ประกาศเทศบาลเมืองปากพูน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๔๘ เตรส แห่งพระราชบัญญัติเทศบาล พ.ศ.๒๔๙๖ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๑๔) พ.ศ.๒๕๔๒ นายกเทศมนตรีเมืองปากพูน จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศเทศบาลเมืองปากพูน เรื่อง นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ วัตถุประสงค์

เพื่อให้ผู้ใช้งานระบบสารสนเทศของเทศบาลเมืองปากพูน ได้ทราบถึงข้อปฏิบัติในการใช้งานระบบสารสนเทศให้เกิดความมั่นคงปลอดภัยไม่ละเมิดระเบียบกฎหมายหรือทำให้เกิดความเสียหายเนื่องมาจากการใช้งานระบบสารสนเทศ

ข้อ ๓ ขอบเขต

ผู้ใช้งานระบบสารสนเทศของเทศบาลเมืองปากพูนทุกคน จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศเทศบาลเมืองปากพูน

ข้อ ๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๕ ในการประกาศนี้

๕.๑ ผู้ใช้งาน หมายถึง ผู้บริหาร พนักงานเทศบาล พนักงานจ้างเทศบาล ผู้ดูแลระบบ ของเทศบาลเมืองปากพูน รวมทั้ง ผู้รับบริการ ผู้ใช้งานทั่วไป ที่ได้รับสิทธิของผู้ใช้งานให้สามารถเข้าใช้งาน หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของเทศบาลเมืองปากพูน ทั้งนี้ให้รวมถึงผู้ให้บริการและผู้ได้รับการว่าจ้าง

๕.๒ ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมาย จากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการเข้าถึง จัดการ ดูแลรักษาระบบสารสนเทศและเครือข่าย คอมพิวเตอร์ ซึ่งสามารถเข้าถึงระบบเครือข่าย จัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๕.๓ ผู้บริหารระดับสูง หมายถึง นายกเทศมนตรีเมืองปากพูน ในฐานะผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

๕.๔ สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับการเข้าถึงและใช้งานระบบสารสนเทศของเทศบาลเมืองปากพูน

๕.๕ สินทรัพย์ หมายถึง สิ่งใดก็ตามที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศที่มีคุณค่าสำหรับเทศบาลเมืองปากพูน

/๕.๖ การเข้าถึง...

๕.๖ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนด สิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน การเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

๕.๗ ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพความพร้อม (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๕.๘ เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security) หมายถึงกรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืน นโยบายด้านความมั่นคงปลอดภัย หรือมาตรฐานป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่า อาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๕.๙ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของเทศบาบเมืองปากพูนถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๕.๑๐ การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับ ระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลเมืองปากพูน

๕.๑๑ ผู้ถือครองเครื่องคอมพิวเตอร์ หมายถึง ผู้ได้รับเครื่องคอมพิวเตอร์ไว้ใช้ประจำ ในการปฏิบัติงานและถือครอง รับผิดชอบ ดูแลเครื่อง/อุปกรณ์คอมพิวเตอร์

๕.๑๒ ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบ คอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๕.๑๓ ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ ระบบฐานข้อมูล โปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ ระบบจดหมายอิเล็กทรอนิกส์ และระบบคลาวด์ ของเทศบาลเมืองปากพูน

๕.๑๔ เจ้าของข้อมูล หมายถึง เจ้าหน้าที่ของเทศบาลเมืองปากพูน ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้รับผิดชอบดูแลปรับปรุงข้อมูลของระบบงานนั้น ๆ ซึ่งเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นสูญหาย

๕.๑๕ จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่ง ข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวไปยังคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP , POP๓ และ IMAP

/๕.๑๖ รหัสผ่าน...

๕.๑๖ รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระ หรือตัวเลขที่ใช้เป็น เครื่องมือในการตรวจสอบสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษา ความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

๕.๑๗ ชุดคำสั่งไม่พึงประเมิน หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๖ นโยบายด้านการควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ

๖.๑ การควบคุมข้อมูลภายในระบบสารสนเทส (Data Access Control)

๖.๑.๑ กำหนดให้ต้องระบุประเภทของข้อมูลในระบบเทคโนโลยีสารสนเทศ ได้แก่ ๑. ข้อมูลที่เป็นตัวเลข (Numeric Data) ๒. ข้อมูลประเภทตัวอักษร (Text Data) ๓. ข้อมูลที่อยู่ใน ลักษณะไฟล์เสียง (Audio Data) ๔. ข้อมูลรูปภาพ (Images Data) ๕. ข้อมูลที่เป็นภาพเคลื่อนไหว (Video Data) และข้อมูลอื่น ๆ เพื่อให้สามารถควบคุมการจัดการได้อย่างปลอดภัยและมีประสิทธิภาพ

๖.๑.๒ กำหนดให้ข้อมูลในระบบเทคโนโลยีสารสนเทศให้มีการแบ่งระดับความสำคัญของข้อมูลดังนี้ ระดับต่ำสุด ระดับสำคัญ และระดับสำคัญทั่วไป

๖.๑.๓ กำหนดให้ข้อมูลในระบบเทคโนโลยีสารสนเทศให้มีการแบ่งชั้นความลับ ของข้อมูลดังนี้ ข้อมูลลับที่สุด ข้อมูลลับ ข้อมูลทั่วไป โดยอาจกำหนดเพิ่มเติมเป็นข้อมูลสาธารณะ (Open Data) ได้

๖.๑.๔ กำหนดให้มีระดับชั้นของผู้มีสิทธิเข้าใช้งานเข้าถึงข้อมูลประกอบด้วย สิทธิระดับผู้ดูแลระบบ (System Administrator) และสิทธิระดับผู้ใช้งาน (User) เป็นอย่างน้อย ทั้งนี้สามารถกำหนดให้มีสิทธิระดับผู้ใช้งานระอับอื่น ๆ ตามความจำเป็น รวมถึงการเข้าถึงข้อมูลระดับกลุ่มผู้ใช้งาน (User Group) ได้

๖.๑.๕ กำหนดให้ผู้ใช้งานสามาระเข้าถึงข้อมูลภายในระบบสารสนเทศได้เฉพาะเวลาที่กำหนด โดยให้คำนึงถึงความจำเป็นของการใช้เทคโนโลยีสารสนเทศนั้น

๖.๑.๖ กำหนดให้มีช่องทางในการเข้าถึงระบบสารสนเทศได้เฉพาะช่องทางได้รับสิทธิของผู้ใช้งานหรือตกลงไว้ และมีการยืนยันตัวตนผ่านระบบยืนยันตัวตนด้วยวิธีการของระบบเทคโนโลยีสารสนเทศนั้น

๖.๒ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๖.๒.๑ ผู้ดูแลระบบและผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ต้องเป็นผู้ได้รับ อนุญาตเป็นผู้ได้รับมอบอำนาจ เป็นผู้มีภาระงานตามตำแหน่ง เป็นผู้รับบริการ หรืออย่างใดอย่างหนึ่ง เพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศของเทศบาลเมืองปากพูน ในการนี้รวมถึงผู้ให้บริการและผู้รับจ้าง

/๖.๒.๒ ผู้ดูแล....

๖.๒.๒ ผู้ดูแลระบบและผู้ใช้งานระบบเทคโนโลยีสารสนเทศทุกคนต้องมีบัญชีผู้ใช้งาน (User Account) ประกอบด้วยรสผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่ผ่านการลงทะเบียนและได้รับสิทธิของผู้ใช้งานที่พึงมีตามข้อ ๔.๒.๑ และ ๔.๒.๓

๖.๒.๓ การกำหนดสิทธิของผู้ใช้งานหรืออนุญาตเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของบัญชีผู้ใช้งานกำหนดให้มีบัญชีผู้ใช้งานในระบบเทคโนโลยีสารสนเทศ ที่มีระดับสิทธิ ในการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ อย่างน้อย ๒ ระดับ ได้แก่

- สิทธิสำหรับผู้ดูแลระบบ (System Administrator) โดย กำหนดให้มีสิทธิในการอ่าน สร้าง ป้อน แก้ไข อนุมัติ ระงับ และยกเลิกข้อมูล รวมถึงอนุญาต กำหนดสิทธิ แก้ไข ปรับเปลี่ยน และยกเลิกสิทธิของบัญชีผู้ใช้งานระดับผู้ใช้งาน (User) ในระบบเทคโนโลยีสารสนเทศ เป็นอย่างน้อย ทั้งนี้ไม่รวมการถอดรหัสข้อมูลใด ๆ ของบัญชีสิทธิระดับผู้ใช้งาน (User)

- สิทธิสำหรับบัญชีผู้ใช้งาน (User) โดยกำหนดให้มีสิทธิในการอ่าน สร้าง ป้อน และแก้ไขข้อมูล ตามสิทธิของผู้ใช้งานที่ได้รับมอบหมายของตนเองตามข้อ ๔.๒.๑ ที่มีต่อระบบ เทคโนโลยีสารสนเทศเท่านั้น

๖.๒.๔ กำหนดให้ผู้ดูแลระบบทำหน้าที่ในการอนุมัติบัญชีผู้ใช้งานระดับต่าง ๆ พร้อมกำหนดสิทธิของผู้ใช้งานให้เป็นไปตามที่ได้รับอนุญาต การได้รับการมอบอำนาจ การเป็นผู้มีภาระงาน ตามตำแหน่ง หรืออย่างใดอย่างหนึ่ง รวมถึงทำหน้าที่ในการปรับปรุง ระงับ ยกเลิกบัญชีดังกล่าวตามภารกิจ

๖.๓ การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (User Access Management)

๖.๓.๑ จัดให้มีการสร้างความรู้ความเข้าใจให้กับผู้งานเพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระวังหรือรู้เท่าไม่ถึงการ ผ่านช่องทางประชาสัมพันธ์ของเทศบาลเมืองปากพูน ประกาศ หรือการอบรม

๖.๓.๒ จัดให้มีระบบความปลอดภัยพื้นฐาน ได้แก่

-ระบบป้องกันการบุกรุกเครือข่าย (Firewall) ในรูปแบบอุปกรณ์หรือ ระบบที่ติดตั้งบนคลาวด์

-ระบบป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) ในรูปแบบอุปกรณ์หรือระบบที่ติดตั้งบนคลาวด์

- ระบบยืนยันตัวตน (Authentication System) ในลักษณะต่าง ๆ ตามความเหมาะสมของระบบเทคโนโลยีสารสนเทศนั้น

๖.๓.๓ การเข้าถึงระบบเทคโนโลยีสารสนเทศ กำหนดให้ผู้มีสิทธิใช้งานทำการยืนยันตัวตน (User Authentication) ก่อนเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ด้วยบัญชีผู้ใช้งาน (User Account) ซึ่งประกอบด้วยรหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) หรือ วิธีการใด ๆ ของระบบเทคโนโลยีสารสนเทศ นั้น

๖.๓.๔ ระบบเทคโนโลยีสารสนเทศมีความสำคัญ เช่น ระบบที่มีการจัดเก็บหรือ ส่งข้อมูลสำคัญ ระบบที่มีกระบวนการยืนยันลงนาม หรือระบบที่มีธุรกรรมทางการเงินและบัญชี ให้นำ การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication) เข้ามาใช้งานเพิ่มเติมจากรหัสผู้ใช้ (Username)

/และรหัส....

และรหัสผ่าน (Password) โดยอาจให้ทำการยืนยันตัวตนผ่านโทรศัพท์ E-mail หรือ อื่น ๆ

๖.๓.๕ การลงทะเบียนผู้ใช้งาน (User Registration) เพื่อสร้างบัญชีผู้ใช้งาน (User Account) ของระบบเทคโนโลยีสารสนเทศ ต้องมีขั้นเป็นอย่างน้อย ดังนี้

-ระบุข้อมูลของบุคคล เพื่อระบุหรือยืนยันตัวตน และช่องทางติดต่อกลับ

-ระบุบริการที่ต้องการรับ เพื่อเข้าถึงข้อมูลและระดับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศนั้น

-ระบุอุปกรณ์ที่งานร่วมกับระบบบัญชี (ถ้ามี) เช่น เครื่องคอมพิวเตอร์ USB-Token เครื่องอ่านบัตรต่าง ๆ

-ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีจำนวนอักขระไม่น้อยกว่า ๘ ตัวโดยประกอบด้วยตัวอักษรภาษาอังกฤษพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ (!@#$%^&*=+) และปิดการใช้งานคำใบ้ของรหัสผ่าน และทำการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ ให้แก่บัญชีผู้ใช้งานของตนเอง เพื่อเพิ่มความซับซ้อนและเพิ่มเวลาในการถอดรหัสของผู้ไม่หวังดี

-มีการยืนยันการยอมรับ กฎ ข้อบังคับ หรือข้อตกลงตามที่กำหนดเพื่อเข้าถึงระบบสารสนเทศนั้น ก่อนการยืนยันเพื่อลงทะเบียน

๖.๓.๖ การบริหารจัดการสิทธิของผู้ใช้งานให้เป็นไปตามข้อ ๖.๑ และ ๖.๒

๖.๓.๗ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Managements) ต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

-กำหนดให้การลงทะเบียนผู้ใช้งาน เป็นไปตามข้อ ๖.๓.๕ และได้รับสิทธิผู้ใช้งานตามข้อ ๖.๒.๓

-กำหนดให้เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ หรือเมื่อพบเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ โดยกำหนดรหัสผ่านต้องมีจำนวนอักขระไม่น้อยกว่า ๔ ตัว ประกอบด้วยตัวอักษรภาษาอังกฤษพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ !@#$%^&*=+ และปิดการใช้คำใบ้ของรหัสผ่าน และทำการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ ให้แก่ผู้ใช้งานของตนเอง เพื่อเพิ่มความซับซ้อนและเพิ่มเวลาในการถอดรหัสของผู้ไม่หวังดี

-กำหนดให้จัดเก็บรหัสผ่านด้วยวิธีการเข้ารหัสและจัดเก็บไว้ในที่ปลอดภัยยากต่อการเข้าถึงจากภัยคุกคาม

-กรณีลืมรหัสผู้ใช้งาน (Username) หรือรหัสผ่าน (Password) ให้ทำการติดต่อผู้ดูแลระบบ (System Administrator) หรือขอแก้ไขข้อมูล พร้อมระบุข้อมูลที่ทำการระบุไว้ในข้อ ๔.๓.๕ เพื่อยืนยันตัวตน

๖.๓.๘ กำหนดให้มีการทบทวนสิทธิการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศตามระยะเวลาที่กำหนด

/๖.๔ การกำหนด....

๖.๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๖.๔.๑ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ ให้จัดเก็บอุปกรณ์และสินทรัพย์ รวมถึงเอกสาร ในที่ปลอดภัยเข้าถึงได้เฉพาะบุคคลหรือระบบที่เกี่ยวข้อง หรือเสี่ยงต่อความเสียหาย และให้ทำการออกจากการใช้งาน (Logout) ในระบบเทคโนโลยีสารสนเทศ

๖.๔.๒ กำหนดให้แยกสื่อบันทึกส่วนบุคคล ได้แก่ เอกสาร USB Flash-drive External-Hard disk ออกจากสื่อบันทึกที่ใช้งานกับระบบเทคโนโลยีสารสนเทศของเทศบาลเมืองปากพูน เพื่อป้องกันการเข้าถึงหรือลักลอบทำสำเนา รวมถึงเพื่อป้องกันการติดไวรัสคอมพิวเตอร์

๖.๔.๓ กำหนดให้ผู้มีสิทธิใช้งานระบบสารสนเทศผ่านระบบเครือข่าย ที่มีการป้องกันด้วยอุปกรณ์ป้องกันเครือข่ายที่เกี่ยวข้อง ภายในเทศบาลเมืองปากพูน

๖.๔.๔ กำหนดให้งดใช้งาน (User Account) และรหัสผ่าน (Password) ร่วมกัน ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของเทศบาลเมืองปากพูน

๖.๔.๕ เมื่อพบการเข้าถึงข้อมูลหรือระบบสารสนเทศด้วยชุดคำสั่งไม่พึงประสงค์ หรือด้วยวิธีการใดโดยไม่ได้รับอนุญาต เพื่อการเปิดเผย การล่วงรู้ การลักลอบทำสำเนา การลักขโมย ลักลอบดัดแปลง หรือแก้ไข ข้อมูลหรือระบบเทคโนโลยีสารสนเทศ กรณีพบผู้ใช้งานใดเป็นผู้กระทำหรือมีส่วนร่วม ให้บุคคลดังกล่าวเป็นผู้รับผิดชอบ และให้ดำเนินการตามประพระราชบัญญัติ ว่าด้วยการกระทำหรือมีส่วนร่วม ให้บุคคลดังกล่าวเป็นผู้รับผิดชอบ และให้ดำเนินการตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่๒) พ.ศ.๒๕๖๐ ทั้งนี้ให้รวมถึงการกระทำให้ระบบหยุดชะงัก ไม่สามารถใช้งานได้ตามปกติ

๖.๕ การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๖.๕.๑ กำหนดให้มีการตั้งค่าอุปกรณ์เครือข่าย (Firewall) หรืออุปกรณ์ที่เกี่ยวข้อง เพื่ออนุญาตให้ผู้ใช้งานระบบเทคโนโลยีสารสนเทศจากเครือข่ายภายใน ใช้งานระบบสารสนเทศ บริการเว็บไซต์ เครือแม่ข่าย ที่อยู่ภายนอกระบบเครือข่าย และอนุญาตให้ระบบภายนอกเข้าถึงเครือข่ายหรือ ระบบเทคโนโลยีสารสนเทศได้เท่าที่จำเป็นและมีความปลอดภัย เป็นไปตามภารกิจที่จำเป็น

๖.๕.๒ กำหนดให้มีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connection) ด้วยวิธีการที่เหมาะสม เช่น การออกบัญชีผู้ใช้งาน ชั่วคราว หรือ การออกรหัสผ่านชั่วคราว เพื่อทำการยืนยันตัวตน หรือการเข้าถึงระบบเครือข่ายด้วยระบบ VPN

๖.๕.๓ กำหนดให้ระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network) ดังนี้

-ตั้งชื่อเครื่องคอมพิวเตอร์โดยระบุชื่อเป็น สำนัก/กอง หมายเลขลำดับเครื่องที่ใช้งาน เป็นอย่างน้อย

- ตั้งชื่อเครื่องพิมพ์ที่เชื่อมต่อระบบเครือข่ายโดยระบุชื่อเป็นสำนัก/กอง ชนิดอุปกรณ์ ยี่ห้อหรือรุ่น และหมายเลขลำดับเครื่องใช้งาน และตั้งค่าเครื่องหมายเลขไอพีแอดเดรส แบบคงที่ (Static IP Address) เป็นอย่างน้อย

/-ตั้งชื่ออุปกรณ์...

-ตั้งชื่ออุปกรณ์เครือข่าย โดยระบุชื่อที่มีเนื้อหาประกอบด้วย ชนิด อุปกรณ์ที่ตั้ง ตั้งค่าหมายเลขไอพีแอดเดรสแบบคงที่ (Static IP Address) เป็นอย่างน้อย พร้อมตั้งค่ารหัสผ่าน เพื่อป้องกันการเข้าถึงสำหรับการบริหารจัดการ และกำหนดหมายเลขพอร์ต (Service Port Number) สำหรับการเข้าถึงทางไกล

-ตั้งชื่ออุปกรณ์แม่ข่ายหรืออุปกรณ์จัดเก็บข้อมูล โดยระบุชื่อที่มีเนื้อหาประกอบด้วยชนิดอุปกรณ์ ที่ตั้ง เป็นอย่างน้อย และตั้งค่าหมายเลขไอพีแอดเดรสแบบคงที่ (Static IP Address) ให้อปุกรณ์พร้อมตั้งค่ารหัสผ่านเพื่อป้องกันการเข้าถึงสำหรับการบริหารจัดการ และกำหนดหมายเลขพอร์ต (Service Port Number) สำหรับการเข้าถึงทางไกล (Remote Access)

๖.๕.๔ กำหนดให้มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration) โดยใช้หมายเลขที่ใช้ระบุบริการ (Service Port Number) เฉพาะที่มีบริการอยู่ในระบบเครือข่ายเท่านั้น รวมถึงการตั้งค่ารหัสผ่านสำหรับพอร์ตทางกายภาพ (Physical Port)

๖.๕.๕ กำหนดการแบ่งแยกเครือข่าย (Segregation in Network) โดยการทำการแบ่งเป็นกลุ่มต่าง ๆ ด้วยหมายเลข VLAN ID และ Network ID ที่แตกต่างกัน ดังนี้

-กลุ่มของฐานข้อมูลและเครื่องแม่ข่ายบริการสารสนเทศ

-กลุ่มของระบบคอมพิวเตอร์ และเครื่องพิมพ์ โดยจำแนกเป็น บริเวณที่ตั้งอาคารสำนักงาน ชั้น หรือสำนัก/กอง

-กลุ่มของอุปกรณ์ป้องกันความปลอดภัย และอุปกรณ์เครือข่าย

-กลุ่มของอุปกรณ์และระบบที่ใช้งานใน Demilitarized Zone หรือกลุ่มที่สามารถเข้าถึงได้จากระบบเครือข่ายภายในและเครือข่ายภายนอก

-กลุ่มของอุปกรณ์ภายนอกเครือข่าย

๖.๕.๖ กำหนดให้มีระบบจัดเก็บ Log File ระบบเครือข่าย ในลักษณะอุปกรณ์หรือระบบที่ติดตั้งบนคลาวด์ เพื่อบันทึกกิจกรรมของอุปกรณ์เครือข่ายหรือข้อมูลจราจร อย่างน้อย ๙๐ วัน เป็นไปตามมาตรา ๒๖ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐

๖.๖ กำหนดให้มีการตั้งค่าการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ด้วยการทำ Network Access list เพื่อควบคุมการเชื่อมต่อระหว่าง VLAN ID หรือ Network ID ที่มีในระบบเครือข่าย เพื่อควบคุมและจำกัดการเชื่อมต่อทางเครือข่ายระหว่างเครือข่ายภายใน ด้วยกัน และการเชื่อมต่อระหว่างเครือข่ายภายนอกและเครือข่ายภายใน

๖.๗ กำหนดให้ควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) โดยควบคุมเส้นทาง (Routing) ระหว่างเครือข่ายอย่างเป็นระบบ หลีกเสี่ยงการทำ Backdoor Routes โดยไม่จำเป็น

๖.๘ กำหนดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยจัดให้มีการ Login เข้าสู่ระบบปฏิบัติการด้วยรหัสผ่านของผู้ใช้นั้น ๆ ปิดการใช้งาน “hint”หรือคำใบ้ของรหัสผ่าน เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ ติดตั้งซอฟต์แวร์ทุกครั้งต้องใช้สิทธิ์ผู้ดูแลเสมอ และ

/กำหนด...

กำหนดให้ยุติการใช้งานเมื่อมีการว่างเว้นจากการใช้งาน (Session Out)

๖.๙ กำหนดให้มีการควบคุมการเข้าถึงระบบสารสนเทศ(Information Access Restriction) ให้เป็นไปตามข้อ ๖.๒.๑ ถึง ๖.๒.๓ และข้อ ๖.๓.๓ และเข้าถึงโปรแกรมประยุกต์หรือ แอพพลิเคชั่นผ่าน IP Address พอร์ต และ URL ที่กำหนดเท่านั้น

ข้อ ๗ นโยบายด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

๗.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจัดทำระบบสำรอง ไม่ว่าระบบดังกล่าว จะอยู่ภายในระบบเครือข่ายของเทศบาลเมืองปากพูน หรือดูแลและติดตั้งภายนอกเครือข่ายโดยผู้ให้บริการ

๗.๒ กำหนดให้มีการสำรองข้อมูลที่สำคัญตามกฎ ๓-๒-๑ โดยเก็บข้อมูลสำคัญเอาไว้ ชุด ได้แก่ ข้อมูลหลัก ๑ ชุด และข้อมูลสำรอง ๒ ชุด เก็บไฟล์เหล่านั้นเอาไว้บนอุปกรณ์ที่แยกขาดจากกัน ๒ ประเภท และข้อมูลสำรอง ๑ ชุดเก็บไว้แบบ Offline และมีการดำเนินการสำรองข้อมูลเสมอ

๗.๓ มีการปรับปรุงแพตช์ (Update Patch) ของระบบปฏิบัติการและซอฟต์แวร์ รวมถึงติดตั้งโปรแกรมป้องกันมัลแวร์ให้กับคอมพิวเตอร์ อุปกรณ์ป้องกันความปลอดภัย และปรับปรุงโปรแกรมให้ทันอยู่เสมอ

๗.๔ เปิดใช้งานระบบความปลอดภัยของระบบปฏิบัติการ หรือจัดหาซอฟต์แวร์ เพื่อตรวจจับความเสี่ยงที่อาจเกิดขึ้นต่ออุปกรณ์คอมพิวเตอร์

๗.๕ กำหนดให้อุปกรณ์และระบบเทคโนโลยีสารสนเทศติดตั้งอยู่ในนถานที่ที่เหมาะสม ปลอดภัย มีระบบไฟฟ้าสำรอง และอุณหภูมิที่เหมาะสมเข้าถึงได้เฉพาะผู้ที่เกี่ยวข้อง

ข้อ ๘ ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

๘.๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในเทศบาลเมืองปากพูน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๘.๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของเทศบาลเมืองปากพูนและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๘.๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๘.๔ ระบบทั้งหมดใน (Demilitarized Zone : DMZ) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๘.๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๘.๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

/๘.๗ มีการตรวจสอบ...

๘.๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๘.๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๘.๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๘.๑๐ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุกโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้ดูแลระบบทราบทันทีที่ตรวจพบ

๘.๑๑ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้ดูแลระบบทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๘.๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๘.๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนินการตามแผน

๘.๑๔ เทศบาลเมืองปากพูน มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๘.๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของเทศบาลเมืองปากพูน การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบสารสนเทศของเทศบาลเมืองปากพูน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ข้อ ๙ นโยบายด้านการตรวจสอบและประเมินความเสี่ยง

กำหนดให้มีการตรวจสอบและควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหรือหน่วยงานหรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

ข้อ ๑๐ กำหนดให้มีการให้ความรู้ผ่านช่องทางอิเล็กทรอนิกส์ของเทศบาลเมืองปากพูน เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในองค์กรอย่างสม่ำเสมอ

ข้อ ๑๑ ให้นายกเทศมนตรีเมืองปากพูนเป็นผู้รักษาการตามประกาศ

/ข้อ ๑๒ การติดต่อ....

ข้อ ๑๒ การติดต่อสอบถามนโยบายและแนวปฏิบัติในการรักษาความปลอดภัย ด้านสารสนเทศ สามารถติดต่อได้ ดังนี้

สำนักงานเทศบาลเมืองปากพูน (งานประชาสัมพันธ์)

เลขที่ ๑๗๔ หมู่ ๔ ต.ปากพูน

อ.เมืองนครศรีธรรมราช

จ.นครศรีธรรมราช

เว็บไซต์ www.pakpooncity.go.th

อีเมล์ saraban@pakpooncity.go.th

โทรศัพท์/โทรสาร : ๐-๗๕๗๗-๔๑๓๐-๓๓

Smart city : https://lin.ee/NxxoRRF

จึงประกาศให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๑๓ พฤศจิกายน พ.ศ.๒๕๖๘

(นายธนาวุฒิ ถาวรพราหมณ์)
นายกเทศมนตรีเมืองปากพูน