ประกาศเทศบาลนครนครศรีธรรมราช
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
เทศบาลนครนครศรีธรรมราช ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครนครศรีธรรมราช มีความมั่นคงปลอดภัย(Security) เชื่อถือได้ (Reliability) มีความพร้อมใช้งาน (Availability) รองรับการให้บริการประชาชนและงานบริหารราชการได้อย่างต่อเนื่อง รวมถึงเพื่อป้องกันภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลราชการและข้อมูลส่วนบุคคล

อาศัยอำนาจตามความในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เทศบาลนครนครศรีธรรมราช จึงประกาศกำหนดนโยบายและแนวปฏิบัติ ดังนี้

หมวด ๑ บททั่วไป

ข้อ ๑ ชื่อประกาศ ประกาศนี้เรียก “ประกาศเทศบาลนครนครศรีธรรมราช เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ “

ข้อ ๒ ขอบเขตการบังคับใช้ นโยบายนี้มีผลบังคับใช้กับ

๒.๑ ข้าราชการ พนักงาน ลูกจ้าง และบุคลากรทุกคนของเทศบาล

๒.๒ บุคคลภายนอก (Outsource/Vender) นักศึกษาฝึกงาน หรือผู้รับจ้างที่ได้รับอนุญาตให้เข้าถึงระบบเครือข่ายและข้อมูลของเทศบาล

๒.๓ อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารทุกชนิด ทั้งที่เป็นทรัพย์สินของเทศบาลและทรัพย์สินส่วนตัว (BYOD) ที่นำมาเชื่อมต่อกับระบบเครือข่ายของเทศบาล

ข้อ ๓ คำนิยาม

- ผู้ใช้งาน (User) หมายถึง บุคคลที่ได้รับสิทธิ์ให้เข้าถึงระบบสารสนเทศตามภาระหน้าที่
- ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่มีสิทธิ์บริหารจัดการ ปรับปรุงแก้ไขโครงสร้างระบบ หรือเข้าถึงข้อมูลได้ในระดับสูงกว่าผู้ใช้งานทั่วไป
- ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ตามกฎหมาย PDPA
- ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำที่มีเจตนาร้ายเพื่อทำลาย แก้ไข ขโมยข้อมูล หรือทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้

หมวด ๒ การควบคุมการเข้าถึงและการพิสูจน์ตัวตน (Access Control)

ข้อ ๔ การบริหารจัดการบัญชีผู้ใช้งาน (User Account)

๔.๑ ผู้ใช้งานต้องมีบัญชีผู้ใช้งาน (Username) เป็นของตนเอง ห้าม ใช้บัญชีร่วมกัน (Shared Account) โดยเด็ดขาดเพื่อให้ไม่สามารถตรวจสอบยืนยันตัวตนผู้กระทำผิดได้ (Accountability)

๔.๒ สิทธิ์การเข้าถึงข้อมูล (Access Rights) จะถูกกำหนดตามหลักการ "จำเป็นต้องรู้ (Need-to-Know Basis)" คือใช้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น

๔.๓ กรณีผู้ใช้งานพ้นสภาพการเป็น พนักงาน ลาออก หรือย้ายหน่วยงาน หัวหน้าหน่วยงานต้องแจ้งผู้ดูแลระบบเพื่อระงับสิทธิ์การใช้งาน (Disable Account) ภายใน ๒๔ ชั่วโมง

ข้อ ๕ มาตรการด้านรหัสผ่าน (Password Policy) เพื่อให้เกิดความรัดกุม ปลอดภัยจากการคาดเดา ให้ถือปฏิบัติดังนี้

๕.๑ ความยาว รหัสผ่านต้องมีความยาวไม่น้อยกว่า ๑๐ ตัวอักษร (แนะนำ ๑๒ ตัวอักษรขึ้นไป)

๕.๒ ความซับซ้อน ต้องประกอบด้วยอักขระอย่างน้อย ๓ ใน ๔ ประเภท ได้แก่ ตัวอักษรพิมพ์ใหญ่ (A-Z) ตัวอักษรพิมพ์เล็ก (a-z) ตัวเลข (0-9) อักขระพิเศษ (@#$%)

๕.๓ อายุรหัสผ่าน กำหนดให้เปลี่ยนรหัสผ่านใหม่ทุก ๆ ๙๐ - ๑๘๐ วัน

๕.๔ ข้อห้าม

- ห้ามใช้รหัสผ่านซ้ำกับรหัสเดิมที่เคยใช้ล่าสุด ๓ ครั้งหลัง
- ห้ามจดบันทึกรหัสผ่านไว้ในที่เปิดเผย เช่น แปะไว้ใต้คีย์บอร์ด หรือหน้าจอคอมพิวเตอร์
- ห้ามใช้รหัสผ่านเดียวกันกับบัญชีส่วนตัว เช่น Facebook, Line

ข้อ ๖ การล็อคหน้าจอ (Screen Lock)

๖.๑ เครื่องคอมพิวเตอร์ต้องตั้งค่าให้ล็อคหน้าจออัตโนมัติ เมื่อไม่มีการใช้งานเกินกว่า ๕ - ๑๐ นาที

๖.๒ ผู้ใช้งานต้องการล็อคหน้าจอ (Lock Screen) หรือออกจากระบบ (Log off) ทุกครั้งลุกจากที่นั่ง แม้จะเป็นระยะสั้น

หมวด ๓ ความมั่นคงปลอดภัยของอุปกรณ์และเครือข่าย (Device & Network Security)

ข้อ ๗ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์พกพา

๗.๑ เครื่องคอมพิวเตอร์ของเทศบาลทุกเครื่อง ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus/Endpoint Protection) และต้องอัปเดตฐานข้อมูลไวรัสให้เป็นปัจจุบันเสมอ

๗.๒ ห้ามผู้ใช้งานปิดการทำงานของโปรแกรมป้องกันไวรัส หรือ Firewall โดยไม่ได้รับอนุญาต

๗.๓ ห้าม ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ ซอฟต์แวร์เถื่อน (Cracked Software) หรือโปรแกรมสำหรับเจาะระบบ ลงในเครื่องคอมพิวเตอร์ของเทศบาลโดยเด็ดขาด

๗.๔ กรณีนำอุปกรณ์ส่วนตัว (Mobile/Tablet/Notebook) มาใช้ปฏิบัติงาน ต้องมั่นใจว่าอุปกรณ์นั้นไม่มีมัลแวร์ และต้องปฏิบัติตามนโยบายความปลอดภัยเช่นเดียวกันกับอุปกรณ์ของเทศบาล

ข้อ ๘ การใช้งานสื่อบันทึกข้อมูล (Removable Media)

๘.๑ การใช้งาน Flash Drive, External Hard disk หรือสื่อบันทึกข้อมูลอื่น ๆ ต้องทำการสแกนไวรัสก่อนเปิดใช้งานทุกครั้ง

๘.๒ ห้าม นำสื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา (เช่น เก็บได้ตามทางเดิน) มาเสียบเข้ากับเครื่องคอมพิวเตอร์ของเทศบาลเด็ดขาด

หมวด ๔ การใช้งานอินเตอร์เน็ต อีเมล และสื่อสังคมออนไลน์ (Internet & Social Media)

ข้อ ๙ การใช้งานอินเตอร์เน็ตและอีเมล

๙.๑ ห้ามใช้อินเตอร์เน็ตเพื่อเข้าถึงเว็บไซต์สื่อลามกอนาจาร การพนัน เว็บไซต์ละเมิดลิขสิทธิ์ หรือเว็บไซต์ที่มีความเสี่ยงต่อความมั่นคง

๙.๒ การป้องกัน Phishing ห้ามคลิกลิงค์ หรือ ดาวน์โหลดไฟล์แนบจากอีเมลที่ไม่รู้จักผู้ส่ง หรืออีเมลที่มีลักษณะน่าสงสัย (เช่นการเขียนภาษาผิดปกติ การเร่งรัดให้โอนเงิน)

๙.๓ การรับส่งไฟล์ข้อมูลราชการผ่านอีเมลสาธารณะ (เช่า Gmail, Hotmail) ต้องทำด้วยความระมัดระวัง หากเป็นข้อมูลลับ ต้องทำการเข้ารหัสไฟล์ (Encrypt) หรือใส่รหัสผ่านก่อนส่ง

ข้อ ๑๐ การใช้งานสื่อสังคมออนไลน์ (Social Media)

๑๐.๑ ห้ามโพสต์หน้าจอขณะทำงาน ที่ปรากฏข้อมูลส่วนบุคคลของประชาชน หรือข้อมูลภายในราชการ ลงใน Social Media ทุกช่องทาง

๑๐.๒ ห้ามมีการแสดงความคิดเห็นในนามของเทศบาลนครนครศรีธรรมราช โดยไม่ได้รับมอบหมาย ซึ่งอาจก่อให้เกิดความเข้าใจผิดหรือความเสียหายต่อองค์กร

หมวด ๕ การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy & PDPA)

ข้อ ๑๑ การรวบรวมและใช้ข้อมูลส่วนบุคคล

๑๑.๑ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชน (เช่น ชื่อ - สกุล เลขบัตรประชาชน เบอร์โทรศัพท์) ต้องทำภายใต้อำนาจหน้าที่ตามกฎหมาย หรือได้รับความนิยมจากเจ้าของข้อมูลเท่านั้น

๑๑.๒ ห้าม นำข้อมูลส่วนบุคคลของประชาชนไปใช้เพื่อประโยชน์ส่วนตัว ประโยชน์ทางการค้า หรือส่งต้อให้บุคคลภายนอกโดยไม่ได้รับอนุญาต

ข้อ ๑๒ การรักษาความมั่นคงปลอดภัยของข้อมูล

๑๒.๑ เอกสารกระดาษที่มีข้อมูลส่วนบุคคล (Hard Copy) เมื่อเลิกใช้งานแล้ว ต้องทำลายด้วยเครื่องย่อยเอกสาร ห้ามทิ้งลงถังขยะทั่วไป

๑๒.๒ ไฟล์ข้อมูลส่วนบุคคลที่ส่งผ่านแอปพลิเคชัน (เช่น LINE) ควรมีการจำกัดเข้าถึงหรือลบออกจากห้องแชททันทีเมื่อเสร็จภารกิจ

หมวด ๖ นโยบายระบบสารสนเทศ ระบบสำรองข้อมูล และแผนเตรียมความพร้อมฉุกเฉิน

(Information System Backup & BCP)

ข้อ ๑๓ การคัดเลือกระบบสารสนเทศที่สำคัญและการจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศสามารถใช้งานได้อย่างต่อเนื่องและปลอดภัย ให้มีแนวปฏิบัติดังนี้

๑๓.๑ การคัดเลือกระบบ ให้หน่วยงานจัดทำ "บัญชีระบบสารสนเทศที่สำคัญทั้งหมดของหน่วยงาน" พร้อมทั้งประเมินและกำหนดระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองข้อมูล โดยให้มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง

๑๓.๒ องค์ประกอบของข้อมูลที่ต้องสำรอง ชนิดของข้อมูลที่ต้องสำรอง อย่างน้อยต้องประกอบด้วย

- ค่าการตั้งค่า (Configuration) สำหรับระบบ ข้อมูลคู่การปฏิบัติงานสำหรับระบบ
- ฐานข้อมูล (Database) ของระบบสารสนเทศ
- ซอฟต์แวร์ที่เกี่ยวข้อง ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ (OS)
- ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่นใดที่จำเป็นต่อการกู้คืนระบบ

๑๓.๓ แนวทางการสำรองข้อมูล กำหนดขั้นตอน ความถี่ และรูปแบบการสำรองข้อมูลให้เหมาะสมกับชนิดข้อมูล เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือแบบส่วนต่าง (Increment Backup) ต้องมีการบันทึกข้อมูลประวัติการสำรองข้อมูล โดยระบุชื่อผู้ดำเนินการ วันที่ เวลา ชื่อข้อมูลที่สำรอง และสถานะการสำรองข้อมูลอย่างชัดเจน สื่อที่ใช้บันทึกข้อมูลสำรอง (Backup Media) ต้องมีการทำป้ายกำกับ (Label) และควรจัดเก็บแยกจากระบบเครือข่ายหลัก (Offline/Off-site Backup) เพื่อป้องกันความเสียหายจากภัยคุกคาม เช่น ไวรัสเรียกค่าไถ่ (Ransomware) ต้องจัดให้มีการเข้ารหัสข้อมูล (Encryption) สำรหับข้อมูลหรือข้อมูลส่วนบุคคลที่ได้เก็บสำรองไว้

ข้อ ๑๔ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Business Continuity Plan - BCP) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อรองรับสถานการณ์ฉุกเฉินที่ระบบสารสนเทศไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้โดยมีรายละเอียดดังนี้

๑๔.๑ กำหนดโครงสร้าง หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมดอย่างชัดเจน

๑๔.๒ ต้องประเมินสถานการณ์ความเสี่ยง (Risk Assessment) สำหรับสถานการณ์ฉุกเฉินรูปแบบต่าง ๆ ที่อาจเกิดขึ้นกับระบบสารสนเทศ

๑๔.๓ กำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบสารสนเทศ (Disaster Recovery Procedure)

๑๔.๔ กำหนดช่องทางในการติดต่อสื่อสาร รวมถึงรายชื่อผู้ให้บริการภายนอก (Vender/Outsource) ที่จะต้องติดต่อประสานงานเมื่อเกิดเหตุจำเป็นเร่งด่วน

๑๔.๕ จัดให้มีการฝึกอบรมสร้างความตระหนักรู้แก่เจ้าหน้าที่ ถึงขั้นตอนการปฏิบัติและสิ่งที่ต้องดำเนินการเมื่อเกิดเหตุฉุกเฉิน

๑๔.๖ การทดสอบแผน ต้องจัดให้มีการทดสอบความพร้อมใช้งานของระบบสำรองข้อมูล และทดสอบแผนเตรียมความพร้อมกรณีฉุกเฉิน (Restore & BCP Test) อย่างน้อยปีละ ๑ ครั้ง

หมวด ๗ การตรวจสอบและบทลงโทษ

ข้อ ๑๕ การตรวจสอบ (Monitoring & Audit) เทศบาลนครนครศรีธรรมราช ขอสงวนสิทธิ์ในการตรวจสอบจราจรทางคอมพิวเตอร์ (Log File) การเข้าถึงข้อมูล และอุปกรณ์สารสนเทศของหน่วยงาน เพื่อวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัย โดยไม่ถือว่าเป็นการละเมิดสิทธิส่วนบุคคลของผู้ใช้งาน

ข้อ ๑๖ การแจ้งเหตุละเมิด หากผู้ใช้งานพบเห็นความผิดปกติ เช่น เครื่องทำงานช้าผิดปกติ ไฟล์ข้อมูลเปิดไม่ได้หรือสงสัยรหัสผ่านรั่วไหล ให้แจ้งผู้ดูแลระบบหรือศูนย์เทคโนโลยีสารสนเทศ ทันที

ข้อ ๑๗ บทลงโทษ ผู้ใดฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้ จนเป็นเหตุให้เกิดความเสียหายแก่ทางราชการ หรือทำให้ข้อมูลรั่วไหล

๑๗.๑ จะต้องถูกดำเนินการทางวินัยตามระเบียบของเทศบาล

๑๗.๒ อาจต้องรับผิดทางแพ่ง (ชดใช้ค่าเสียหาย)

๑๗.๓ หากการกระทำเข้าข่ายความผิดทางอาญา จะต้องถูกดำเนินคดีตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ประกาศ ณ วันที่ ๒๐ กุมภาพันธ์ พ.ศ.๒๕๖๙

(นายกณพ เกตุชาติ)
นายกเทศมนตรีนครนครศรีธรรมราช