

นางศรีชา มงคลไชยสิทธิ์
(นางศรีชา มงคลไชยสิทธิ์)ผู้อำนวยการส่วนเลขานุการกรม ปฏิบัติราชการแทน
อธิบดีกรมศุลกากร

(สำเนา)

ประกาศกรมศุลกากร

(นายเจษฎา อริยวัตรกุล)

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๕

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล อธิบดีกรมศุลกากรโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมศุลกากร เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๕”

ข้อ ๒ ในประกาศนี้

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

(๒) “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรมศุลกากร

(๓) “สินทรัพย์” (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับกรมศุลกากร

(๔) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

(๕) “ความมั่นคงปลอดภัยด้านสารสนเทศ” (information security) หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

(๖) “เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

(๘) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(๙) “ผู้บริหาร” หมายความว่า อธิบดี รองอธิบดี หรือ ผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของกรมศุลกากร

(๑๐) “กรม/สำนักงาน” หมายความว่า กรมศุลกากร

ข้อ ๓ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ ประกอบด้วยเนื้อหาหลัก ๓ ส่วน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๔ ข้อปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศของกรมศุลกากรให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากรที่แนบท้ายประกาศนี้

ข้อ ๕ ให้ประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

ข้อ ๖ ต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๗ ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ โดยให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติอย่างน้อยปีละครั้ง

ข้อ ๘ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมศุลกากร ให้มีการควบคุมหลักในเรื่องต่อไปนี้

(๑) การใช้งานสารสนเทศ

(๒) การเข้าถึงระบบเครือข่าย

(๓) การเข้าถึงระบบปฏิบัติการ

(๔) การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

ข้อ ๙ ในการเข้าถึงและควบคุมการใช้งานสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 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 ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนบท้ายประกาศในเรื่องดังนี้

(๑) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและ

ผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ 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 และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนวนโยบายประกาศในเรื่องดังนี้

- (๑) การใช้รหัสผ่าน (Password use)
- (๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์
- (๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์
- (๔) ผู้ใช้งานข้อมูลที่เป็นความลับ

ข้อ ๑๓ ในการควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนวนโยบายประกาศในเรื่องดังนี้

- (๑) การใช้งานบริการเครือข่าย
- (๒) การยืนยันตัวตนบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (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 ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนวนโยบายประกาศในเรื่องดังนี้

- (๑) การกำหนดขั้นตอนปฏิบัติเพื่อให้การเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย
- (๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)
- (๓) การบริหารจัดการรหัสผ่าน (Password management system)
- (๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)
- (๕) การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน
- (๖) การจำกัดระยะเวลาการเชื่อมต่อบนระบบสารสนเทศ (Limitation of connection time)

ข้อ ๑๕ ในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control) ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนวนโยบายในเรื่องดังนี้

- (๑) การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)
- (๒) การบริหารจัดการกับระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร
- (๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่
- (๔) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๑๖ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนวนโยบายในเรื่องดังนี้

- (๑) การคัดเลือกและการจัดทำระบบสำรอง
- (๒) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
- (๓) การกำหนดหน้าที่และความรับผิดชอบของบุคลากร
- (๔) การทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อม

กรณีฉุกเฉิน

- (๕) ระยะเวลาของการปฏิบัติ

ข้อ ๑๗ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กรมศุลกากร แนวนโยบายในเรื่องดังนี้

- (๑) ระยะเวลาการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
- (๒) ผู้ตรวจสอบและประเมินความเสี่ยง


ข้อ ๑๘ ให้ผู้บริหารเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องลงเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๙ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๒๗ กรกฎาคม พ.ศ. ๒๕๕๕ เป็นต้นไป

ประกาศ ณ วันที่ ๒๗ กรกฎาคม พ.ศ. ๒๕๕๕

(ลงชื่อ) สมชาย พูลสวัสดิ์
(นายสมชาย พูลสวัสดิ์)
อธิบดีกรมศุลกากร

สำเนาถูกต้อง


(นายพรวิทย์ อุทัยรัฐนิกุล)

นักวิชาการคอมพิวเตอร์ ชำนาญการ

แนวปฏิบัติการรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศ
กรมศุลกากร

คำนำ

การจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของกรมศุลกากรฉบับนี้ จัดทำขึ้นตามมาตรฐานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นมาตรการและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมศุลกากรและหน่วยงานภายนอก โดยช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของกรมศุลกากรและหน่วยงานภายนอก ให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

กรมศุลกากร

๒๗ กรกฎาคม ๒๕๕๕

วัตถุประสงค์

ระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูลของกรมศุลกากร เป็นระบบที่มีความสำคัญต่อการให้บริการประชาชน หน่วยงานทั้งภาครัฐและเอกชน รวมทั้งการใช้งานภายในกรมศุลกากร จึงได้มีการจัดทำแนวทางปฏิบัติ เพื่อให้ระบบสามารถใช้งานได้อย่างเหมาะสม มีประสิทธิภาพและเกิดความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ

เอกสารแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมศุลกากร จึงเป็นเอกสารที่จัดทำขึ้นเพื่อเป็นกรอบสำหรับแนวทางปฏิบัติ ที่สามารถกำหนดขั้นตอนดำเนินการในรายละเอียดได้ตลอดจนเป็นแผนการปรับปรุงที่สามารถให้ กรมศุลกากรดำเนินการให้ครอบคลุมด้านความมั่นคงปลอดภัยต่อไปข้างหน้า ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่น และมีระบบการรักษาความมั่นคงปลอดภัยการใช้งานในระบบเทคโนโลยีสารสนเทศในเครือข่ายคอมพิวเตอร์ของกรมศุลกากร ให้ดำเนินงานไปได้อย่างมีประสิทธิภาพ และประสิทธิผล

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้มีส่วนเกี่ยวข้องได้แก่ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมศุลกากร เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของกรมศุลกากร

๓. เพื่อเป็นกรอบและแนวทางการปรับปรุงพัฒนาระบบเทคโนโลยีสารสนเทศ การสื่อสารข้อมูลของกรมศุลกากร ยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัย

ส่วนที่ ๑ การประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมศิลปากรต้องทำการประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้ ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

๑. หนังสือเวียนภายในองค์กร
๒. หนังสือเวียนภายนอกองค์กร
๓. Website ของกรมศิลปากร

ส่วนที่ ๒ ผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมศิลปากร กำหนดให้ผู้ใช้งานเป็นผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

- (๑) รองอธิบดี ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำกรมศิลปากร
- (๒) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๒. ระดับบริหาร

รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวน วางแผน ติดตาม การบริหาร ความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

- (๑) ผู้อำนวยการสำนัก/กลุ่ม
- (๒) ผู้อำนวยการสำนักงาน
- (๓) นายด้านศิลปากร

๓. ระดับปฏิบัติ

๓.๑. รับผิดชอบดูแลบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายและความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ซ่อมอุปกรณ์ต่างๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งการทำสำเนาข้อมูล (Back up) และกู้คืนฐานข้อมูล (Recovery) ของระบบฐานข้อมูลสารสนเทศ ข้อมูลสำหรับตัวระบบและโปรแกรมระบบ ผู้รับผิดชอบ ได้แก่

- (๑) ผู้อำนวยการส่วนพัฒนาระบบนำเข้า
- (๒) ผู้อำนวยการส่วนพัฒนาระบบส่งออกและสิทธิประโยชน์
- (๓) ผู้อำนวยการส่วนประมวลผลและคลังข้อมูล
- (๔) ผู้อำนวยการส่วนแผนงานและมาตรฐาน
- (๕) ผู้อำนวยการส่วนพัฒนาคอมพิวเตอร์และเครือข่าย
- (๖) เจ้าหน้าที่ที่เกี่ยวข้อง

๓.๒. รับผิดชอบในการอนุมัติสิทธิการเข้าใช้ระบบงาน (Applications) รวมถึงการรักษาความ ปลอดภัยของแต่ละระบบงานสารสนเทศ ผู้รับผิดชอบ ได้แก่

- (๑) ผู้อำนวยการส่วนพัฒนาระบบนำเข้า
- (๒) ผู้อำนวยการส่วนพัฒนาระบบส่งออกและสิทธิประโยชน์
- (๓) ผู้อำนวยการส่วนประมวลผลและคลังข้อมูล
- (๔) ผู้อำนวยการส่วนแผนงานและมาตรฐาน
- (๕) ผู้อำนวยการส่วนพัฒนาคอมพิวเตอร์และเครือข่าย

(๖) เจ้าหน้าที่ที่เกี่ยวข้อง

ส่วนที่ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๑. กรมศุลกากรต้องระบุวัตถุประสงค์การใช้งานสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูล และอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัยที่เหมาะสม โดยมีข้อปฏิบัติการเข้าถึงและการใช้งานสารสนเทศ ดังนี้

๑.๑. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๒. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นบันทึกและกรอกแบบฟอร์มที่สำนักเทคโนโลยีสารสนเทศและการสื่อสารกำหนดเพื่อขอสิทธิ์ในการเข้าระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้อำนวยการสำนัก/กลุ่ม เพื่อการจัดเก็บไว้เป็นหลักฐาน

๑.๓. เจ้าของข้อมูล และ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

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

๒. กรมศุลกากรต้องกำหนดสิทธิ์ หรือการมอบอำนาจการใช้งานสารสนเทศแต่ละชนิดเพื่อควบคุมการอนุญาตให้เข้าถึงสารสนเทศที่สำคัญ โดยมีการแบ่งแยกอำนาจหน้าที่ของบุคลากรในส่วนของงานคอมพิวเตอร์

๒.๑. มีหน่วยงานควบคุมการให้สิทธิการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

๒.๒. แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System administrator) ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์

๒.๓. กำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

๒.๔. มีบุคลากรสำรองในงานที่สำคัญเพื่อทำงานทดแทนในกรณีจำเป็น เช่น ผู้บริหารระบบเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator)

๒.๕. ให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้อำนวยการสำนัก/กลุ่ม เป็นลายลักษณ์อักษร

๒.๖. มีการตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที

๒.๗ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒.๘. ต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ โดยมีระบบสารสนเทศที่สำคัญ ดังนี้

(๑) ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application)

(๒) จดหมายอิเล็กทรอนิกส์ (e-mail)

(๓) ระบบอินเทอร์เน็ต

๓. กรมศุลกากรต้องกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสำหรับสารสนเทศแต่ละชนิดอย่างเหมาะสม ดังนี้

๓.๑ ประเภทของข้อมูล เช่น

(๑) ข้อมูลประเภทตัวอักษร

(๒) ข้อมูลประเภทตัวเลข

(๓) วันที่และเวลา

(๔) ข้อมูลประเภทค่าตรรกะ

๓.๒ ลำดับความสำคัญ เป็นการลำดับความสำคัญของสารสนเทศตามที่หน่วยงานกำหนด ดังนี้

(๑) ความสำคัญระดับเร่งด่วน

(๒) ความสำคัญระดับกลาง

(๓) ความสำคัญระดับพื้นฐาน

๓.๓ ลำดับชั้นความลับของข้อมูล เช่น

(๑) ลับที่สุด - หากถูกเปิดเผยจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

(๒) ลับมาก - หากเปิดเผยจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

(๓) ลับ - หากเปิดเผยจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๓.๔ ระดับชั้นการเข้าถึง เช่น

(๑) การเข้าถึงเพื่อการอ่าน (Read)

(๒) การเข้าถึงเพื่อการเขียน (Write)

(๓) การเข้าถึงเพื่อแก้ไข (Edit)

(๔) การเข้าถึงเพื่อลบ (Delete)

๓.๕ เวลาได้เข้าถึง

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๓.๖ ช่องทางการเข้าถึงสำหรับสารสนเทศ เช่น

(๑) ผู้บริหารระบบ (Administrator) ต้องได้รับสิทธิ์ในการเข้าใช้งานจากสำนักเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการกำหนด user และ password ในการเข้าใช้งาน โดยผ่าน ทาง Secure Shell ซึ่งแยกประเภทตามความรับผิดชอบ เช่น Network Admin , System Admin , Database Admin เป็นต้น

(๒) ผู้ใช้งาน ต้องได้รับสิทธิ์ในการเข้าใช้งานจากสำนักเทคโนโลยีสารสนเทศและการสื่อสาร โดยต้องใช้งานผ่านระบบ Single Sign-On ของกรมศุลกากรโดยต้องใช้ user และ password พร้อมอุปกรณ์พิสูจน์ตัวตน

ส่วนที่ ๔ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

๑. การสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยมีข้อปฏิบัติ ดังนี้

๑.๑. มีคู่มือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑.๒. มีการฝึกอบรมให้ผู้ใช้งานตระหนักและเข้าใจในเรื่องภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ถูกต้องหรือไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งมาตรการการป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

๒. การลงทะเบียนผู้ใช้งาน (User management)

๒.๑. แจ้งสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอรับสิทธิในการเข้าถึงระบบสารสนเทศที่เกี่ยวข้อง

๒.๒. การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออก หรือเมื่อเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๓. ผู้ใช้สามารถตั้งรหัสผ่านได้ด้วยตนเอง รวมถึงการตั้งคำถามคำตอบ

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User management)

๓.๑. ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับ

๓.๒. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา ต้องได้รับความเห็นชอบและอนุมัติจาก ผอ.สำนัก/กลุ่ม นั้นๆ

(๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๓.๓. ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

๔.๑. ไม่ควรกำหนดรหัสผ่านในส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

๔.๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๔.๓. การกำหนดรหัสผ่าน มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

๕. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

๕.๑. เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน เหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

๑. การใช้งานรหัสผ่าน (Password use)

๑.๑ ต้องเก็บรักษารหัสผ่านไว้เป็นความลับ

๑.๒ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑.๕ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๑.๖ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑.๗ เมื่อเจ้าหน้าที่ของสำนัก/กลุ่ม ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้สำนัก/กลุ่ม แจ้งสำนักเทคโนโลยีสารสนเทศและการสื่อสารทันที เพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ของผู้ที่ลาออก ออกจากระบบทันทีที่ได้รับแจ้ง

๑.๘ มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๒.๑. ผู้ใช้ต้องทำการล็อกหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ หรือไม่อยู่ที่หน้าจอ

๒.๒. ผู้ใช้ต้องทำการ Log out ออกจากระบบทันที เมื่อเลิกใช้ระบบสารสนเทศ

๓. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๓.๑. การจัดการบริเวณล้อมรอบ (Physical security management)

(๑) กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

(๒) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center) ให้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

(๓) มีระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

(๔) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้ได้ตามปกติ

(๕) บุคลากรของกรมศุลกากรต้องล็อกและปิดประตูหน้าต่างอยู่เสมอ หากไม่มีผู้ดูแลเพื่อป้องกันทรัพย์สินของกรมศุลกากร

๓.๒. การควบคุมการเข้า – ออก (Physical entry controls)

(๑) ให้มีการบันทึกวันและเวลาเข้า – ออก พื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

(๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไปเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๓) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๔) สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๕) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๖) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการ

อนุญาต

- (๗) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เพื่อควบคุมการเข้า – ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)
- (๘) จัดเก็บบันทึกการเข้า – ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น
- (๙) เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาการทำงาน
- (๑๐) ผู้ที่มาเยือนต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาที่อยู่ภายในสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
- (๑๑) ต้องจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ
- (๑๒) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างสม่ำเสมอ

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

- (๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- (๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น
- (๓) จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายใน กรมศุลกากร
- (๔) ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน
- (๕) ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของกรมศุลกากร

๓.๔ การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

- (๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้อง Data Center ให้น้อยที่สุด
- (๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย
- (๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center)
- (๔) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๓.๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

- (๑) มีการสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของกรมศุลกากรที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ
 - ระบบสำรองกระแสไฟฟ้า (UPS)
 - เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

- ระบบระบายอากาศ
 - ระบบปรับอากาศ และควบคุมความชื้น
- (๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- (๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน
- ๓.๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling security)
- (๑) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย หรือป้องกันสัตว์ต่างๆ กัดสาย
- (๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- (๓) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น
- (๔) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง
- (๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก
- ๓.๗ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)
- (๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด
- (๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
- (๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- (๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- (๕) ควบคุมสอดส่องดูแลการปฏิบัติงานของผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ ที่มาทำการบำรุงรักษาอุปกรณ์ภายในกรมศุลกากร
- (๖) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ๓.๘ การนำทรัพย์สินของกรมศุลกากร ออกนอกสำนักงาน (Removal of property)
- (๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกกรมศุลกากร
- (๒) บันทึกข้อมูลการนำอุปกรณ์ของกรมศุลกากรออกนอกกรมศุลกากรเพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน
- (๓) สำรองและลบข้อมูลที่เกี่ยวข้องในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม
- ๓.๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)
- (๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของกรมศุลกากรออกไปใช้งานข้างนอก
- (๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของกรมศุลกากรไว้โดยลำพังในที่สาธารณะ
- (๓) ให้เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง
- ๓.๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

- (๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว
- (๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๔. ผู้ใช้งานข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เก็บความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๕๔

ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย (Network access control)

๑. การใช้งานบริการเครือข่าย

๑.๑ การใช้งานอินเทอร์เน็ต (Use of the Internet)

- (๑) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอัปเดตช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
- (๒) ผู้ใช้ต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของกรมศุลกากร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
- (๓) ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของกรมศุลกากร โดยผ่านความเห็นชอบจาก ผอ.สำนัก/กลุ่ม
- (๔) ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมศุลกากร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
- (๕) ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
- (๖) การใช้งานเว็บบอร์ด (Web Board) ของกรมศุลกากรผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของกรมศุลกากร
- (๗) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ
- (๘) ผู้ใช้ต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

- (๑) ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมศุลกากร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- (๒) ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้นิยามใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมศุลกากร
- (๓) การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

- (๔) รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “o” ในการพิมพ์แต่ละตัวอักษร
- (๕) ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของกรมศุลกากรเพื่อใช้ในการติดต่อกับราชการ
- (๖) ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
- (๗) ผู้ใช้ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ตามแนวทางปฏิบัติที่ระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”
- (๘) ผู้ใช้ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อกรมศุลกากรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมายหรือละเมิดศีลธรรมและแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมศุลกากร
- (๙) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- (๑๐) ผู้ใช้ต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น
- (๑๑) ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- (๑๒) ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
- (๑๓) ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒. การยืนยันตัวบุคคลสำหรับผู้ที่อยู่ภายนอกองค์กร (User authentication for external connections) ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบของกรมศุลกากร โดยมีแนวทางปฏิบัติ ดังนี้

๒.๑ กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๒.๒ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๒.๓ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน

๒.๔ การเข้าสู่ระบบสารสนเทศของกรมศุลกากรจากอินเทอร์เน็ตนั้น ต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๕ การใช้งานอินเทอร์เน็ตเข้ามายังระบบสารสนเทศของกรมศุลกากร ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

๒.๖ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ (เช่น เครือข่ายอินเทอร์เน็ต เป็นต้น) หรือเครือข่ายไร้สาย

๒.๗ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๒.๘ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๓. การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks)

๓.๑ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๒ การใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับอนุมัติจากกรมศุลกากร และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๓ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล

๓.๔ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๓.๕ การบริหารจัดการ การบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบ ป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๓.๖ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๓.๗ มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (เก็บ log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

๔.๑ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมศุลกากร ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๔.๒ IP address ภายในของระบบงานเครือข่ายภายในของกรมศุลกากร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ได้โดยง่าย

๔.๓ หากผู้บริหารระบบ (Administrator) จำเป็นต้องใช้งานผ่านพอร์ต ต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๕. การแบ่งแยกเครือข่าย (Segregation in networks)

กรมศุลกากร มีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่ออำนวยความสะดวกในการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ ดังนี้

๕.๑ เครือข่ายภายนอก

๕.๒ เครือข่ายสาธารณะ

๕.๓ เครือข่ายภายในกรมศุลกากร

๕.๔ เครือข่ายไร้สาย

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

๖.๑ ระบบเครือข่ายทั้งหมดของกรมศุลกากร ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกกรมศุลกากร ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ

๖.๒ ให้ผู้ดูแลระบบ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งาน อินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS/IDS เป็นต้น

๖.๓ การควบคุมการเข้าถึงระบบเครือข่ายภายในของกรมศุลกากร

(๑) การเข้าสู่ระบบเครือข่ายภายในของกรมศุลกากร โดยผ่านทางอินเทอร์เน็ตจะต้อง ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และการสื่อสาร ก่อนที่จะสามารถใช้งานได้ทุกกรณี

(๒) การเข้าสู่ระบบเครือข่ายภายในกรมศุลกากร ผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความ ถูกต้อง

๖.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

(๑) ผู้ใช้ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมศุลกากร จะต้องทำการ ลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร ตามความจำเป็นในการใช้งาน

(๒) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบ เครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๓) ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของ ระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control)

๗.๑ ผู้ดูแลระบบ ต้องมีวิธีจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะ เครือข่ายที่ได้รับอนุญาตเท่านั้น

๗.๒ ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน (Enforced Path)

๗.๓ ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จาก เครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๗.๔ กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการ กำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

๑. การควบคุมการเข้าถึงระบบปฏิบัติการ

๑.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์

๑.๒ ผู้ใช้ต้องกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามที่ระบุไว้ในเอกสาร “ประกาศกรม ศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

๑.๓ ผู้ใช้ต้องทำการล็อกหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ หรือไม่อยู่ที่หน้าจอ

๑.๔ ผู้ใช้ต้องทำการ Logout ออกจากระบบสารสนเทศทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication)

๒.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

๒.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

๓. การบริหารจัดการรหัสผ่าน (Password management system)

มีการกำหนดรหัสผ่านตามที่ระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

๔. การใช้ประโยชน์โปรแกรมอรรถประโยชน์ (Use of system utilities)

กำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันโปรแกรมไม่ประสงค์ดี ดังนี้

๔.๑ ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่ กรมศุลกากร ไม่อนุญาตให้ใช้งาน

๔.๒ ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๔.๓ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศของกรมศุลกากร

๔.๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

๔.๖ มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๔.๗ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่ที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๕. การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน (Session time-out)

๕.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มิกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

๕.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงานที่มีข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

๖.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งาน โดยให้ระบบยกเลิกการเชื่อมต่อ หากผู้ใช้งานไม่มีการใช้งานเกิน ๓๐ นาที

๖.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกกรมศุลกากร) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๘ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)

๑. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๑.๑ ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ

- (๑) กำหนดข้อมูลตามระดับชั้นความลับ เช่น ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน ข้อมูลความลับ เป็นต้น
- (๒) ขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับต้องประกอบด้วยวิธีการประมวลผล การควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อบันทึกข้อมูล การทำปายบ่งชี้ และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย
- (๓) ให้มีการจำกัดการเข้าถึงข้อมูลสำคัญเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- (๔) มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป
- (๕) มีความตระหนัก และมาตรการป้องกันข้อมูลสำคัญที่มีการส่งพิมพ์ออกมาทางเครื่องพิมพ์เพื่อป้องกันการเข้าถึงโดยผู้อื่น
- (๖) จัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๑.๒ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)

- (๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย
- (๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น
- (๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

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 ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่กรมศุลกากรต้องปฏิบัติตาม

๑.๔ ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreement) จัดทำแนวทางข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างกรมศุลกากรกับหน่วยงานภายนอก ดังต่อไปนี้

- (๑) กำหนดขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูล ที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

- (๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น
- (๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล
- (๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล เพื่อเป็นการป้องกันการปฏิเสธ
- (๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น
- (๖) กำหนดสิทธิการเข้าถึงข้อมูล
- (๗) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์
- (๘) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

๑.๕ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

พิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่างๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างกรมศุลกากร หรือ หน่วยงานที่มาขอเชื่อมโยง มีดังต่อไปนี้

- (๑) กำหนดมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน
- (๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- (๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน
- (๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
- (๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๑.๖ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่

สำคัญ ดังนี้

- (๑) ข้อมูลชื่อบัญชีผู้ใช้
- (๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
- (๓) ข้อมูลวันเวลาที่ออกจากระบบ
- (๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- (๕) ข้อมูลชื่อเทอมินัล
- (๖) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
- (๗) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- (๘) ข้อมูลการเปลี่ยนคอนฟิกูเรชัน(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) ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญ
- (๑๗) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๒. การบริหารจัดการกับระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร

๒.๑ จัดให้มีการบริหารจัดการสภาพแวดล้อมในส่วนของพื้นที่ศูนย์คอมพิวเตอร์ ดังนี้

- (๑) มีกำหนดระเบียบหรือแนวการปฏิบัติในการเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์ ระบุไว้ในเอกสาร “คำสั่งสำนักเทคโนโลยีสารสนเทศ ที่ ๑/๒๕๕๔ เรื่อง การเข้า-ออกศูนย์ควบคุมคอมพิวเตอร์”
- (๒) มีการควบคุมการเข้า-ออก ด้วยระบบ Hand Scan และระบบ Finger Print พร้อมระบบ CCTV
- (๓) ระบบสำรองกระแสไฟฟ้า (UPS)
- (๔) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- (๕) ระบบระบายอากาศ
- (๖) ระบบปรับอากาศ และควบคุมความชื้น
- (๗) ระบบดับเพลิง ระบบตรวจสอบควันไฟและน้ำรั่วซึม

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

๒.๔ มีแผนฉุกเฉิน กรณีระบบคอมพิวเตอร์ขัดข้อง ระบุไว้ในเอกสาร “แผนฉุกเฉิน กรณีระบบเครื่องคอมพิวเตอร์ขัดข้อง”

๒.๕ มีแผนฉุกเฉิน กรณีเกิดอุทกภัย หรือภัยพิบัติทางธรรมชาติ ระบุไว้ในเอกสาร “แผนฉุกเฉิน กรณีเกิดอุทกภัย หรือภัยพิบัติทางธรรมชาติ”

๒.๖ ในระบบที่มีผลกระทบและความสำคัญสูงต่อกรมศุลกากร หากต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่างๆ ซึ่งมีใช้ของทรัพย์สินของกรมศุลกากรต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศและการสื่อสาร กรมศุลกากร

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อดูแลรักษาความปลอดภัยในการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ดังนี้

๓.๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

๓.๑.๑ แนวทางปฏิบัติในการใช้งานทั่วไป

- (๑) เครื่องคอมพิวเตอร์ที่กรมศุลกากร อนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินของ กรมศุลกากร ดังนั้น ผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของกรมศุลกากร
- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของกรมศุลกากร ต้องเป็นโปรแกรมที่ กรมศุลกากร ได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของกรมศุลกากร
- (๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับ กรมศุลกากร เท่านั้น
- (๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- (๖) ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์
- (๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง
- (๘) ทำการล็อกหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์
- (๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของกรมศุลกากร ยกเว้นจะได้รับการตรวจสอบจากสำนักเทคโนโลยีสารสนเทศและการสื่อสารก่อนการใช้งาน

๓.๑.๒ แนวทางปฏิบัติในการใช้รหัสผ่าน

- (๑) ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

๓.๑.๓ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- (๑) ผู้ใช้ ต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- (๒) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- (๓) ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๓.๑.๔ การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น
- (๒) ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง(Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ

๓.๒ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook Computer) และอุปกรณ์สื่อสารเคลื่อนที่

๓.๒.๑ แนวทางปฏิบัติการใช้งานทั่วไป

- (๑) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่กรมศุลกากรอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินของกรมศุลกากร ดังนั้น ผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ อย่างมีประสิทธิภาพเพื่องานของกรมศุลกากร
- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของกรมศุลกากร ต้องเป็นโปรแกรมที่กรมศุลกากร ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- (๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
- (๕) ในกรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- (๖) หลีกเลี่ยงการใช้น้ำหรือของแข็ง เช่น ปลายปากกา สัมผัสหน้าจอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของกรมศุลกากรซึ่งอาจทำให้แตกเสียหายได้
- (๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (๘) การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- (๙) หากมีการนำเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งไม่ใช่ทรัพย์สินของกรมศุลกากรมาใช้กับระบบเครือข่ายของกรม

บุคลากร ต้องได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศและการสื่อสารก่อนการใช้งาน

๓.๒.๒ ความปลอดภัยทางด้านกายภาพ

- (๑) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- (๒) ผู้ใช้ต้องไม่เก็บ หรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระแทบ

๓.๒.๓ แนวทางปฏิบัติในการใช้งานรหัสผ่าน

- (๑) ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “ประกาศกรมศุลกากร ที่ ๑๐๑/๒๕๕๓ เรื่อง การเข้าใช้ระบบเครือข่ายกรมศุลกากร”

๓.๒.๔ การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของกรมศุลกากร โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล
- (๒) ผู้ใช้จะต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- (๓) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ
- (๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้นำไปใช้งานได้

๔. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ในกรมศุลกากร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๔.๑ ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

๔.๒ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของกรมศุลกากร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของกรมศุลกากร การควบคุมบุคคลที่เข้าสู่ระบบของกรมศุลกากรจากระยะไกล จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๔.๓ วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๔.๔ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับกรมศุลกากร อย่างเพียงพอและต้องได้รับการอนุมัติจากกรมศุลกากร

๔.๕ มีการควบคุมพอร์ต(Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องเหมาะสมแล้วเท่านั้น

๔.๖ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ส่วนที่ ๙ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ

กรมศุลกากร จัดให้มีระบบสำรองสำหรับระบบสารสนเทศ โดยมีข้อปฏิบัติดังนี้

๑. การคัดเลือกและการจัดทำระบบสำรอง

๑.๑ กำหนดระบบงานที่มีความสำคัญทั้งหมดของกรมศุลกากร

๑.๒ กำหนดรายละเอียดของระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อย ต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่น ๆที่เกี่ยวข้อง เป็นต้น

๑.๓ กำหนดขั้นตอนการสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง

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

๑.๕ เตรียมอุปกรณ์ที่จำเป็นต่อการสำรองข้อมูล และการกู้คืนข้อมูล

๑.๖ ทำการสำรองข้อมูลตามชนิด ความถี่ และ วิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

๑.๗ ต้องนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๒.๑ ระบุวัตถุประสงค์หลักของแผนเตรียมความพร้อมกรณีฉุกเฉิน

๒.๒ จัดทำบัญชีรายชื่อของระบบงานที่มีความสำคัญ รวมทั้งปรับปรุงบัญชีรายชื่อดังกล่าวให้มีความทันสมัยอยู่เสมอ

๒.๓ กำหนดปัจจัยเสี่ยงและภัยพิบัติที่อาจส่งผลกระทบต่อระบบงานที่มีความสำคัญ และ กำหนดมาตรการ เพื่อลดความเสี่ยงที่พบ เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๒.๔ ประเมินสถานการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๕ จัดทำแผนกู้คืนเพื่อรับมือกับสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๒.๕.๑ การกำหนดหน้าที่ความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๒.๕.๒ การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน

๒.๕.๓ การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ เช่น ไฟไหม้

๒.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๗ ให้ทำการปรับปรุงแผนกู้คืนอย่างน้อยปีละ ๑ ครั้ง

๒.๘ ให้จัดประชุม และ แจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้ง เมื่อมีการปรับปรุงแผนกู้คืนใหม่จะต้องจัดประชุมใหม่ และ แจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

๓. การกำหนดหน้าที่และความรับผิดชอบของบุคลากร

กรมศุลกากรกำหนดหน้าที่ความรับผิดชอบในการสำรองและกู้คืนระบบคอมพิวเตอร์ ระบุไว้ในเอกสาร “แผนการสำรองและกู้คืนระบบคอมพิวเตอร์ (Backup and Recovery Plan)”

๔. การทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมฉุกเฉิน

๔.๑ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

๔.๒ ให้ทำการตรวจสอบกู้คืนข้อมูลที่สำรองไว้นั้น ว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และ บันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีแก้ไขอย่างเป็นลายลักษณ์อักษร

๕. ระยะเวลาถี่ของการปฏิบัติ

๕.๑ ระยะเวลาถี่การสำรองข้อมูลของระบบงาน ขึ้นอยู่กับความสำคัญของระบบ และสภาพความเปลี่ยนแปลงของระบบงานนั้น ๆ เช่น ระบบงานที่มีการเปลี่ยนแปลงบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๕.๒ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ และความพร้อมในการใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๕.๓ ให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กรมศุลกากรจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล โดยกลุ่มตรวจสอบภายในของกรมศุลกากรอย่างน้อยปีละ ๑ ครั้ง และในการตรวจสอบและประเมินความเสี่ยง มีสิ่งที่ต้องคำนึงถึง ดังนี้

๑. จัดลำดับความสำคัญของความเสี่ยง

๒. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

๓. ข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๕. ในการตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยให้ครอบคลุมหัวข้ออย่างน้อย

ต่อไปนี้เป็น

ปฏิบัติการ

- ๕.๑ การตรวจสอบและประเมินด้านการบริหารสินทรัพย์ด้านเทคโนโลยีสารสนเทศ
- ๕.๒ การตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม
- ๕.๓ การตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการ
- ๕.๔ การตรวจสอบและประเมินการควบคุมการเข้าถึง
- ๕.๕ การตรวจสอบและประเมินด้านการพัฒนาระบบ จัดซื้อจัดหาระบบและการดูแลระบบ
- ๕.๖ การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์