นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
กรมส่งเสริมการปกครองท้องถิ่น พ.ศ. ๒๕๕๔

ด้วย กรมส่งเสริมการปกครองท้องถิ่นได้จัดให้มีระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศเพื่ออำนวยความสะดวกแก่เจ้าหน้าที่ในการปฏิบัติงาน ดังนั้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดจากการใช้งานเครือข่ายคอมพิวเตอร์และระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง กรมส่งเสริมการปกครองท้องถิ่นจึงกำหนดให้มีนโยบายเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีรายละเอียดดังต่อไปนี้

วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นได้ทราบถึงข้อปฏิบัติในการใช้งานระบบสารสนเทศให้เกิดความมั่นคงปลอดภัยไม่ละเมิดระเบียบกฎหมายหรือทำให้เกิดความเสียหายเนื่องมาจากการใช้งานระบบสารสนเทศ

ขอบเขต

ผู้ใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นทุกคน จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศกรมส่งเสริมการปกครองท้องถิ่น

นิยามคำศัพท์

"หน่วยงาน" หมายถึง หน่วยงานภายในสังกัดกรมส่งเสริมการปกครองท้องถิ่น

"เจ้าหน้าที่" หมายถึง ข้าราชการ พนักงานราชการ และลูกจ้างของหน่วยงานภายในสังกัดกรมส่งเสริมการปกครองท้องถิ่นหรือผู้ที่กรมส่งเสริมการปกครองท้องถิ่นมอบหมายให้ปฏิบัติงานตามสัญญาข้อตกลงหรือใบสั่งซื้อ

"ผู้ดูแลระบบ (System Administrator)" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

"ผู้ใช้งาน" หมายถึง ผู้ที่ได้รับอนุญาต (Authorized user) จากผู้ดูแลระบบให้สามารถเข้าใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"สารสนเทศ (Information)" หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือรูปภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย (Network System)" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบเครือข่ายภายใน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

"ระบบอินทราเน็ต (Intranet)" หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"ระบบอินเทอร์เน็ต (Internet)" หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)" หมายถึง ระบบงานของกรมส่งเสริมการปกครองท้องถิ่นที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากผู้ดูแลระบบให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"ชุดคำสั่งไม่พึงประสงค์" หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศ ของกรมส่งเสริมการปกครองท้องถิ่น พ.ศ. ๒๕๕๔ ประกอบด้วย ๗ หมวดดังนี้

หมวด ๑
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยการใช้งานระบบสารสนเทศอย่างถูกต้อง (Acceptable Use Policy)

๑.๑ การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑ ผู้ใช้งานต้องทำการลงทะเบียนเพื่อขอใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น และต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้งานร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานควรตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ ๔ ผู้ใช้งานต้องไม่นำรหัสผ่านที่เคยใช้มาแล้วกลับมาใช้งานใหม่

ข้อ ๕ ผู้ใช้งานควรเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น โดยมีแนวทางปฏิบัติดังนี้

(๑) กรณีที่ผู้ใช้งานมีเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น ควรมีการตั้งค่าชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ก่อนเข้าถึงระบบปฏิบัติการเพื่อพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบเครือข่ายของกรมส่งเสริมการปกครองท้องถิ่น ทั้งระบบอินเทอร์เน็ต (Internet) และระบบอินทราเน็ต (Intranet) ต้องทำการพิสูจน์ตัวตนโดยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สามารถบ่งบอกถึงตัวบุคคลได้

(๓) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ จะต้องทำการออกจากระบบโดยใช้คำสั่ง Lock หรือ Log Off หน้าจอทุกครั้ง

(๔) ผู้ใช้งานควรตั้งเวลาพักหน้าจอ (screen saver) เครื่องคอมพิวเตอร์ทุกเครื่องอย่างน้อย ๑๕ นาที

ข้อ ๗ หากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านหรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๑.๒ การบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๑ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของกรมส่งเสริมการปกครองท้องถิ่นซึ่งถูกกำหนดให้เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server Room) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมต่อเข้ากับระบบเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ ๕ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

ข้อ ๖ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่กรมส่งเสริมการปกครองท้องถิ่นมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของตนเอง

ข้อ ๗ ในกรณีที่ปฏิบัติงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่นที่ได้รับมอบหมาย

ข้อ ๘ ผู้ใช้งานต้องรับผิดชอบค่าเสียหายในกรณีที่ทรัพย์สินที่อยู่ในความรับผิดชอบนั้นชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของตน และหากมีการเปลี่ยนแปลงผู้ใช้งานเครื่องคอมพิวเตอร์นั้น จะต้องมีการบันทึกการเปลี่ยนแปลงไว้เป็นลายลักษณ์อักษร

ข้อ ๑๐ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่กรมส่งเสริมการปกครองท้องถิ่น จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้ในการปฏิบัติงานของกรมส่งเสริมการปกครองท้องถิ่นเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่กรมส่งเสริมการปกครองท้องถิ่นไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๑๑ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๐ ให้ถือเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๑.๓ การบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของกรมส่งเสริมการปกครองท้องถิ่น หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๒ ข้อมูลที่อยู่ภายในระบบคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น ถือเป็นทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น สามารถนำไปเผยแพร่ได้ ยกเว้นข้อมูลที่มีการจำกัดสิทธิการเข้าถึงข้อมูล ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกรมส่งเสริมการปกครองท้องถิ่น หรือข้อมูลของผู้รับบริการหากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิดหรือนำไปเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๔ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๕ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมส่งเสริมการปกครองท้องถิ่น จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมส่งเสริมการปกครองท้องถิ่นต้องการตรวจสอบข้อมูลที่คาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมส่งเสริมการปกครองท้องถิ่น ซึ่งผู้ดูแลระบบสามารถทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๑.๔ การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๑ ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือสุ่มรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๓) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๔) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความหรือรูปภาพ ที่ไม่เหมาะสมขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย ในกรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๒ ผู้ใช้งานห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent) อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๔ ผู้ใช้งานห้ามใช้ทรัพยากร ระบบการสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมส่งเสริมการปกครองท้องถิ่น ในการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรมความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๕ ผู้ใช้งานห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมส่งเสริมการปกครองท้องถิ่น ในการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๖ ผู้ใช้งานห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมส่งเสริมการปกครองท้องถิ่นเพื่อประโยชน์ทางการค้า

ข้อ ๗ ผู้ใช้งานห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๘ ผู้ใช้งานห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น ต้องหยุดชะงัก

ข้อ ๙ ผู้ใช้งานห้ามใช้ระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น เพื่อการควบคุมเครื่องคอมพิวเตอร์ หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๑๐ ผู้ใช้งานห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากร

ข้อ ๑๑ ผู้ใช้งานห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๑.๕ การใช้งานซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual property)

ข้อ ๑ กรมส่งเสริมการปกครองท้องถิ่น ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นกรมส่งเสริมการปกครองท้องถิ่นอนุญาตให้ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย เท่านั้น

ข้อ ๒ หากผู้ใช้งานมีความประสงค์จะให้ใช้ซอฟต์แวร์ประเภท Open Source สามารถรับการสนับสนุนทางเทคนิคได้จากศูนย์เทคโนโลยีสารสนเทศท้องถิ่น เพื่อใช้งานต่อไป

ข้อ ๓ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ กรมส่งเสริมการปกครองท้องถิ่นถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๔ ซอฟต์แวร์ (Software) ที่กรมส่งเสริมการปกครองท้องถิ่นได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑.๖ การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

ข้อ ๑ เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antl virus) ตามที่กรมส่งเสริมการปกครองท้องถิ่นได้กำหนดให้ใช้

ข้อ ๒ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๕ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทราบ

ข้อ ๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของกรมส่งเสริมการปกครองท้องถิ่น

๑.๗ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

ข้อปฏิบัติให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

๑.๘ บทลงโทษ

กรณีที่ผู้ใช้งานไม่ปฏิบัติตามนโยบายความมั่นคงดังกล่าว หรือก่อให้เกิดความเสียหายต่อบุคคลอื่นหรือต่อสมบัติของทางราชการ จะต้องรับโทษตามบทลงโทษต่อไปนี้

(๑) ระงับสิทธิการใช้งานเครือข่ายสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นตามระยะเวลาที่เหมาะสม

(๒) หากการละเมิดฝ่าฝืนนั้นก่อให้เกิดความเสียหาย ต่อผู้อื่น หรือต่อทรัพย์สินของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบและกฎหมายที่เกี่ยวข้อง

หมวด ๒
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point)

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายภายใน และระบบเครือข่ายไร้สายของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดทำรายงานผลการตรวจสอบทุกเดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้

สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้ดูแลระบบกรมส่งเสริมการปกครองท้องถิ่นทราบทันที

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของกรมส่งเสริมการปกครองท้องถิ่น

หมวด ๓
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบไฟร์วอลล์ (Firewall Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องเปิดใช้งานไฟร์วอลล์ (Firewall) ตลอดเวลา

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องบันทึกชื่อผู้เข้าใช้งานและรหัสผ่าน (Username and Password) เพื่อเป็นการตรวจสอบผู้ใช้ก่อนใช้งานระบบ และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้หรือแก้ไขเปลี่ยนแปลงข้อมูลในระบบไฟร์วอลล์ (Firewall)

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตตามนโยบาย (Policy)

ข้อ ๔ การเปลี่ยนแปลงการกำหนดค่า (Configuration) ทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์หรือการปรับตั้งค่าต่างๆ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๙ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๐ ผู้ดูแลระบบ (System Administrator) มีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๑ การเชื่อมต่อในลักษณะของการเข้าถึงเครือข่ายระยะไกล (Remote Login) จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

ข้อ ๑๒ หากมีการละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ ผู้ใช้งานจะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ข้อ ๑๓ หลังจากใช้งานระบบไฟร์วอลล์ (Firewall) เสร็จสิ้น ผู้ดูแลระบบ (System Administrator) จะต้องตัดการเชื่อมต่อกับระบบไฟร์วอลล์โดยการ Log out ออกจากระบบทุกครั้ง

หมวด ๔
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

ข้อ ๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้จะต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) โดยยื่นคำขอกับผู้ดูแลระบบ

ข้อ ๒ เมื่อผู้ใช้งานได้รับรหัสผ่าน (Password) ของระบบจดหมายอิเล็กทรอนิกส์ (E-mail) และมีการเข้าใช้งานระบบ ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที หลังจากการเข้าสู่ระบบในครั้งแรก

ข้อ ๓ ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๔ ผู้ใช้งานควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

ข้อ ๕ ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-mail) ของตน

ข้อ ๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) เสร็จสิ้นควรออกจากระบบโดยการ Log out ทุกครั้ง

ข้อ ๗ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-mail)

ข้อ ๘ ผู้ใช้งานควรตรวจสอบ Spam Mail ในกล่องจดหมายทุกครั้งที่ระบบหรือผู้ดูแลระบบแจ้งเตือน

ข้อ ๙ ผู้ใช้งานต้องไม่ใช้งาน E-mail ในทางที่อาจก่อให้เกิดความเสียหายต่อบุคคลหรือหน่วยงาน

หมวด ๕
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของระบบอินเทอร์เน็ต (Internet Security Policy)

ข้อ ๑ ผู้ใช้งานไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของกรมส่งเสริมการปกครองท้องถิ่น เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ผู้ใช้งานห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมส่งเสริมการปกครองท้องถิ่นที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ ผู้ใช้งานควรระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานไม่ควรเปิดเผยข้อมูลที่สำคัญและเป็นความลับของกรมส่งเสริมการปกครองท้องถิ่น

ข้อ ๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมส่งเสริมการปกครองท้องถิ่น การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เรียบร้อยแล้ว ผู้ใช้งานควรตัดการเชื่อมต่อระบบโดยการ Log out ออกจากระบบอินเทอร์เน็ตทุกครั้ง เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

หมวด ๖
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control Policy)

๖.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ กรมส่งเสริมการปกครองท้องถิ่น กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศ เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่นจะต้องขออนุญาตเป็นลายลักษณ์อักษร

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น และตรวจสอบการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๖.๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของกรมส่งเสริมการปกครองท้องถิ่น ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออกการพ้นจากตำแหน่งหรือการย้ายหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะ การปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของผู้ใช้งานดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยและควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่ไม่มีการป้องกันการเข้าถึงข้อมูล

(๕) การกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับพิจารณาจากผู้ดูแลระบบ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานแตกต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภท ชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานต่างๆ

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนที่แท้จริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูลได้

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๕) ควรกำหนดให้มีการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดและระดับความสำคัญของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมส่งเสริมการปกครองท้องถิ่น เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งไปตรวจซ่อม เป็นต้น

หมวด ๗
นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
ว่าด้วยความมั่นคงปลอดภัยของการตรวจจับการบุกรุก
(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในของกรมส่งเสริมการปกครองท้องถิ่น ให้มีความมั่นคงปลอดภัย และเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกรมส่งเสริมการปกครองท้องถิ่น และข้อมูลในเครือข่ายทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลการจราจรคอมพิวเตอร์ พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้ดูแลระบบทราบภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๓ กรมส่งเสริมการปกครองท้องถิ่น มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งให้ผู้ใช้งานทราบล่วงหน้า

ข้อ ๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของกรมส่งเสริมการปกครองท้องถิ่น การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบสารสนเทศของกรมส่งเสริมการปกครองท้องถิ่น จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ประกาศ ณ วันที่ ๑๑ สิงหาคม พ.ศ.๒๕๕๔

(นายวีระวัฒน์ ชื่นวาริน)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง