ประกาศกรมธนารักษ์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมธนารักษ์ พ.ศ. ๒๕๕๘

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมธนารักษ์ หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงเป็นการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กรและหน่วยงานในสังกัด และเพื่อให้การดำเนินงานเป็นไปตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งกำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ รวมถึงให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการ หรือหน่วยงานที่คณะกรรมการได้มอบหมาย จึงมีผลบังคับใช้ได้ กรมธนารักษ์จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กรโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กรมธนารักษ์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมธนารักษ์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมธนารักษ์ พ.ศ. ๒๕๕๘”

ข้อ ๒ วัตถุประสงค์

๒.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร สำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบ และเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

/ข้อ ๓ ในประกาศนี้...

ข้อ ๓ ในประกาศนี้

(๑) องค์กร หมายถึง กรมธนารักษ์

(๒) ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

(๓) ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) หมายถึง อธิบดีกรมธนารักษ์

(๔) ผู้บริหารระดับสูงสุดด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) หมายถึง รองอธิบดีกรมธนารักษ์

(๕) ศูนย์เทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงานสารสนเทศภายในองค์กร

(๖) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

(๗) การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับเทคโนโลยีสารสนเทศขององค์กร

(๘) มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย

(๙) วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

(๑๐) แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

(๑๑) ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ดังนี้

๑) ผู้บริหาร หมายถึง อธิบดี รองอธิบดี ที่ปรึกษาฯ ผู้เชี่ยวชาญ ผู้อำนวยการสำนัก/กอง/กลุ่ม/ศูนย์ และหัวหน้าหน่วยงานราชการในสังกัด

๒) ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์และระบบเครือข่ายซึ่งสามารถเข้าถึงโปรแกรมระบบคอมพิวเตอร์และระบบเครือข่ายเพื่อการจัดการฐานข้อมูล หรือข้อมูลของระบบคอมพิวเตอร์และระบบเครือข่าย

๓) เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราวและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร

(๑๒) สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

/(๑๓) หน่วยงานภายนอก...

(๑๓) หน่วยงานภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่องค์กรอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูล หรือทรัพย์สินต่างๆ ขององค์กร โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๑๔) ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

(๑๕) สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูล ที่นำมาประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่ายและสามารถไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

(๑๖) ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๑๗) ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการรับ – ส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบ Intranet ระบบ Internet เป็นต้น

๑) ระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในองค์กรเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในองค์กร

๒) ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ขององค์กรเข้ากับระบบเครือข่ายอินเทอร์เน็ตทั่วโลก

(๑๘) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานขององค์กรที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่องค์กรสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนในการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

(๑๙) พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace) หมายถึง พื้นที่ที่องค์กรอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

๑) พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน และอุปกรณ์ต่อพ่วงต่างๆ

๒) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย (IT Equipment or Network Area)

/๔) พื้นที่จัดเก็บ...

๔) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

๕) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)

(๒๐) เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

(๒๑) สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

(๒๒) ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน

(๒๓) รหัสผ่าน (Password) หมายถึง ชุดตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒๔) ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๒๕) การเข้าถึง หรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๒๖) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๒๗) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๒๘) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted

/or Unexpected...

or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศขององค์กรถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ องค์ประกอบนโยบาย

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศ

(๑) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๑) กำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

๒) จัดให้มีเวรยามรักษาอาคารและห้องควบคุมระบบเครือข่ายและอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายใน เพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูลและระบบเครือข่าย

๓) การเข้าถึงอาคารของหน่วยงานภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในเอกสาร “บันทึกการเข้า - ออกพื้นที่”

๔) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕) รณรงค์ หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงาน เพื่อใช้ระบุตัวตนก่อนเข้าอาคาร หรือสถานที่สำคัญขององค์กร

(๒) นโยบายการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย

๑) ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องกำหนดสิทธิบุคคลในการเข้า - ออกห้องควบคุมระบบเครือข่าย มีการบันทึก “ทะเบียนผู้มีสิทธิเข้า - 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”และในการเข้าห้องควบคุมระบบเครือข่ายเจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และต้องคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

/(๓) นโยบายการควบคุม...

(๓) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) ต้องมีการกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิต่างๆ สอดคล้องกับหน้าที่ที่ได้รับมอบหมาย รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออก หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

๒) ผู้ดูแลระบบต้องตรวจสอบการอนุมัติการกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ ทุก ๖ เดือนเป็นอย่างน้อย

๓) ผู้ดูแลระบบต้องบริหารจัดการสิทธิและการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน การทบทวนสิทธิการใช้งานและตรวจสอบการละเมิดความปลอดภัย

๔) เจ้าของข้อมูล และ ผู้ดูแลระบบงาน ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบงานและข้อมูลได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น และการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจ

๕) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๖) การควบคุมการเข้าใช้งานระบบจากภายนอก (Remote Access) ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งานระบบจากภายนอก โดยต้องทำการกำหนดสิทธิ ควบคุมพอร์ต (Port) และพิสูจน์ยืนยันตัวตน (Authentication) โดยการป้อนชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบความถูกต้อง

(๔) นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ กรมธนารักษ์

๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญา หรือข้อตกลงการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาหรือข้อตกลงต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓) สำหรับงานลักษณะโครงการ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของหน่วยงานภายนอก ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๔) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

/(๕) นโยบายการควบคุม...

(๕) นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

๑) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒) การเข้าสู่ระบบเครือข่ายภายในองค์กร โดยผ่านทางระบบเครือข่ายอินเทอร์เน็ต ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ก่อนการเข้าใช้งานในทุกกรณี

๓) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายในส่วนที่ได้รับอนุญาตเท่านั้น

๔) ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกองค์กร ต้องเชื่อมต่อผ่าน Firewall หรือ Hardware อื่นๆ ที่มีคุณสมบัติป้องกันการบุกรุก หรือการทำ Packet Filtering

๕) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กร โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงค่าการทำงานของระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๖) การเข้าสู่ระบบเครือข่ายภายในองค์กรผ่านทางระบบเครือข่ายอินเทอร์เน็ต ต้องมีการ Login เพื่อพิสูจน์ยืนยันตัวตน (Authentication) และเพื่อตรวจสอบความถูกต้อง

๗) ผู้ใช้งานต้องใช้เครือข่ายสารสนเทศอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่เกินไป หรือดูหนังฟังเพลงออนไลน์ในระหว่างเวลาปฏิบัติงาน ซึ่งเป็นเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น

๘) ผู้ใช้งานต้องรับผิดชอบและระมัดระวังความปลอดภัยในการใช้เครือข่ายโดยเฉพาะอย่างยิ่งผู้ใช้งานต้องไม่ยอมให้ผู้อื่นเข้าใช้เครือข่าย หรือเข้าถึงระบบสารสนเทศจากบัญชีผู้ใช้งานของตนเอง

๙) IP Address ของระบบเครือข่ายภายในองค์กร ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบสารสนเทศขององค์กรได้โดยง่าย

๑๐) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศหรือเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบเท่านั้น

(๖) นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๒) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้งและต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

/๓) ผู้ใช้งาน...

๓) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งาน หรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบปฏิบัติการ อุปกรณ์เครือข่ายมีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

๕) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบปฏิบัติการ ทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

(๗) นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ

๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กรเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น

๒) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญโดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓) ต้องมีการจำกัดระยะเวลาในการเชื่อมต่อระบบโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศรวมถึงมีการพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุกๆ ๑ ชั่วโมง หรือตามความเหมาะสมของลักษณะงาน

๔) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ที่พัฒนาในรูปแบบ Web Based Application กำหนดให้เข้าถึงได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายภายใน

๕) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๘) นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพา

๑) กำหนดให้ใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินขององค์กรอย่างมีประสิทธิภาพและโปรแกรมที่ติดตั้งต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๒) กำหนดให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานเครื่อง-คอมพิวเตอร์ รวมทั้ง Logout ออกจากเครื่องคอมพิวเตอร์และล็อกหน้าจอด้วยโปรแกรม Screen Saver ในระหว่างเวลาพักกลางวันและหลังเลิกงาน

๓) ผู้ใช้งานต้องรับผิดชอบในการตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Thumb Drive และ External Hard Disk อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ตรวจสอบหาไวรัสจากเครื่องคอมพิวเตอร์ที่ใช้งาน รวมถึงตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากระบบเครือข่ายอินเทอร์เน็ต

๔) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น และจัดเก็บไว้ในสถานที่ที่เหมาะสม

/(๙) นโยบายการควบคุม...

(๙) นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและระบบจดหมายอิเล็กทรอนิกส์

๑) ผู้ดูแลระบบต้องมีการกำหนดสิทธิการเข้าถึงระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์เฉพาะบัญชีผู้ใช้งานที่มีสิทธิเท่านั้น

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

๓) กำหนดแนวทางปฏิบัติในการใช้งานระบบเครือข่ายอินเทอร์เน็ตและระบบจดหมายอิเล็กทรอนิกส์ โดยผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร หรือผิดกฎหมาย

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

(๑๐) นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑) ผู้ดูแลระบบจะต้องกำหนดบัญชีผู้ใช้งาน รหัสผ่าน และสิทธิผู้ใช้งาน ในการเข้าใช้งานระบบเครือข่ายไร้สาย (Wireless Lan)

๒) กรณีที่องค์กรมีนโยบายในการใช้ชื่อผู้ใช้งานกลางให้ผู้ใช้งานติดต่อเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศเพื่อรับค่า SSID (Service Set Identifier) และ (Network Key) ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

๓) ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมและลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง เพื่อควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งานและป้องกันไม่ให้ผู้โจมตีสามารถรับ - ส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

(๑๑) นโยบายการป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑) ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในองค์กร ผู้ใช้งานต้องรับผิดชอบในการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นๆ ไม่มีไวรัสคอมพิวเตอร์ หรือซอฟต์แวร์อันตรายแฝงอยู่

๒) ผู้ดูแลระบบต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่นำมาเชื่อมต่อกับระบบเครือข่ายเพื่อตรวจหาไวรัสและซอฟต์แวร์อันตราย รวมทั้งมีการปรับปรุงโปรแกรมป้องกันไวรัส และฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตราย หรือไวรัสคอมพิวเตอร์

(๑๒) นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

๑) อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งาน ปิดบริการ รวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบนไฟร์วอลล์ ไม่อนุญาตให้สแกนเพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools ต่างๆ

/๒) ใช้ไฟร์วอลล์...

๒) ใช้ไฟร์วอลล์หลายชนิดรวมกัน ได้แก่ ไฟร์วอลล์แบบกรองแพ็คเกตไฟร์วอลล์แบบ Proxy เพื่อควบคุมการใช้งานเครือข่าย และกรอง Packet ที่ผ่านเข้า - ออก ระบบเครือข่ายขององค์กร

๓) ใช้ระบบรักษาความปลอดภัยอื่นทำงานรวมกับไฟร์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมล์ (Anti Spam) และกรองเว็บ (Web Filtering) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมให้มีประสิทธิภาพมากขึ้น

๔) ตรวจสอบกฎที่กำหนดไว้บนไฟร์วอลล์ ให้ไม่มีข้อใดขัดแย้งกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมถึงตรวจสอบกฎของไฟร์วอลล์เพื่อกำจัดกฎที่ไม่มีความจำเป็น ซึ่งเป็นการเพิ่มประสิทธิภาพการประมวลผลกฎของไฟร์วอลล์ที่กำหนดไว้

ส่วนที่ ๒ นโยบายการสำรอง การกู้คืนข้อมูล (Backup and Recovery Policy) และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๑) ผู้ดูแลระบบต้องสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร โดยเก็บรักษาไว้ตามแนวปฏิบัติการเก็บรักษาข้อมูลขององค์กร และจัดเก็บไว้ในสถานที่ที่เหมาะสม

๒) ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือสำรองข้อมูลของระบบที่อยู่ในความรับผิดชอบตามความเหมาะสมของแต่ละระบบ ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๓) ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป ต้องสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๔) ผู้ดูแลระบบต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์/ซอฟต์แวร์ เพื่อให้สามารถฟื้นฟูระบบข้อมูลจากความเสียหายที่อาจเกิดขึ้น หรือจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ

๕) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

ส่วนที่ ๓ นโยบายการตรวจสอบการดำเนินการตามนโยบาย แนวปฏิบัติ และการประเมินความเสี่ยงด้านสารสนเทศ

๑) กำหนดให้มีการตรวจสอบระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ ว่าสอดคล้องกับนโยบาย หรือไม่ โดยรายงานสรุปผลอย่างน้อยปีละ ๑ ครั้ง ให้ CEO ทราบ พร้อมเสนอแนะแนวทางการปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

๒) หัวหน้างานในแต่ละส่วนงานต้องรับผิดชอบในการตรวจสอบการปฏิบัติงานให้สอดคล้องกับนโยบายอย่างสม่ำเสมอ

๓) จัดให้มีการประเมินความเสี่ยงด้านสารสนเทศ และจัดทำรายงานสรุปผลอย่างน้อยปีละ ๑ ครั้ง โดยศูนย์เทคโนโลยีสารสนเทศ

/๔) กำหนดให้...

๔) กำหนดให้มีการตรวจสอบการประเมินความเสี่ยง โดยผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔ นโยบายการสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๑) กำหนดให้มีการฝึกอบรมการปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ

๒) ให้ความรู้เกี่ยวกับแนวปฏิบัติ โดยการจัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงานในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๓) สร้างการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ข้อ ๕ การกำหนดความรับผิดชอบ

(๑) ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้บริหารระดับสูงสุดด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบ ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

(๒) ระดับปฏิบัติ

๑) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ผู้รับผิดชอบ ได้แก่

๑.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑.๒) สำนักการคลัง

๑.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒) นโยบายการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

๒.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ และนโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

๓.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๓.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๓) บุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร

๔) นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

๔.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

/๔.๒) ผู้ดูแลระบบ...

๔.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๕) นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ ผู้รับผิดชอบ ได้แก่

๕.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๕.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๕.๓) ผู้ใช้งาน

๖) นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ผู้รับผิดชอบ ได้แก่

๖.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๖.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๗) นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ผู้รับผิดชอบ ได้แก่

๗.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๗.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๗.๓) ผู้ใช้งาน

๘) นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและระบบจดหมายอิเล็กทรอนิกส์ผู้รับผิดชอบ ได้แก่

๘.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๘.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๘.๓) ผู้ใช้งาน

๙) นโยบายควบคุมการเข้าถึงระบบเครือข่ายไร้สาย และนโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก ผู้รับผิดชอบ ได้แก่

๙.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๙.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐) นโยบายการป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี และนโยบายการสำรองและกู้คืนข้อมูล ผู้รับผิดชอบ ได้แก่

๑๐.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑๐.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐.๓) ผู้ใช้งาน

๑๑) นโยบายการตรวจสอบการดำเนินการตามนโยบายและแนวปฏิบัติ และการประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑๑.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑๑.๒) ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

/๑๑.๓) ผู้ดูแลระบบ...

๑๑.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๒) นโยบายการสร้างความรู้ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑๒.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑๒.๒) กองบริหารทรัพยากรบุคคล

๑๒.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๒.๔) เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๖ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งทบทวน ปรับปรุงนโยบายและแนวปฏิบัติฯ ตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๗ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมธนารักษ์” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ข้อ ๘ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑๕ มิถุนายน พ.ศ. ๒๕๕๘

(นายจักรกฤศฎิ์ พาราพันธกุล)
อธิบดีกรมธนารักษ์