถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (Clear Desk)

๑๔.๖ ต้องมีการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (Clear screen) เช่น การตัดออกจากระบบ (Session time out) และการล็อคหน้าจอ (Lock screen)