



## ประกาศกรมชลประทาน

เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ  
กรมชลประทาน พ.ศ. ๒๕๕๖ (Information Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมชลประทาน หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กรและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินงานตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาคีรัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ ให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ มาตรา ๗ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลบังคับใช้ได้ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ผู้บริหารระดับสูงกรมชลประทาน จึงออกประกาศ ดังต่อไปนี้

**ข้อ ๑** ประกาศนี้เรียกว่า “ประกาศกรมชลประทาน เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศกรมชลประทาน พ.ศ. ๒๕๕๖”

**ข้อ ๒** ขอบเขตการดำเนินการ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศกรมชลประทาน มีขอบเขตรอบคลุมการบริหารจัดการ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา การใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ การป้องกันระบบเครือข่ายและตรวจจับการบุกรุก การสำรองและกู้คืนข้อมูล การสอบทานการปฏิบัติตามนโยบาย รวมถึงการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ Annex A และวิธีปฏิบัติทางเทคนิคจาก ISO/IEC ๑๗๗๙๙:๒๐๐๕

**ข้อ ๓** วัตถุประสงค์

(๑) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานในทั้งองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

(๒) เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

(๓) เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

ข้อ ๔ ในประกาศ...

ข้อ ๔ ในประกาศนี้

- (๑) องค์กร หมายถึง กรมชลประทาน
- (๒) ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- (๓) ผู้บริหารสูงสุด หมายถึง อธิบดีกรมชลประทาน
- (๔) CIO (Chief Information Officer) หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงขององค์กร (รองอธิบดีฝ่ายบริหาร เป็นผู้ได้รับมอบหมาย)
- (๕) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
- (๖) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ
- (๗) การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศขององค์กร
- (๘) มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- (๙) วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- (๑๐) แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- (๑๑) ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้
  - ๑) ผู้บริหาร หมายถึง อธิบดี รองอธิบดี ผู้เชี่ยวชาญ ผู้อำนวยการสำนักฯ กองฯ ศูนย์ฯ และหัวหน้าหน่วยงานราชการ
  - ๒) ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
  - ๓) เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร
- (๑๒) สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
- (๑๓) หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมชลประทานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- (๑๔) ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

(๑๕) สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

(๑๖) ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๑๗) ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือ การส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น

๑) ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ คอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยน ข้อมูลและสารสนเทศภายในหน่วยงาน

๒) ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

(๑๘) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงาน ของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การ พัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

(๑๙) 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)

(๒๐) เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของ ระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิด สูญหาย

(๒๑) สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

(๒๒) จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP3 และ IMAP เป็นต้น

(๒๓) รหัสผ่าน...

(๒๓) รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒๔) ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๒๕) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

(๒๖) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๒๗) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

#### ข้อ ๕ องค์ประกอบนโยบาย

(๑) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๑) กำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร

๒) จัดให้มีเวรยามรักษาอาคาร และห้องควบคุมระบบเครือข่ายและอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายใน เพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูลและระบบเครือข่าย

๓) การเข้าถึงอาคารของหน่วยงานภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตเข้าเป็นต้น เพื่อรับบัตรผู้ติดต่อ "Visitor" แล้วลงบันทึกข้อมูลในเอกสาร "บันทึกการเข้า - ออกพื้นที่"

๔) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕) รมรงค์หรือออกกฎให้เจ้าหน้าที่องค์กรแขวนบัตรพนักงาน เพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

(๒) นโยบายการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย

๑) ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องกำหนดสิทธิบุคคลในการเข้า - ออกห้องควบคุมระบบเครือข่าย มีการบันทึก “ทะเบียนผู้มีสิทธิเข้า - ออกพื้นที่”

๒) เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้า - ออกห้องควบคุมระบบเครือข่าย

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

๔) ผู้ติดต่อจากหน่วยงานภายนอก ต้องแลกบัตรที่ใช้ระบุตัวตน เช่นบัตรประจำตัวประชาชนหรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า - ออกพื้นที่” และในการเข้าห้องควบคุมระบบเครือข่ายเจ้าหน้าที่ผู้ดูแลระบบขององค์กรจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

(๓) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) ด้านการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่กรมชลประทาน

๑.๑) ต้องมีการกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิต่าง ๆ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

๑.๒) ผู้ดูแลระบบต้องตรวจสอบการอนุมัติการกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ ทุก ๖ เดือนเป็นอย่างน้อย

๑.๓) ผู้ดูแลระบบต้องบริหารจัดการสิทธิและการเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน การทบทวนสิทธิการใช้งาน และตรวจสอบการละเมิดความปลอดภัย

๑.๔) เจ้าของข้อมูล และ “เจ้าของระบบงาน” ต้องอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น และการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

๑.๕) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๖) การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งานระบบจากภายนอก ระยะไกล (Remote Access) โดยการกำหนดสิทธิ การควบคุมพอร์ต (Port) และพิสูจน์ยืนยันตัวตน (Authentication) โดยการป้อนชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบความถูกต้อง

๒) ด้านการควบคุม...

๒) ด้านการควบคุมการเข้าถึงระบบเครือข่าย

๒.๑) ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒.๒) การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ต หรือ อินทราเน็ต ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๒.๓) ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๔) ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกองค์กร ต้องเชื่อมต่อผ่าน Firewall หรือ Hardware อื่นๆ ที่มีคุณสมบัติป้องกันการบุกรุกหรือการทำ Packet Filtering

๒.๕) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒.๖) การเข้าสู่ระบบงานเครือข่ายภายในองค์กรผ่านทางอินเทอร์เน็ต ต้องมีการ Login และมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๗) ผู้ใช้งานต้องใช้เครือข่ายสารสนเทศอย่างมีประสิทธิภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่เกินไป หรือดูหนังฟังเพลงออนไลน์ในระหว่างเวลาปฏิบัติงาน ซึ่งเป็นเวลาที่มีการใช้เครือข่ายอย่างหนาแน่น

๒.๘) ผู้ใช้งานต้องรับผิดชอบระมัดระวังความปลอดภัยในการใช้เครือข่ายโดยเฉพาะอย่างยิ่งผู้ใช้งานต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่าย หรือเข้าถึงระบบสารสนเทศจากบัญชีผู้ใช้งานของตนเอง

๒.๙) IP Address ภายในของระบบงานเครือข่ายภายในองค์กร ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

๒.๑๐) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๓) ด้านการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๒) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง และต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๓) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๔) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ...

๓.๔) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่ายมีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที

๓.๕) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๑๕ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๓.๖) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สิ้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง เช่น ระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔) ด้านการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๔.๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์กรเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น

๔.๒) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญโดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๔.๓) ต้องมีการจำกัดระยะเวลาในการเชื่อมต่อระบบโปรแกรมประยุกต์ หรือแอปพลิเคชันและสารสนเทศ รวมถึงมีการพิสูจน์ตัวตน เพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุกๆ ๑ ชั่วโมง

๔.๔) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ที่พัฒนาในรูปแบบ Webbase Application กำหนดให้เข้าถึงได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายภายใน

(๔) นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑) บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมชลประทาน

๒) หน่วยงานภายนอกที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

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

๔) ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด และให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่กำหนดไว้

(๕) นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา

๑) กำหนดให้ใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินขององค์กรอย่างมีประสิทธิภาพ และโปรแกรมที่ติดตั้งต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๒) กำหนดให้ใช้ชื่อผู้ใช้งาน...

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

๓) ผู้ใช้งานต้องรับผิดชอบในการตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk Thumb Drive และ External Harddisk อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ ตรวจสอบหาไวรัสจากเครื่องคอมพิวเตอร์ที่ใช้งาน รวมทั้งตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต

๔) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Harddisk เป็นต้น และจัดเก็บไว้ในสถานที่ที่เหมาะสม

(๖) นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๑) ผู้ดูแลระบบต้องมีการกำหนดสิทธิการเข้าถึงระบบอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ เฉพาะบัญชีผู้ใช้งานที่มีสิทธิเท่านั้น (User Authentication)

๒) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Proxy Firewall IPS/IDS เป็นต้น

๓) กำหนดแนวทางปฏิบัติการใช้งานระบบอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ที่ถูกต้อง โดยผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

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

(๗) นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑) ผู้ดูแลระบบจะต้องกำหนดบัญชีผู้ใช้งาน รหัสผ่าน และสิทธิผู้ใช้งาน ในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan)

๒) กรณีที่องค์กรมีนโยบายในการใช้ชื่อผู้ใช้งานกลางให้ผู้ใช้งานติดต่อเจ้าหน้าที่ของคุณ์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อรับค่า SSID (Service Set Identifier) และ Network Key) ในการระบุตัวตน ก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

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

(๘) นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี

๑) ก่อนนำซอฟต์แวร์จากภายนอกมาใช้ภายในองค์กร ผู้ใช้งานต้องรับผิดชอบในการตรวจสอบซอฟต์แวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้นๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

๒) ผู้ดูแลระบบต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่นำมาเชื่อมต่อกับระบบเครือข่าย เพื่อตรวจหาไวรัสและซอฟต์แวร์อันตราย รวมทั้งมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลขององค์กร จากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

(๙) นโยบายป้องกันระบบเครือข่าย...



(๙) นโยบายป้องกันระบบเครือข่ายและตรวจจัดการบุกรุก

๑) อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งานปิดบริการ รวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบนไฟร์วอลล์ ไม่อนุญาตให้สแกน เพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools เช่น Nmap เป็นต้น

๒) ใช้ไฟร์วอลล์หลายชนิดรวมกัน ได้แก่ ไฟร์วอลล์แบบกรองแพ็กเก็ต ไฟร์วอลล์แบบProxy เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็กเก็ตที่ผ่านเข้ามาในเครือข่ายองค์กร

๓) ใช้ระบบอื่นทำงานร่วมกับไฟร์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมลและกรองเว็บ (Anti Spam) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมได้สูงขึ้น

๔) ตรวจสอบกฎที่กำหนดไว้บนไฟร์วอลล์ไม่มีข้อขัดแย้งกับนโยบายความมั่นคงปลอดภัยขององค์กร หมั่นตรวจสอบกฎของไฟร์วอลล์เพื่อกำจัดกฎที่ไม่มีความจำเป็นทิ้งไป ซึ่งเป็นการเพิ่มประสิทธิภาพการประมวลผลกฎของไฟร์วอลล์ที่กำหนดไว้

(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

๕) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๑๑) นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑) กำหนดให้มีการสอบทานระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมถึงการปฏิบัติงาน ขั้นตอน และกระบวนการที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ว่าสอดคล้องกับนโยบายหรือไม่ โดยรายงานสรุปผลอย่างน้อยปีละครั้ง ให้ CIO ทราบ พร้อมเสนอแนะแนวทางปรับปรุงแก้ไขในกรณีที่พบว่าระบบการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีจุดบกพร่อง

๒) หัวหน้างานในแต่ละหน่วยงานต้องรับผิดชอบในการสอบทานอย่างสม่ำเสมอถึงการปฏิบัติงานให้สอดคล้องกับนโยบาย

๓) จัดให้มี “การประเมินความเสี่ยงด้านสารสนเทศ” และจัดทำรายงานสรุปผลอย่างน้อยปีละ ๑ ครั้ง โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔) กำหนดให้มีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง

(๑๒) นโยบายการสร้างความตระหนัก...

(๑๒) นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑) กำหนดให้มีการฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ

๒) ให้ความรู้เกี่ยวกับแนวปฏิบัติ โดยการจัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงานในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๓) ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ข้อ ๖ การกำหนดความรับผิดชอบ

(๑) ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

กำหนดให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบ ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

(๒) ระดับปฏิบัติ

๑) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ผู้รับผิดชอบ ได้แก่

๑.๑) ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

๑.๒) สำนักงานเลขานุการกรม

๑.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๒) นโยบายการควบคุมการเข้า - ออกห้องควบคุมระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

๒.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

๓.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๓) เจ้าหน้าที่ประจำโครงการขององค์กร

๔) นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๓) เจ้าหน้าที่ประจำโครงการขององค์กร

๕) นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา

ผู้รับผิดชอบ ได้แก่

๕.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๕.๒) ผู้ใช้งาน

๖) นโยบายการควบคุมการใช้งาน...

๖) นโยบายการควบคุมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ ผู้รับผิดชอบ ได้แก่

- ๖.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๖.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๖.๓) ผู้ใช้งาน

๗) นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้รับผิดชอบ ได้แก่

- ๗.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๗.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๘) นโยบายป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี ผู้รับผิดชอบ ได้แก่

- ๘.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๘.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๘.๓) ผู้ใช้งาน

๙) นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก ผู้รับผิดชอบ ได้แก่

- ๙.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๙.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๐) นโยบายการสำรองและกักเก็บข้อมูล ผู้รับผิดชอบ ได้แก่

- ๑๐.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๑๐.๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๑๐.๓) ผู้ใช้งาน

๑๑) นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

- ๑๑.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๑๑.๒) ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก

(External Auditor)

- ๑๑.๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๑๒) นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

- ๑๒.๑) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ๑๒.๒) สำนักงานเลขานุการกรม
- ๑๒.๓) หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
- ๑๒.๔) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๑๒.๕) เจ้าหน้าที่ที่ได้รับมอบหมาย

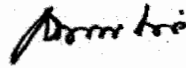
ข้อ ๗ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบาย และ ข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปี

ข้อ ๘ องค์ประกอบของนโยบาย...

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

ข้อ ๙ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑๗ ตุลาคม พ.ศ. ๒๕๕๖ เป็นต้นไป

ประกาศ ณ วันที่ ๑๗ ตุลาคม พ.ศ. ๒๕๕๖



(นายเลิศวิโรจน์ โกวัฒนะ)  
อธิบดีกรมชลประทาน