ประกาศการท่าเรือแห่งประเทศไทย

เรื่อง นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ

เพื่อให้ระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการใช้อุปกรณ์อิเล็กทรอนิกส์เทคโนโลยีดิจิทัล และระบบงานสารสนเทศของการท่าเรือแห่งประเทศไทยมีการบริหารจัดการด้านความมั่นคงปลอดภัยจากเหตุการณ์และภัยคุกคามต่าง ๆ อย่างมีประสิทธิภาพ สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ อาศัยอำนาจตามความในมาตรา ๓๒ (๒) แห่งพระราชบัญญัติการท่าเรือแห่งประเทศไทย พ.ศ. ๒๔๙๔ ผู้อำนวยการการท่าเรือแห่งประเทศไทย จึงให้ดำเนินการดังนี้

ข้อ ๑ ยกเลิก

๑.๑ ประกาศการท่าเรือแห่งประเทศไทย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ ๑๕ กันยายน ๒๕๖๔

๑.๒ ประกาศที่ขัดหรือแย้งกับประกาศนี้

ข้อ ๒ กำหนดให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของการท่าเรือแห่งประเทศไทยมีการกำกับดูแลและบริหารจัดการภายใต้วัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อให้ระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ของการท่าเรือแห่งประเทศไทยมีความมั่นคงปลอดภัยน่าเชื่อถือ และมีการดำเนินงานอย่างมีประสิทธิภาพและมีประสิทธิผลเป็นที่ยอมรับ

๒.๒ เพื่อกำหนดมาตรฐาน แนวปฏิบัติ และวิธีการปฏิบัติสำหรับใช้ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของการท่าเรือแห่งประเทศไทย ที่มีความสอดคล้องกับมาตรฐานสากลและเป็นไปในทิศทางเดียวกันกับการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒.๓ เพื่อเผยแพร่กรอบแนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศให้พนักงานการท่าเรือแห่งประเทศไทยและผู้เกี่ยวข้องทั้งหมด ซึ่งรวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับการท่าเรือแห่งประเทศไทยได้รับทราบ เข้าใจ เข้าถึงและถือปฏิบัติตามอย่างเคร่งครัด โดยมีการสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

/ ๒ ...

ข้อ ๓ จัดทำนโยบายที่เกี่ยวข้องในการดำเนินการให้ระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของการท่าเรือแห่งประเทศไทยมีความมั่นคงปลอดภัย พร้อมกำหนดมาตรการและแนวปฏิบัติที่ต้องครอบคลุมประเด็นสำคัญอย่างน้อยดังต่อไปนี้

๓.๑ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) โดยต้องมีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้ในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม รวมถึงต้องจัดให้มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

๓.๒ การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (Information classification) มีการเก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูล (Cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลเพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

๓.๓ การควบคุมการเข้าถึง (Access Control)

๓.๓.๑ การเข้าถึงทางกายภาพและสภาพแวดล้อม ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และระบบสาธารณูปโภค (Facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้งาน

๓.๓.๒ การเข้าถึงระบบปฏิบัติการ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

๓.๔ การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security) ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่มีการรับส่งผ่านเครือข่ายสื่อสารมีความมั่นคงปลอดภัย และสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

๓.๕ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security) และการบริหารจัดการคอนฟิกูเรชั่น (Configuration Management) ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย

/ ๓ ...

๓.๖ การจัดหาและการพัฒนาระบบ (System acquisition and development) ต้องกำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและผู้ให้บริการ เพื่อให้มั่นใจว่าระบบและผู้ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินธุรกิจได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี หรือการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจในอนาคต รวมถึงต้องจัดให้มีการออกแบบ พัฒนาและทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคง ปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่น เพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต

๓.๗ การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT Incident and Problem Management) ต้องจัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติและปัญหา และการแก้ไขตามโครงสร้างการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศให้รับทราบภายในระยะเวลาที่เหมาะสม

๓.๘ การจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ ต้องคำนึงถึงลักษณะการดำเนินธุรกิจปริมาณธุรกรรมความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจขององค์กร รวมทั้งการบริหารความเสี่ยงที่อาจเกิดจากเหตุการณ์ ความเสียหายต่าง ๆ และความเสี่ยงทั่วไป เช่น ความเสี่ยงด้านปฏิบัติการ (Operational risk) ความเสี่ยงด้านชื่อเสียง (Reputational risk) และความเสี่ยงอื่นที่เกี่ยวข้อง เช่น ความเสี่ยงจากการพึ่งพาองค์กรอื่นในการดำเนินธุรกิจ (Interdependency risk) ความเสี่ยงจากการกระจุกตัวของระบบงานหรือทรัพยากรที่สำคัญ (Concentration risk) และความเสี่ยงที่มีผลกระทบต่อองค์กร ผู้ใช้บริการ และผู้มีส่วนได้เสีย พร้อมจัดให้มีระบบสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน เพื่อให้ระบบงานสารสนเทศ โดยเฉพาะอย่างยิ่งระบบงานสารสนเทศที่ถูกกำหนดเป็นบริการที่สำคัญของการท่าเรือแห่งประเทศไทยให้สามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ และแผนเตรียมความพร้อมกรณีฉุกเฉินหรือไม่สามารถให้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ ที่มีการทบทวนอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๔ จัดทำนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศให้ครอบคลุมโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ และต้องนำนโยบายดังกล่าวมาจัดทำมาตรการ วิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศของการท่าเรือแห่งประเทศไทย โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

/ ๔ ...

ข้อ ๕ กำหนดให้มีการตรวจสอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยของระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ซึ่งต้องมีการตรวจสอบและประเมินความเสี่ยงจากภัยคุกคามต่าง ๆ รวมถึงภัยคุกคามทางไซเบอร์และสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือเจตนาฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ โดยกำหนดให้ผู้บริหารสูงสุด (Chief Executive Officer : CEO) ของการท่าเรือแห่งประเทศไทย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๗ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (Department Chief Information Officer : DCIO) เป็นผู้รับผิดชอบให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศอย่างเคร่งครัด และต้องดำเนินการให้มีการทบทวนนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้อง อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

ข้อ ๘ ให้ถือปฏิบัติตามเอกสารนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ ตามแนบท้ายประกาศนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๓ สิงหาคม พ.ศ. ๒๕๖๗

(นายเกรียงไกร ไชยศิริวงศ์สุข)

ผู้อำนวยการการท่าเรือแห่งประเทศไทย