ประกาศเทศบาลเมืองวังสะพุง
เรื่อง แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของเทศบาลเมืองวังสะพุง พ.ศ. ๒๕๖๙

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับ เทศบาลเมืองวังสะพุงเล็งเห็นถึงความสำคัญ จึงกำหนดแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลเมืองวังสะพุง เพื่อเป็นเครื่องมือให้กับผู้ใช้งานผู้ดูแลระบบ และเกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของเทศบาลเมืองวังสะพุง โดยความเห็นชอบของนายกเทศมนตรีเมืองวังสะพุง โดยมีรายละเอียดดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศเทศบาลเมืองวังสะพุง เรื่อง แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลเมืองวังสะพุง พ.ศ. ๒๕๖๙”

ข้อ ๒ วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบสารสนเทศของเทศบาลเมืองวังสะพุงได้ทราบถึงข้อปฏิบัติ ในการใช้งานระบบสารสนเทศให้เกิดความมั่นคงปลอดภัยไม่ละเมิดระเบียบกฎหมายหรือทำให้เกิดความเสียหายเนื่องมาจากการใช้งานระบบสารสนเทศ

ข้อ ๓ ขอบเขต

ผู้ใช้งานระบบสารสนเทศของเทศบาลเมืองวังสะพุงทุกคน จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศเทศบาลเมืองวังสะพุง

ข้อ ๔ นิยามคำศัพท์

“หน่วยงาน” หมายถึง ส่วนราชการในสังกัดเทศบาลเมืองวังสะพุง

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานจ้าง และลูกจ้างของหน่วยงานในสังกัดเทศบาลเมืองวังสะพุงหรือผู้ที่เทศบาลเมืองวังสะพุงมอบหมายให้ปฏิบัติงาน

“ผู้ใช้งาน...

"ผู้ใช้งาน (User)" หมายถึง ผู้ที่ได้รับอนุญาตจากผู้ดูแลระบบให้สามารถเข้าใช้งานระบบสารสนเทศของเทศบาลเมืองวังสะพุง

"ผู้ดูแลระบบ (System Administrator)" หมายถึง บุคคลที่ทำหน้าที่บริหารจัดการ และดูแลเครือข่ายคอมพิวเตอร์และบัญชีผู้ใช้งานภายในเครือข่ายคอมพิวเตอร์ขององค์กร

"ข้อมูลคอมพิวเตอร์ (Data)" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"สารสนเทศ (Information)" หมายถึง ข้อเท็จจริงได้จาการนำข้อมูลมาผ่านประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือรูปภาพให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

"ระบบคอมพิวเตอร์ (Computer System)" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของ คอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย (Network System)" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร (Local Area Network : LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet) เป็นต้น

"ระบบอินทราเน็ต (Intranet)" หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"ระบบอินเตอร์เน็ต (Internet)" หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)" หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

"ชุดคำสั่งไม่พึงประสงค์" หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบ คอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือ ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

แนวนโยบาย...

แนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลเมืองวังสะพุง ประกอบด้วย ๗ หมวด ดังนี้

หมวด ๑
การใช้งานระบบสารสนเทศอย่างถูกต้อง (Acceptable Use Policy)

๑.๑ การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานควรตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet)

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว

ข้อ ๕ ผู้ใช้งานควรเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๓ – ๖ เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของเทศบาลเมืองวังสะพุง ดังนี้

(๑) กรณีที่ผู้ใช้งานมีเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของเทศบาลเมืองวังสะพุงควรมีการตั้งค่าชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ก่อนเข้าถึงระบบปฏิบัติการ เพื่อพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบเครือข่ายของเทศบาลเมืองวังสะพุง ทั้งระบบอินเตอร์เน็ต (Internet) และระบบอินทราเน็ต (Intranet) ต้องทำการพิสูจน์ตัวตนโดยผู้ใช้งาน (Username) และรหัสผ่าน (Password) สามารถบ่งบอกถึงตัวบุคคลได้

(๓) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการออกจากระบบโดยใช้คำสั่ง Lock หรือ Sign out หรือ Log out รวมถึงปิดหน้าจอและปิดเครื่องคอมพิวเตอร์ทุกครั้ง เพื่อปฏิบัติตาม นโยบายการลดพลังงานไฟฟ้าของเทศบาลเมืองวังสะพุง

ข้อ ๗ หากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่าน หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๑.๒ การบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๑ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของเทศบาลเมืองวังสะพุงที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒ ผู้ใช้งาน...

ข้อ ๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่ จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจ ส่วนบุคคล

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

ข้อ ๕ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

ข้อ ๖ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่เทศบาลเมืองวังสะพุงมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

ข้อ ๗ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของเทศบาลเมือง วังสะพุงที่ได้รับมอบหมาย

ข้อ ๘ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์ หรือไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ หากกรณีที่มีการเปลี่ยนแปลงผู้ใช้งานให้แจ้งผู้มีอำนาจดูแลทรัพย์สินของเทศบาลเมืองวังสะพุงทราบ

ข้อ ๑๐ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่เทศบาลเมืองวังสะพุงจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของเทศบาลเมืองวังสะพุงเท่านั้น ห้ามมิให้ใช้งานนำทรัพย์สิน และระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่เทศบาลเมืองวังสะพุงไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อเทศบาลเมืองวังสะพุง

ข้อ ๑๑ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๐ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๑.๓ การบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของเทศบาลเมืองวังสะพุงหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๒ ข้อมูลที่อยู่ภายในระบบคอมพิวเตอร์ของเทศบาลเมืองวังสะพุงถือเป็นทรัพย์สินของเทศบาลเมืองวังสะพุง ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลายโดยไม่ได้รับอนุญาตจากนายกเทศมนตรีเมืองวังสะพุง

ข้อ ๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของเทศบาลเมืองวังสะพุงหรือข้อมูลของผู้รับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๔ นายกเทศมนตรีเมืองวังสะพุงสามารถตรวจสอบข้อมูลของผู้ใช้งานที่คาดว่าข้อมูลนั้นเกี่ยวข้องกับเทศบาลเมืองวังสะพุงได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๑.๔ การบริหาร...

๑.๔ การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๑ ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการ ดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือสุ่มรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๓) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๔) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงาม

ข้อ ๒ ผู้ใช้งานห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent) อีมูล (eMule) เป็นต้น

ข้อ ๓ ผู้ใช้งานห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูภาพยนตร์ การฟังเพลง การเล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ ซึ่งอาจจะส่งผลต่อ ประสิทธิภาพการรับ - ส่งข้อมูลในระบบเครือข่ายคอมพิวเตอร์ลดลง

ข้อ ๔ ผู้ใช้งานห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของเทศบาลเมืองวังสะพุงที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของเทศบาลเมืองวังสะพุง

ข้อ ๕ ผู้ใช้งานห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของเทศบาลเมืองวังสะพุงเพื่อการรบกวน ก่อให้เกิดความเสียหายหรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของเทศบาลเมืองวังสะพุง

ข้อ ๖ ผู้ใช้งานห้ามใช้ทรัพยากรทุกประเภทที่เป็นของเทศบาลเมืองวังสะพุงเพื่อประโยชน์ทางการค้า

ข้อ ๗ ผู้ใช้งานห้ามกระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในระบบเครือข่ายสารสนเทศของเทศบาลเมืองวังสะพุงโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๘ ผู้ใช้งานห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของเทศบาลเมืองวังสะพุงขัดข้องหรือหยุดชะงัก

ข้อ ๙ ผู้ใช้งานห้ามใช้ระบบสารสนเทศของเทศบาลเมืองวังสะพุง เพื่อการควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๑๐ ผู้ใช้งานห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสผ่านส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากร

ข้อ ๑๑ ผู้ใช้งานห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของเทศบาลเมืองวังสะพุง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๑.๕ การใช้งาน...

๑.๕ การใช้งานซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)

ข้อ ๑ เทศบาลเมืองวังสะพุงได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่เทศบาลเมืองวังสะพุงอนุญาตให้ใช้งาน หรือที่เทศบาลเมืองวังสะพุงมีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และเทศบาลเมืองวังสะพุงห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ เทศบาลเมืองวังสะพุงถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๒ ซอฟต์แวร์ (Software) ที่เทศบาลเมืองวังสะพุงได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑.๖ การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

ข้อ ๑ เครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) หรือเปิดการใช้งาน Anti-virus ที่ติดตั้งมากับระบบปฏิบัติการที่ถูกลิขสิทธิ์เป็นอย่างน้อย หรือตามที่เทศบาลเมืองวังสะพุงกำหนดให้ใช้

ข้อ ๒ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบโดยทันที

ข้อ ๕ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ เข้าสู่ระบบเครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบโดยทันที

ข้อ ๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของเทศบาลเมืองวังสะพุง หรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ (Malware) หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของเทศบาลเมืองวังสะพุง

๑.๗ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail)

ข้อปฏิบัติในข้อนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

หมวด ๒...

หมวด ๒
ความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย (Wireless Policy)

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

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

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมและดูแลระบบการยืนยันตัวตน (Authentication) เพื่อให้ผู้ใช้งานสามารถเข้าใช้งานระบบเครือข่ายสัญญาณอินเตอร์ของเทศบาลเมืองวังสะพุง ซึ่งเป็นไปตามระเบียบกฎหมายที่เกี่ยวข้องกำหนด ในกรณีระบบการยืนยันตัวตนมีเหตุขัดข้อง

ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (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) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบ ความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดทำรายงานผลการตรวจสอบทุกเดือน และในกรณีที่ตรวจสอบพบการใช้งาน ระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บังคับบัญชาเทศบาลเมืองวังสะพุงทราบทันที

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

หมวด ๓...

หมวด ๓
ความมั่นคงปลอดภัยของระบบไฟร์วอลล์ (Firewall Policy)

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

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องบันทึกชื่อผู้เข้าใช้งานและรหัสผ่าน (Username and Password) เพื่อเป็นการตรวจสอบผู้ใช้ก่อนใช้งานระบบและควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึงล่วงรู้หรือแก้ไขเปลี่ยนแปลงข้อมูลในระบบไฟร์วอลล์ (Firewall)

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตตามนโยบาย (Policy) ที่เทศบาลเมืองวังสะพุงกำหนด

ข้อ ๔ การเปลี่ยนแปลงการกำหนดค่า (Configuration) ทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๙ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๐ ผู้ดูแลระบบ (System Administrator) มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๑ การเชื่อมต่อในลักษณะของการเข้าถึงเครือข่ายระยะไกล (Remote Login) จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายและจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบ (System Administrator) ก่อน

ข้อ ๑๒ หากมีการละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ ผู้ใช้งานจะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ข้อ ๑๓ ผู้ดูแลระบบ (System Administrator) จะต้องออกจากระบบในช่วงเวลาที่ไม่ได้อยู่หน้าอุปกรณ์ไฟร์วอลล์ (Firewall) ทุกครั้ง

หมวด ๔...

หมวด ๔
ความมั่นคงปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

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

ข้อ ๒ ผู้ใช้งานได้รับรหัสผ่าน (Password) ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) เมื่อมีการ เข้าสู่ระบบในครั้งแรก ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่โดยทันที

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) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๗ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-mail)

หมวด ๕
ความมั่นคงปลอดภัยของระบบอินเตอร์เน็ต (Internet Security Policy)

ข้อ ๑ ผู้ใช้งานไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของเทศบาลเมืองวังสะพุงเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ผู้ใช้งานห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

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

ข้อ ๔ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) หรือแพลตฟอร์มสื่อสังคมออนไลน์ ผู้ใช้งานไม่ควรเปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๕ การใช้งาน...

ข้อ ๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) หรือแพลตฟอร์มสื่อสังคมออนไลน์ ต้องระมัดระวังในการเสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) ผู้ใช้งานควรออกจากระบบอินเตอร์เน็ตทุกครั้ง (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

หมวด ๖
ความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๖.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ เทศบาลเมืองวังสะพุง กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบ สารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ใน การเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของเทศบาลเมืองวังสะพุง และตรวจสอบการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

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

๖.๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของเทศบาลเมืองวังสะพุง ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก การพ้น จากตำแหน่ง หรือการย้ายหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ...

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและ รหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓) (๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

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

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงานต่างๆ

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(๕) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

หมวด ๗...

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

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในเทศบาลเมืองวังสะพุงให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของเทศบาลเมืองวังสะพุงและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่าย อินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการ ตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน (Demilitarized Zone : DMZ) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

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

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๐ พฤติกรรมการใช้งานกิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุกโจมตีระบบพฤติกรรมที่น่าสงสัยหรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พฤติกรรมกิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบจะต้องมีการรายงานให้ผู้ดูแลระบบทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนินการตามแผน

ข้อ ๑๔ เทศบาลเมืองวังสะพุงมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๕ ผู้ที่ถูกตรวจสอบ...

ข้อ ๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของเทศบาลเมืองวังสะพุง การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันทีหากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบสารสนเทศของเทศบาลเมืองวังสะพุงจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ประกาศ ณ วันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๖๘

นางนันทนา ตันติทวีโชค
นายกเทศมนตรีเมืองวังสะพุง