ประกาศกรมศุลกากร
ที่ ๘๖ /๒๕๖๙
เรื่อง นโยบายและประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของกรมศุลกากร

เพื่อให้การกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ลงวันที่ ๒ สิงหาคม พ.ศ. ๒๕๖๔

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ อธิบดีกรมศุลกากรออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมศุลกากร มีรายละเอียดดังนี้

(๑) ให้มีการกำหนดกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมศุลกากร เพื่อให้หน่วยงานภายในกรมศุลกากรมีแนวทางและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นมาตรฐานเดียวกันทั้งองค์กร

(๒) ให้มีการกำหนดหลักการ มาตรการ และแนวปฏิบัติในการคุ้มครองระบบสารสนเทศและข้อมูลของหน่วยงานครอบคลุมการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบสารสนเทศ

(๓) ให้ทุกหน่วยงาน มีความตระหนักถึงการบริหารจัดการและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(๔) ให้มีกระบวนการรองรับและป้องกันภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นและซับซ้อนมากขึ้น เช่น การเข้าถึงระบบโดยมิชอบ การโจมตีระบบ การทำลายหรือปลอมแปลงข้อมูล หรือภัยคุกคามรูปแบบใหม่

(๕) เพื่อยกระดับมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของกรมศุลกากร เพื่อสร้างความเชื่อมั่นในการให้บริการภาครัฐ การจัดเก็บรายได้ของรัฐ และการอำนวยความสะดวกทางการค้าระหว่างประเทศ

ข้อ ๒ เพื่อให้การดำเนินงานของกรมศุลกากร สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมศุลกากร และสามารถปฏิบัติตามได้อย่างเป็นรูปธรรม จึงกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมศุลกากรไว้ ท้ายประกาศนี้

/ข้อ ๓ ให้ศูนย์...

ข้อ ๓ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการแจ้งให้ผู้ที่เกี่ยวข้องและผู้ใช้งานทั้งหมดได้รับทราบประกาศนี้โดยทั่วกันผ่านทางเว็บไซต์ของกรมศุลกากร

ข้อ ๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๙ เป็นต้นไป

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๙

(นายพันธ์ทอง ลอยกุลนันท์)
อธิบดีกรมศุลกากร

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมศุลกากร พ.ศ. ๒๕๖๙

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมศุลกากร พ.ศ. ๒๕๖๙

๑. บทนำ

ในบริบทของการบริหารราชการแผ่นดินยุคดิจิทัล เทคโนโลยีสารสนเทศและระบบอิเล็กทรอนิกส์ได้กลายเป็นกลไกหลักในการขับเคลื่อนภารกิจของหน่วยงานภาครัฐ โดยเฉพาะหน่วยงานที่เกี่ยวข้องกับการจัดเก็บรายได้ของรัฐและการกำกับดูแลการค้าระหว่างประเทศ ซึ่งต้องพึ่งพาระบบสารสนเทศที่มีความเชื่อมโยงกับหน่วยงานทั้งภายในและภายนอกประเทศอย่างต่อเนื่อง ภายใต้สภาพแวดล้อมดังกล่าว ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มขึ้นทั้งในด้านความถี่และความซับซ้อน อันอาจส่งผลกระทบต่อความต่อเนื่องในการให้บริการ ความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย และเสถียรภาพทางเศรษฐกิจของประเทศ

กรมศุลกากร มีภารกิจสำคัญด้านการจัดเก็บอากร การอำนวยความสะดวกทางการค้า การป้องกันและปราบปรามการลักลอบนำเข้า-ส่งออกสินค้า ตลอดจนการบริหารความเสี่ยงด้านศุลกากร ซึ่งต้องอาศัยระบบสารสนเทศและข้อมูลอิเล็กทรอนิกส์เป็นโครงสร้างพื้นฐานหลัก ข้อมูลที่อยู่ในความครอบครองของกรมศุลกากรมีทั้งข้อมูลทางการค้า ข้อมูลทางภาษีอากร และข้อมูลส่วนบุคคลที่มีความอ่อนไหว จึงจำเป็นต้องได้รับการคุ้มครองให้มีความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานตามหลักสากล โดยภัยคุกคามทางไซเบอร์ เช่น การเข้าถึงระบบโดยมิชอบ การโจมตีแบบปฏิเสธการให้บริการ การปลอมแปลงหรือทำลายข้อมูล และการเรียกค่าไถ่ข้อมูล อาจก่อให้เกิดความเสียหายต่อการดำเนินภารกิจของกรมศุลกากร ทั้งในด้านรายได้ของรัฐและความเชื่อมั่นของภาคเอกชน ดังนั้น การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงมีความจำเป็นอย่างยิ่ง

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำขึ้นเพื่อกำหนดหลักการ มาตรการ และแนวทางปฏิบัติที่เป็นมาตรฐานเดียวกันทั้งองค์กร พร้อมทั้งส่งเสริมวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งยกระดับมาตรฐานการคุ้มครองข้อมูลและระบบสารสนเทศของกรมศุลกากรให้มีความมั่นคง ทันสมัย และสามารถรองรับภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็วได้อย่างมีประสิทธิภาพและยั่งยืน

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กรมศุลกากร ให้มีความชัดเจน เป็นมาตรฐานเดียวกัน และสามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรมทั่วทั้งองค์กร

๒.๒ เพื่อคุ้มครองข้อมูล ระบบสารสนเทศ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมศุลกากร ให้มีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ตามหลักสากล

๒.๓ เพื่อให้ทุกภาคส่วน มีการตระหนักถึงการบริหารจัดการและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม

/๒.๔ เพื่อระบุ...

๒.๔ เพื่อระบุความเสี่ยง ป้องกัน ตรวจสอบและเฝ้าระวัง ตอบสนอง และฟื้นฟูจากเหตุการณ์ภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

๒.๕ เพื่อส่งเสริมวัฒนธรรมองค์กรและยกระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในองค์กร

๓. ขอบเขตการใช้

๓.๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ให้ใช้บังคับกับทุกหน่วยงานในสังกัดกรมศุลกากร รวมถึงบุคลากรทุกประเภท ไม่ว่าจะเป็นข้าราชการ พนักงานราชการ และลูกจ้าง

๓.๒ ครอบคลุมระบบสารสนเทศ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เครือข่าย อุปกรณ์คอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ระบบคลาวด์ ฐานข้อมูล และระบบเชื่อมโยงข้อมูลกับหน่วยงานภายนอก ทั้งที่พัฒนาเองและที่จัดหาจากภายนอก

๓.๓ ครอบคลุมข้อมูลทุกประเภทที่อยู่ในความครอบครองหรือความรับผิดชอบของกรมศุลกากร ทั้งข้อมูลราชการ ข้อมูลทางการค้า ข้อมูลทางภาษีอากร ข้อมูลส่วนบุคคล และข้อมูลที่เกี่ยวข้องกับความมั่นคงของรัฐ ไม่ว่าจะจัดเก็บในรูปแบบอิเล็กทรอนิกส์หรือสื่ออื่นใด

๓.๔ ใช้เป็นกรอบอ้างอิงในการบริหารจัดการความเสี่ยง การกำหนดมาตรการควบคุม การตรวจสอบประเมินผล การจัดทำแผนป้องกันและตอบสนองเหตุการณ์ไซเบอร์ รวมถึงการจัดทำข้อตกลงหรือข้อกำหนดด้านความมั่นคงปลอดภัยกับผู้ให้บริการภายนอก

๓.๕ ใช้เป็นแนวทางในการเสริมสร้างความรู้ ความตระหนัก และวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนเป็นเกณฑ์ในการกำกับ ติดตาม และประเมินการปฏิบัติงานให้สอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง

๔. คำนิยาม

เพื่อประโยชน์ในการตีความและการบังคับใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมศุลกากร ให้คำหรือถ้อยคำต่อไปนี้มีความหมายดังต่อไปนี้

“ความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ เพื่อให้สามารถรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของระบบสารสนเทศได้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมต่อการทำงานเข้าด้วยกัน โดยมีคำสั่ง ชุดคำสั่ง หรือโปรแกรมที่ทำให้อุปกรณ์นั้นสามารถประมวลผลข้อมูลได้โดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ซึ่งระบบคอมพิวเตอร์สามารถประมวลผลได้

/“โครงสร้าง...

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า ระบบคอมพิวเตอร์หรือระบบสารสนเทศที่มีความสำคัญต่อความมั่นคงของรัฐ ความปลอดภัยสาธารณะ หรือเศรษฐกิจของประเทศ ซึ่งหากเกิดความเสียหายหรือหยุดชะงักอาจส่งผลกระทบอย่างร้ายแรงต่อประเทศ

“การบริหารจัดการความเสี่ยง” หมายความว่า กระบวนการระบุ วิเคราะห์ ประเมิน และควบคุมความเสี่ยงที่อาจส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูล และการดำเนินงานของหน่วยงาน

“การประเมินความเสี่ยง” หมายความว่า การวิเคราะห์และประเมินระดับความเสี่ยงที่อาจเกิดขึ้นต่อระบบสารสนเทศหรือข้อมูล เพื่อกำหนดมาตรการควบคุมและลดความเสี่ยงที่เหมาะสม

“ทะเบียนทรัพย์สิน” หมายความว่า รายการบันทึกทรัพย์สินด้านเทคโนโลยีสารสนเทศและระบบสารสนเทศของกรมศุลกากร เช่น อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม และฐานข้อมูล เพื่อใช้ในการบริหารจัดการและควบคุมความมั่นคงปลอดภัย

“ผู้ใช้งาน” หมายความว่า บุคลากรของกรมศุลกากร หรือบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบสารสนเทศของกรมศุลกากรตามหน้าที่หรือข้อตกลงที่กำหนด

“ผู้ดูแลระบบ” หมายความว่า บุคคลที่ได้รับมอบหมายให้มีหน้าที่ดูแล บริหารจัดการ และควบคุมการทำงานของระบบคอมพิวเตอร์ เครือข่าย หรือระบบสารสนเทศของกรมศุลกากร

“ผู้ให้บริการภายนอก” หมายความว่า บุคคลหรือนิติบุคคลที่มิได้เป็นบุคลากรของกรมศุลกากร แต่ให้บริการด้านระบบสารสนเทศหรือเทคโนโลยีสารสนเทศแก่กรมศุลกากรตามสัญญาหรือข้อตกลง

“บุคคลภายนอก” หมายความว่า บุคคลธรรมดา หรือนิติบุคคลที่มิได้เป็นข้าราชการ พนักงานราชการ ลูกจ้าง หรือบุคลากรของกรมศุลกากร แต่ได้รับอนุญาตหรือมีความเกี่ยวข้องกับการดำเนินงานของกรมศุลกากร เช่น ผู้รับจ้าง ที่ปรึกษา ผู้ให้บริการ ผู้พัฒนาระบบ ผู้ตรวจสอบ หรือหน่วยงานอื่นของรัฐหรือเอกชน ที่มีการเข้าถึงหรือใช้ประโยชน์จากระบบสารสนเทศ ข้อมูล หรือทรัพยากรด้านเทคโนโลยีสารสนเทศของกรมศุลกากร ตามขอบเขตที่ได้รับอนุญาตหรือกำหนดไว้ในสัญญา ข้อตกลง หรือกฎหมายที่เกี่ยวข้อง

“การควบคุมการเข้าถึง” หมายความว่า มาตรการหรือกระบวนการที่กำหนดขึ้นเพื่อจำกัดและควบคุมสิทธิในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูล หรือทรัพยากรสารสนเทศให้เฉพาะผู้ที่ได้รับอนุญาต

“การสำรองข้อมูล” หมายความว่า กระบวนการจัดเก็บสำเนาข้อมูลคอมพิวเตอร์ไว้ในสื่อหรือระบบอื่นเพื่อใช้ในการกู้คืนข้อมูลเมื่อเกิดความเสียหายหรือเหตุขัดข้อง

“บันทึกเหตุการณ์ (Log)” หมายความว่า ข้อมูลที่ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์บันทึกเกี่ยวกับการใช้งาน การเข้าถึง หรือกิจกรรมที่เกิดขึ้นในระบบสารสนเทศ

“การกู้คืนระบบ” หมายความว่า กระบวนการฟื้นฟูระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือระบบสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติหลังจากเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบ

“การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์” หมายความว่า กระบวนการตรวจสอบและประเมินมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามนโยบาย มาตรฐาน และกฎหมายที่เกี่ยวข้อง

/ทั้งนี้...

ทั้งนี้ คำอื่นใดที่มิได้กำหนดไว้ในประมวลฉบับนี้ ให้ตีความตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม

๕. ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ๓ องค์ประกอบหลัก ดังนี้

๕.๑ องค์ประกอบที่ ๑: แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๑.๑ จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบจากภายนอกอย่างน้อยปีละ ๑ ครั้ง

๕.๒ องค์ประกอบที่ ๒: การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๒.๑ จัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงระบบงานอย่างมีนัยสำคัญ

๕.๓ องค์ประกอบที่ ๓: แผนการรับมือภัยคุกคามทางไซเบอร์

๕.๓.๑ มีขั้นตอนปฏิบัติภายใต้การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ และระบบคอมพิวเตอร์

๕.๓.๒ จัดให้มีการสื่อสารและซักซ้อมแผนการรับมือเหตุการณ์ไปยังบุคลากรที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๖. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประกอบด้วย ๕ หัวข้อหลักตามมาตรฐานสากล ได้แก่ การระบุความเสี่ยง (Identify) มาตรการป้องกัน (Protect) มาตรการตรวจสอบและเฝ้าระวัง (Detect) มาตรการเผชิญเหตุ (Respond) และมาตรการกู้คืน (Recover) โดยมีรายละเอียดแต่ละหัวข้อ ดังนี้

๖.๑ หัวข้อหลักที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่น ที่เกี่ยวข้องกับคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๖.๑.๑ การจัดการทรัพย์สิน

(๑) มีการจัดทำทะเบียนทรัพย์สิน ที่ระบุทรัพย์สินของบริการที่สำคัญ และให้ดำเนินการปรับปรุงทะเบียนทรัพย์สินให้เป็นปัจจุบัน

(๒) มีการทบทวนและประเมินความเสี่ยงทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างระบบงานหรือทรัพยากรสารสนเทศที่สำคัญ

๖.๒ หัวข้อหลักที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๖.๒.๑ การควบคุมการเข้าถึง

(๑) มีการกำหนดนโยบายควบคุมการเข้าถึงระบบสารสนเทศและระบบสนับสนุนเพื่อให้ผู้ใช้งานเข้าถึงข้อมูลและระบบงานได้เฉพาะที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบเท่านั้น

(๒) การเข้าใช้งานระบบงานต้องมีการพิสูจน์ตัวตน แบบหลายปัจจัย (Multi-factor Authentication : MFA)

/(๓) มีการ...

(๓) มีการบริหารจัดการบัญชีผู้ใช้งานอย่างเป็นระบบ ทั้งการสร้าง การเปลี่ยนแปลง และการยกเลิกสิทธิเมื่อบุคลากรลาออกหรือเปลี่ยนหน้าที่

(๔) มีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างองค์กรอย่างมีนัยสำคัญ

๖.๒.๒ การสร้างความตระหนักรู้และการฝึกอบรม

(๑) มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ให้กับบุคลากรของกรมศุลกากร อย่างน้อยปีละ ๑ ครั้ง

(๒) มีการอบรมเฉพาะทางเพิ่มเติมเกี่ยวกับการป้องกันภัยคุกคาม ให้กับผู้ดูแลระบบ อย่างน้อยปีละ ๑ ครั้ง

(๓) มีการสื่อสารและแจ้งเตือนเกี่ยวกับภัยคุกคามไซเบอร์รูปแบบใหม่ ให้บุคลากร ทราบอย่างสม่ำเสมอ

๖.๒.๓ ความมั่นคงปลอดภัยของข้อมูล

(๑) ข้อมูลที่มีความสำคัญ ต้องมีการเข้ารหัส (Encryption) ทั้งในขณะจัดเก็บ และขณะรับส่งข้อมูลผ่านเครือข่าย

(๒) มีมาตรการป้องกันการรั่วไหลของข้อมูล เพื่อตรวจสอบและป้องกันการส่งข้อมูล สำคัญออกนอกหน่วยงานโดยไม่ได้รับอนุญาต

(๓) มีการตรวจสอบช่องโหว่ของระบบคอมพิวเตอร์อย่างน้อยปีละ ๑ ครั้ง

๖.๒.๔ กระบวนการและขั้นตอนการคุ้มครองข้อมูล

(๑) มีแผนบริหารความต่อเนื่องในสภาวะวิกฤตและแผนสำรองภาวะฉุกเฉิน สำหรับระบบงานศุลกากรที่สำคัญ

(๒) มีนโยบายการสำรองข้อมูลสารสนเทศและการกู้คืน

(๓) มีระเบียบขั้นตอนการบริหารจัดการความเสี่ยง

๖.๒.๕ เทคโนโลยีเพื่อการป้องกัน

(๑) มีระบบป้องกันภัยคุกคามในส่วนของระบบคอมพิวเตอร์ เช่น Firewall DDoS Protection และ Endpoint Protection เป็นต้น

(๒) มีการบันทึกเหตุการณ์ (Log) การใช้งานระบบและเครือข่าย และเก็บรักษาไว้ ไม่น้อยกว่าระยะเวลาที่กฎหมายกำหนด

๖.๒.๖ การกำกับดูแลบุคคลภายนอก

มีนโยบายและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดเงื่อนไข ควบคุม และกำกับการเข้าถึงและใช้งานระบบคอมพิวเตอร์สำหรับบุคคลภายนอก

/๖.๓ หัวข้อ...

๖.๓ หัวข้อหลักที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๖.๓.๑ การตรวจจับความผิดปกติและเหตุการณ์

มีระบบเฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติ ที่เกิดขึ้นกับระบบสารสนเทศและเครือข่ายของกรมศุลกากร

๖.๓.๒ การรักษาความปลอดภัยอย่างต่อเนื่อง

(๑) มีการตรวจสอบสถานะความมั่นคงปลอดภัยของอุปกรณ์และระบบอย่างสม่ำเสมอ

(๒) มีการเฝ้าระวังการเข้าถึงจากบุคคลภายนอกหรือระบบงานหรือผู้ให้บริการภายนอกที่มีการเชื่อมต่อกับเครือข่ายของกรมศุลกากร

๖.๓.๓ กระบวนการตรวจจับ

(๑) มีระบบการตรวจจับภัยคุกคาม รวมถึงการกำหนดบทบาทหน้าที่ของเจ้าหน้าที่หรือผู้รับผิดชอบที่เกี่ยวข้อง

(๒) มีการทบทวนระบบตรวจจับอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(๓) เมื่อตรวจพบเหตุการณ์ผิดปกติที่เข้าข่ายเป็นภัยคุกคามไซเบอร์ ต้องมีการแจ้งเตือนไปยังผู้รับผิดชอบหรือผู้ดูแลระบบและหน่วยงานที่เกี่ยวข้อง

๖.๔ หัวข้อหลักที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๖.๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์

(๑) จัดทำ สื่อสาร ฝึกซ้อม และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

(๒) มีขั้นตอนปฏิบัติการแก้ไขและป้องกันเมื่อมีเหตุการณ์ภัยคุกคามทางไซเบอร์

๖.๔.๒ แผนการสื่อสารในภาวะวิกฤต

(๑) มีกระบวนการสื่อสารเพื่อตอบสนองต่อวิกฤตภัยคุกคามทางไซเบอร์ โดยระบุช่องทางและผู้รับผิดชอบในการให้ข้อมูลแก่ผู้เกี่ยวข้องที่ได้รับผลกระทบ

(๒) มีการจัดตั้งคณะบริหารความต่อเนื่องของกรมศุลกากร สำหรับสื่อสารในภาวะวิกฤต

(๓) มีการประสานงานและแจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือหน่วยงานอื่น ๆ ตามที่กฎหมายกำหนด

๖.๔.๓ การวิเคราะห์และลดผลกระทบ

มีการวิเคราะห์เพื่อระบุประเภท ระดับความรุนแรง สาเหตุ และแนวทางการลดผลกระทบ เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบสารสนเทศของกรมศุลกากร

/๖.๕ หัวข้อ...

๖.๕ หัวข้อหลักที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๖.๕.๑ แผนการกู้คืนระบบ

(๑) มีนโยบายการสำรองข้อมูลคอมพิวเตอร์และการกู้คืน และมีการปรับปรุงอย่างน้อยปีละ ๑ ครั้ง

(๒) มีการตรวจสอบความถูกต้องและความสมบูรณ์ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ หลังการกู้คืน ก่อนที่จะเปิดให้ผู้ใช้งานเข้ามาใช้งานระบบคอมพิวเตอร์

(๓) เมื่อระบบคอมพิวเตอร์สามารถกลับมาให้บริการได้ตามปกติ ให้แจ้งสถานการณ์การกู้คืนระบบให้ผู้ที่เกี่ยวข้องทราบ โดยเป็นไปตามข้อกำหนดแผนบริหารความต่อเนื่องสภาวะวิกฤตของกรมศุลกากร

๖.๕.๒ การปรับปรุงและพัฒนา

มีการสรุปผล ถอดบทเรียน และวิเคราะห์สาเหตุที่ทำให้เกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อนำมาปรับปรุงระบบสารสนเทศ นโยบายและแนวปฏิบัติของกรมศุลกากร ที่เกี่ยวข้องให้มีประสิทธิภาพดียิ่งขึ้น ภายหลังจากการกู้คืนระบบเสร็จสิ้น