ประกาศกรมประมง

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมง พ.ศ. ๒๕๕๖ (Information Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมประมง หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินงานใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ มาตรา ๗ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลบังคับใช้ได้ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมประมง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมง พ.ศ. ๒๕๕๖”

ข้อ ๒ ขอบเขตการดำเนินการ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมง มีขอบเขตครอบคลุมการบริหารจัดการ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา การใช้งานระบบเครือข่ายอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์ การป้องกันระบบเครือข่ายและตรวจจับการบุกรุก การสำรองและกู้คืนข้อมูล การสอบทานการปฏิบัติตามนโยบาย รวมถึงการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอ้างอิงตามมาตรฐาน ISO/IEC 27001 Annex A และวิธีปฏิบัติทางเทคนิคจาก ISO/IEC 17799:2005

ข้อ ๓ วัตถุประสงค์...

ข้อ ๓ วัตถุประสงค์

(๑) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

(๒) เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

(๓) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

ข้อ ๔ ในประกาศนี้

(๑) องค์กร หมายถึง กรมประมง

(๒) ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

(๓) ศูนย์สารสนเทศ หมายถึง ศูนย์สารสนเทศ เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร

(๔) ผู้อำนวยการศูนย์สารสนเทศ หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

(๕) การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

(๖) มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

(๗) วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

(๘) แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

(๙) ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้

๑) ผู้บริหาร หมายถึง อธิบดี รองอธิบดี ผู้เชี่ยวชาญ ผู้ตรวจราชการกรมประมง ผู้อำนวยการสำนักฯ กองฯ ศูนย์ฯ สถานีฯ ประมงจังหวัด หัวหน้าหน่วยงานราชการ

๒) ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๓) เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำและเจ้าหน้าที่ประจำโครงการขององค์กร

(๑๐) สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๑๑) หน่วยงาน...

(๑๑) หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมประมงอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๑๒) ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

(๑๓) สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

(๑๔) ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๑๕) ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น

๑) ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๒) ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

(๑๖) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

(๑๗) พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

๑) พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

๒) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)

๔) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

๕) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)

(๑๘) เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

(๑๙) สินทรัพย์...

(๑๙) สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

(๒๐) จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน มาตรฐานที่ใช้ในการรับ - ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP เป็นต้น

(๒๑) รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒๒) ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๒๓) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๒๔) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๒๕) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๒๖) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๕ องค์ประกอบนโยบาย

(๑) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๑) กำหนดมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

๒) จัดให้มีเวรยามรักษาอาคาร และห้องควบคุมระบบเครือข่ายและอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายใน เพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูลและระบบเครือข่าย

๓) การเข้าถึงอาคารของหน่วยงานภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในเอกสาร “บันทึกการเข้า - ออกพื้นที่”

๔) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้า - ออกพื้นที่ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕) รณรงค์หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงาน เพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

(๒) นโยบายการควบคุมการเข้า - 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 บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่” และในการเข้าห้องควบคุมระบบเครือข่าย เจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

(๓) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ด้านการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่กรมประมง

๑) ต้องมีการกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิ์ต่าง ๆ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

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

๓) ผู้ดูแลระบบ...

๓) ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์และการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน การทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัย

๔) เจ้าของข้อมูล และ “เจ้าของระบบงาน” ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น และการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๕) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

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

๓.๒ ด้านการควบคุมการเข้าถึงระบบเครือข่าย

๑) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒) การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเตอร์เน็ตหรืออินทราเน็ต ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์สารสนเทศก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๓) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๔) ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กร ต้องเชื่อมต่อผ่าน Firewall หรือ Hardware อื่น ๆ ที่มีคุณสมบัติป้องกันการบุกรุกหรือการทำ Packet Filtering

๕) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๖) การเข้าสู่ระบบงานเครือข่ายภายในองค์กรผ่านทางอินเตอร์เน็ต ต้องมีการ Login และมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๗) ผู้ใช้ต้องใช้เครือข่ายสารสนเทศอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่เกินไป หรือดูหนังฟังเพลงออนไลน์ในระหว่างเวลาปฏิบัติงาน ซึ่งเป็นเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น

๘) ผู้ใช้...

๘) ผู้ใช้ต้องรับผิดชอบระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งผู้ใช้ต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่าย หรือเข้าถึงระบบสารสนเทศจากบัญชีผู้ใช้ของตนเอง

๙) IP Address ภายในของระบบงานเครือข่ายภายในขององค์กร ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์สารสนเทศและการสื่อสารได้โดยง่าย

๑๐) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์สารสนเทศเท่านั้น

๓.๓ ด้านการควบคุมการเข้าถึงระบบปฏิบัติการ

๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง และต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่ายมีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๐ นาที

๕) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๖) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๔ ด้านการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กร เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น

๒) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓) ต้องมี...

๓) ต้องมีการจำกัดระยะเวลาในการเชื่อมต่อระบบโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ รวมถึงมีการพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุก ๆ ๑ ชั่วโมง

๔) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ที่พัฒนาในรูปแบบ Webbase Application กำหนดให้เข้าถึงได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายภายใน

(๔) นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อขออนุมัติจากผู้อำนวยการศูนย์สารสนเทศ กรมประมง

๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

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

๔) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

(๕) นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา

๑) กำหนดให้ใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินขององค์กรอย่างมีประสิทธิภาพ และโปรแกรมที่ติดตั้งต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

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

๓) ผู้ใช้ต้องรับผิดชอบในการตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk Thumb Drive และ External Harddisk อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ตรวจสอบหาไวรัสจากเครื่องคอมพิวเตอร์ที่ใช้งาน รวมทั้งตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ต

๔) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Harddisk เป็นต้น และจัดเก็บไว้ในสถานที่ที่เหมาะสม

(๖) นโยบาย...

(๖) นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

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)

(๗) นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

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

(๘) นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑) ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ผู้ใช้งานต้องรับผิดชอบในการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้น ๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

๒) ผู้ดูแลระบบต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่นำมาเชื่อมต่อกับระบบเครือข่ายเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตราย รวมทั้งมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

(๙) นโยบาย...

(๙) นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑) อนุญาตเฉพาะบริการเครือขายที่จำเปนตอการใชงาน ปดบริการรวมทั้งซอฟตแวร์ที่ไมจำเป็นบนไฟรวอลล์ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือขายดวยโปรแกรมประเภท Network Scanning Tools เชน Nmap เป็นต้น

(๙) นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑) อนุญาตเฉพาะบริการเครือขายที่จำเปนตอการใชงาน ปดบริการรวมทั้งซอฟตแวร์ที่ไมจำเป็นบนไฟรวอลล์ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือขายดวยโปรแกรมประเภท Network

๒) ใชไฟรวอลลหลายชนิดรวมกัน ได้แก่ ไฟรวอลลแบบกรองแพ็กเก็ต ไฟรวอลลแบบพร็อกซี่ เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็กเก็ตที่ผ่านเข้ามาในเครือข่ายองค์กร

๓) ใชระบบอื่นทำงานรวมกับไฟรวอลล ไดแก ระบบปองกันการบุกรุก (IPS) ไฟรวอลลส่วนตัว (Personal Firewall) โปรแกรมปองกันไวรัส (Antivirus) โปรแกรมกรองอีเมลและกรองเว็บ (Anti Spam) ซึ่งเปนการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมไดสูงขึ้น

๔) ตรวจสอบวากฎที่กำหนดไวบนไฟรวอลลไมมีขอใดขัดแยงกับนโยบายความมั่นคงปลอดภัยขององคกร หมั่นตรวจสอบกฎของไฟรวอลลเพื่อกำจัดกฎที่ไมมีความจำเป็นทิ้งไป ซึ่งเป็นการเพิ่มประสิทธิภาพการประมวลผลกฎของไฟรวอลลที่กำหนดไว้

(๑๐) นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

๑) ผู้ดูแลระบบต้องสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร โดยเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร และจัดเก็บไว้ในสถานที่ที่เหมาะสม

๒) ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือสำรองข้อมูลของระบบที่อยู่ในความรับผิดชอบตามความเหมาะสมของแต่ละระบบ ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๓) ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป ต้องสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

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

(๑๑) นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

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

๒) หัวหน้างาน...

๒) หัวหน้างานในแต่ละหน่วยงานต้องรับผิดชอบในการสอบทานอย่างสม่ำเสมอ ถึงการปฏิบัติงานให้สอดคล้องกับนโยบาย

๓) กำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบภายในหน่วยงานภาครัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง

(๑๒) นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑) กำหนดให้มีฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ

๒) ให้ความรู้เกี่ยวกับแนวปฏิบัติ โดยการจัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงานในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๓) ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ข้อ ๖ การกำหนดความรับผิดชอบ

(๑) ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศขององค์กร (CIO) เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมง และเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจาก ความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้อำนวยการศูนย์สารสนเทศ เป็นผู้รับผิดชอบติดตาม กำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

(๒) ระดับปฏิบัติ

๑) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ผู้รับผิดชอบ ได้แก่

๑. ศูนย์สารสนเทศ
๒. สำนักงานเลขานุการกรม
๓. สำนักวิจัยและพัฒนาประมงน้ำจืด
๔. สำนักวิจัยและพัฒนาประมงทะเล
๕. สำนักบริหารจัดการด้านการประมง
๖. สำนักพัฒนาและถ่ายทอดเทคโนโลยีการประมง
๗. กองตรวจสอบรับรองมาตรฐานคุณภาพสัตว์น้ำและผลิตภัณฑ์สัตว์น้ำ
๘. ผู้ดูแลระบบที่ได้รับมอบหมาย

๒) นโยบาย...

๒) นโยบายการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
   ๓. เจ้าหน้าที่ประจำโครงการขององค์กร

๔) นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
   ๓. เจ้าหน้าที่ประจำโครงการขององค์กร

๕) นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ใช้งาน

๖) นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์ ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
   ๓. ผู้ใช้งาน

๗) นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๘) นโยบายป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
   ๓. ผู้ใช้งาน

๙) นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐) นโยบายการสำรองและกู้คืนข้อมูล ผู้รับผิดชอบ ได้แก่
   ๑. ศูนย์สารสนเทศ
   ๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
   ๓. ผู้ใช้งาน

๑๑) นโยบาย...

๑๑) นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑. ศูนย์สารสนเทศ
๒. ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๒) นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑. ศูนย์สารสนเทศ
๒. ส่วนถ่ายทอดเทคโนโลยีการประมง สำนักพัฒนาและถ่ายทอดเทคโนโลยีการประมง
๓. ฝ่ายประชาสัมพันธ์ สำนักงานเลขานุการกรม
๔. หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
๕. ผู้ดูแลระบบที่ได้รับมอบหมาย
๖. เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๗ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๘ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมประมง” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ข้อ ๙ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑๑ กุมภาพันธ์ พ.ศ. ๒๕๕๖ เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กุมภาพันธ์ พ.ศ. ๒๕๕๖

(นายสุรจิตต์ อินทรชิต)
รองอธิบดีกรมประมง
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง