แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สารบัญ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทรัพยากรทางทะเลและชายฝั่ง

๑. หลักการและเหตุผล

ระบบเทคโนโลยีสารสนเทศ เป็นสิ่งสำคัญยิ่งสำหรับองค์กร เป้นระบบงานที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อระหว่างกันในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ รวมไปถึงระบบงาน ระบบฐานข้อมูลที่เป็นหัวใจสำคัญยิ่งของหน่วยงาน และแม้ว่าระบบเทคโนโลยีสารสนเทศจะมีประโยชน์ มีความสำคัญ และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ ได้ แต่ในขณะเดียวกันยิ่งสำคัญก็ยิ่งมีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน

เนื่องจาก การจราจรที่เข้าออกของระบบมีการใช้งานด้านสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่างๆ มากเท่าใด ก็จะมีโอกาสหรือเปิดช่องให้ถูกบุกรุกโจมตีได้มากยิ่งขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น มาจากโปรแกรมที่ประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก นอกจากนี้ยังทำให้สูญเสียชื่อเสียงหรือภาพพจน์ ความเชื่อมั่นของหน่วยงานอีกด้วย ดังนั้น กรมทรัพยากรทางทะเลและชายฝั่งในฐานะเจ้าของระบบงานสารสนเทศทั้งหมดจะต้องให้ความตระหนักถึงการดูแลบำรุงรักษา การควบคุม การเตรียมพร้อม การเฝ้าระวัง และรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีประสิทธิภาพในขั้นสูง

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ

จากสภาพการปฏิบัติงาน ความเสี่ยง และข้อกฎหมายที่เกี่ยวข้อง กรมทรัพยากรทางทะเลและชายฝั่งจึงได้ปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานขึ้นใหม่ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ มากขึ้น เพื่อให้รองรับการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ของกรมได้อย่างมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมาย และตามระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตาม การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากทุกหน่วยและต้องดำเนินการอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และสามารถปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว ศูนย์สารสนเทศฯ ในฐานะหน่วยงานที่กำกับดูแลหวังเป็นอย่างยิ่งว่า แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่งทุกคน ใช้เป็นแนวทางปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของกรมทรัพยากรทางทะเลและชายฝั่งที่มีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมทรัพยากรทางทะเลและชายฝั่งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศ และนำไปปฏิบัติตามโดยเคร่งครัด

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของกรมทรัพยากรทางทะเลและชายฝั่ง

๓.๒ กำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสม หากพบการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓ เน้นกำกับดูแลการดำเนินงาน เพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๔ เผยแพร่ความรู้ ความเข้าใจ เพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้อง ทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๓.๕ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

๔. องค์ประกอบของนโยบาย

๔.๑ คำนิยาม
๔.๒ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
๔.๓ การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
๔.๔ การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
๔.๕ การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
๔.๖ การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์
๔.๗ การรักษาความมั่นคงปลอดภัยของอีเมล์
๔.๘ การรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต
๔.๙ การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
๔.๑๐ ความมั่นคงปลอดภัยของการสำรองข้อมูล
๔.๑๑ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ