ประกาศกรมประมง

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมประมง

(Information Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมประมง หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรและหน่วยงานในสังกัด องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีขอบเขต วัตถุประสงค์และนโยบายดังนี้

๑. ขอบเขตการดำเนินการ

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กรมประมง มีขอบเขตครอบคลุมการบริหารจัดการ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา และการใช้งานระบบเครือข่ายอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์ รวมถึงการสอบทานการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ซึ่งอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Annex A และวิธีปฏิบัติทางเทคนิคจาก ISO/IEC ๑๗๗๙๙:๒๐๐๕

นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินผลการปฏิบัติเพื่อปรับปรุงนโยบายอย่างน้อย ๑ ครั้งต่อปี

๒. วัตถุประสงค์

๑) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒) เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๓) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

/๓. นโยบาย...

๓. นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๓.๑ นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

(๑) ด้านการควบคุมการเข้าถึงอาคารสถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๑) กำหนดมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

๒) จัดให้มีเวรยามรักษาอาคาร และห้องควบคุมระบบเครือข่ายและอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายในเพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูลและระบบเครือข่าย

๓) การเข้าถึงอาคารของหน่วยงานภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชนใบอนุญาตขับขี่ เป็นต้น เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในเอกสาร “บันทึกการเข้า-ออกพื้นที่”

๔) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้า-ออกพื้นที่ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕) รณรงค์หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงาน เพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

(๒) ด้านการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่าย

๑) ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย มีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่”

๒) เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่าย

๓) การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออกทุกคนต้องกรอกแบบฟอร์มดังกล่าวทุกครั้ง

๔) ผู้ติดต่อจากหน่วยงานภายนอก ต้องแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” และในการเข้าห้องควบคุมระบบเครือข่ายเจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

/๓.๒ นโยบาย...

๓.๒ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(๑) ด้านการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่กรมประมง

๑) ต้องมีการกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิ์ต่างๆ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

๒) ผู้ดูแลระบบต้องตรวจสอบการอนุมัติการกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเตอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ ทุก ๖ เดือนเป็นอย่างน้อย

๓) ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์และการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน การทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัย

๔) การบริหารจัดการการเข้าถึงระดับเครือข่าย ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายแบบแบ่งโซนเพื่อการควบคุมและป้องกันการบุกรุก ต้องมีการกำหนดเส้นทางการเชื่อมต่อของระบบเครือข่ายทั้งหมดในองค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกองค์กร โดยต้องผ่านระบบรักษาความปลอดภัย เช่น Firewall, IPS/IDS, Proxy, การตรวจสอบไวรัส เป็นต้น

๕) การเข้าสู่ระบบงานเครือข่ายภายในองค์กรผ่านทางอินเตอร์เน็ต ต้องมีการ Login และมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๖) ผู้ใช้ต้องใช้เครือข่ายสารสนเทศอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่เกินไป หรือดูหนังฟังเพลงออนไลน์ในระหว่างเวลาปฏิบัติงาน ซึ่งเป็นเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น

๗) ผู้ใช้ต้องรับผิดชอบระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งผู้ใช้ต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่าย หรือเข้าถึงระบบสารสนเทศจากบัญชีผู้ใช้ของตนเอง

๘) การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์สารสนเทศ ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งานระบบจากภายนอก กรณีผู้ใช้เข้าสู่ระบบจากระยะไกล (Remote access) โดยการกำหนดสิทธิ์ การควบคุมพอร์ต (Port) และพิสูจน์ยืนยันตัวตน (Authentication) โดยการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบความถูกต้อง

(๒) ด้านการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อขออนุมัติจากผู้อำนวยการศูนย์สารสนเทศ กรมประมง

๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

/๓) สำหรับ...

๓) สำหรับโครงการขนาดใหญ่ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๔) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

(๓) ด้านการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา

๑) กำหนดให้ใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินขององค์กรอย่างมีประสิทธิภาพ และโปรแกรมที่ติดตั้งต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๒) กำหนดให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์ รวมทั้ง Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver ในระหว่างเวลาพักกลางวันและหลังเลิกงาน

๓) ผู้ใช้ต้องรับผิดชอบในการตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive และ External Harddisk อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ตรวจสอบหาไวรัสจากเครื่องคอมพิวเตอร์ที่ใช้งาน รวมทั้งตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ต

๔) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Harddisk เป็นต้น และจัดเก็บไว้ในสถานที่ที่เหมาะสม

๓.๓ นโยบายการใช้งานระบบเครือข่ายอินเตอร์เน็ต และจดหมายอิเล็กทรอนิกส์

(๑) ด้านการควบคุมการใช้งานระบบเครือข่ายอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๑) ผู้ดูแลระบบต้องมีการกำหนดสิทธิ์การเข้าถึงระบบอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์ เฉพาะบัญชีผู้ใช้ที่มีสิทธิ์เท่านั้น (User Authentication)

๒) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Proxy, Firewall, IPS/IDS เป็นต้น

๓) กำหนดแนวทางปฏิบัติการใช้งานระบบอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์ที่ถูกต้อง โดยผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๔) ต้องมีการเก็บข้อมูลการเข้าถึงระบบ (Log File) และข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data)

/(๒) ด้าน...

(๒) ด้านการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑) ผู้ดูแลระบบจะต้องกำหนดบัญชีผู้ใช้ รหัสผ่าน และสิทธิ์ผู้ใช้งาน ในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan)

๒) กรณีที่องค์กรมีนโยบายในการใช้ชื่อผู้ใช้กลางให้ผู้ใช้งานติดต่อเจ้าหน้าที่ของศูนย์สารสนเทศ เพื่อรับค่า SSID (Service Set Identifier) และ Network Key ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

๓) ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม และลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง เพื่อควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับ-ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๓) ด้านการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑) ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ผู้ใช้งานต้องรับผิดชอบในการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

๒) ผู้ดูแลระบบต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่นำมาเชื่อมต่อกับระบบเครือข่ายเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตราย รวมทั้งมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

(๔) ด้านการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑) อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งาน ปิดบริการรวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบนไฟร์วอลล์ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท network scanning tools เช่น Nmap เป็นต้น

๒) ใช้ไฟร์วอลล์หลายชนิดร่วมกัน เช่น ไฟร์วอลล์แบบกรองแพ็กเก็ต ไฟร์วอลล์แบบพร็อกซี่ เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็กเก็ตที่ผ่านเข้ามาในเครือข่ายองค์กร

๓) ใช้ระบบอื่นทำงานร่วมกับไฟร์วอลล ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมล์และกรองเว็บ (Anti spam) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมได้สูงขึ้น

๔) ตรวจสอบว่ากฎที่กำหนดไว้บนไฟร์วอลล์ไม่มีข้อใดขัดแย้งกับนโยบายความมั่นคงปลอดภัยขององค์กร หมั่นตรวจสอบกฎของไฟร์วอลล์เพื่อกำจัดกฎที่ไม่มีความจำเป็นทิ้งไป ซึ่งเป็นการเพิ่มประสิทธิภาพการประมวลผลกฎของไฟร์วอลล์ที่กำหนดไว้

(๕) ด้านการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

๑) ผู้ดูแลระบบต้องสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร โดยเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร และจัดเก็บไว้ในสถานที่ที่เหมาะสม

๒) ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือสำรองข้อมูลของระบบที่อยู่ในความรับผิดชอบตามความเหมาะสมของแต่ละระบบ ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

/๓) ผู้ใช้...

๓) ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป ต้องสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๔) ผู้ดูแลระบบต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์/ซอฟต์แวร์ เพื่อให้สามารถฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้น จากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ

๓.๔ นโยบายการสอบทานการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

กำหนดให้มีการสอบทานระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ ว่าสอดคล้องกับนโยบายหรือไม่ โดยรายงานสรุปผลอย่างน้อยทุก ๖ เดือน ให้ CIO ทราบ พร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๓๑ สิงหาคม พ.ศ. ๒๕๕๔

(นางนันทิยา อุ่นประเสริฐ)
รองอธิบดีกรมประมง
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง