ประกาศเทศบาลนครขอนแก่น
เรื่อง นโยบายรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)

ด้วย เทศบาลนครขอนแก่น ได้จัดให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้บริการแก่ประชาชนทั่วไป หน่วยงานภาครัฐ ภาคเอกชน และบุคลากรในสังกัดเทศบาลนครขอนแก่น อำนวยความสะดวก เพิ่มประสิทธิภาพ และให้ประสิทธิผลต่อการทำงานทั้งระบบ ทั้งนี้ เพื่อให้การใช้บริการและการให้บริการสามารถดำเนินการใช้งานร่วมกันได้อย่างเหมาะสม สอดคล้องกับนโยบายความมั่นคงปลอดภัยและป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องทั้งจากผู้ใช้งาน และภัยคุกคามต่างๆ ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของเทศบาลนครขอนแก่นให้ได้รับความเสียหายได้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของเทศบาลนครขอนแก่นคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ จึงเห็นสมควรกำหนดนโยบายรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกัน ดังต่อไปนี้

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคง ปลอดภัยทางเทคโนโลยีสารสนเทศ

๑.๒ เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม

๑.๓ เพื่อให้พนักงาน และผู้ที่ต้องใช้ หรือเชื่อมต่อระบบคอมพิวเตอร์ของเทศบาลนครขอนแก่น ให้สามารถใช้งานระบบคอมพิวเตอร์ของเทศบาลนครขอนแก่นได้อย่างถูกต้องและเหมาะสม

๑.๔ เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของเทศบาลนครขอนแก่นโดนบุกรุก ขโมย ทำลายแทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินงานของเทศบาลนครขอนแก่น

๒. ขอบเขตของประกาศ

นโยบายฉบับนี้ใช้กับเทศบาลนครขอนแก่น ครอบคลุมการใช้งานระบบเครือข่ายคอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของเทศบาลนครขอนแก่น

๓. หลักการปฏิบัติ ...

๓. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

๓.๑ ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของเทศบาลนครขอนแก่น

๓.๒ ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูล ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต

๓.๓ ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้

๓.๔ การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

๓.๕ การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

๓.๖ การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่ามีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

๔. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

๔.๑ การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

- ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่ผู้ใช้งานได้รับอนุญาต หรือได้รับการมอบอำนาจตามที่กำหนด “การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

- ผู้ดูแลระบบมีการกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้ อ่านข้อมูล สร้างข้อมูล นำเข้าข้อมูล แก้ไขข้อมูล อนุมัติ และดูข้อมูลได้เท่านั้น

- ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

- ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องได้รับการพิจารณาจากผู้บริหารของหน่วยงานสังกัดเป็นลายลักษณ์อักษร และหรือตามแบบฟอร์มที่ ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณ กำหนด

- ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายในเป็นไปตามลำดับชั้นความลับของข้อมูล

- ผู้ดูแลระบบกำหนดลำดับความสำคัญของข้อมูล ได้แก่ สำคัญมากที่สุด สำคัญมาก และทั่วไป

- ผู้ดูแลระบบ ...

- ผู้ดูแลระบบกำหนดระดับชั้นการเข้าถึง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ เจ้าของระบบ และผู้ใช้ระบบ

- ผู้ดูแลระบบกำหนดเวลาและช่องทางที่เข้าถึงได้ให้เหมาะสมตามแต่ละระบบงาน

๔.๒ การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

- ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารของหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบ ข้อมูลและระบบงานเพื่อเข้าใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่ งานควบคุมและบริการเทคโนโลยี ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณกำหนด ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

- ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ โดยต้องมีการอนุญาตเข้าใช้งานเป็นลายลักษณ์อักษรจากผู้บริหารสูงสุด เพื่อการจัดเก็บไว้เป็นหลักฐาน

- เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นในการใช้งาน โดยต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลหรือเจ้าของระบบงาน

๔.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

- การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออก โอน ย้าย หรือเมื่อเปลี่ยนตำแหน่งงาน

- ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศ โปรแกรมประยุกต์ (Application) ภายในหน่วยงาน จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้สาย (Wireless LAN) โดยไม่ต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔.๔ การกำหนดชั้นความสำคัญหรือความลับของข้อมูล (Data classification)

ใช้เกณฑ์ระดับของผู้ใช้งานระบบสารสนเทศหรือสิทธิ์การเข้าใช้งานระบบสารสนเทศของเทศบาลนครขอนแก่น เพื่อกำหนดระดับชั้นการเข้าถึงข้อมูล ดังนี้

- ผู้ดูแลระบบงานของเทศบาลนครขอนแก่น (ADMIN) สามารถกำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งานทั้งหมดในระบบได้

- ผู้ใช้งานเทศบาลนครขอนแก่น สามารถเข้าถึงข้อมูลเฉพาะหน่วยงานเท่านั้น

- ผู้ใช้งานสำหรับการบันทึกข้อมูลต่างๆ (create, edit, del และ export รายงาน)

- ผู้ใช้งานสำหรับดูข้อมูลได้อย่างเดียว (viewer และ export รายงาน)

- ผู้ใช้งานสำหรบการรับรองข้อมูลในระบบ (Approve)

๔.๕ การควบคุมการเข้าใช้งานระบบจากภายนอก

- ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากเทศบาลนครขอนแก่น

- หัวหน้าฝ่ายสถิติข้อมูล ...

- หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ หรือหัวหน้างานบริการและควบคุมเทคโนโลยี ฝ่ายสถิติข้อมูลสารสนเทศ กองยุทธศาสตร์และงบประมาณ เป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)

- ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากผู้บริหารระดับสูง และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบ และข้อมูลอย่างเคร่งครัด

- หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ หรือหัวหน้างานบริการและควบคุมเทคโนโลยี ฝ่ายสถิติข้อมูลสารสนเทศ กองยุทธศาสตร์และงบประมาณ เป็นผู้ดูแลระบบ ต้องควบคุมช่องทางหรือ firewall ที่ระบบสารสนเทศให้บริการใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการเข้าถึงต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

- การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น และให้ปิดช่องทางเมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

๔.๗ การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านการบริหารรหัสผ่าน

- งานบริการและควบคุมเทคโนโลยี ฝ่ายสถิติข้อมูลสารสนเทศ กองยุทธศาสตร์และงบประมาณ ต้องกำหนดชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ เฉพาะบุคคลไม่ซ้ำกัน และกำหนดชื่อผู้ใช้ในส่วนของชื่อผู้ใช้ของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่นๆ ให้มีความแตกต่างกัน

- ผู้ใช้งานต้องเก็บรักษารหัสผ่าน (Password) ของตนเอง และของกลุ่มไว้เป็นความลับ

- ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในจดหมายอิเล็กทรอนิกส์ (e-mail) หรือแบบฟอร์มอิเล็กทรอนิกส์ต่างๆ

- ไม่จดหรือบันทึกรหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

- กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

- ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

- ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบดำเนินการเปลี่ยนรหัสผ่านทันที หรือแจ้งให้งานควบคุมและบริการเทคโนโลยี ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณ ทราบเพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

- หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

- กรณีผู้ใช้งานของหน่วยงานภายในหน่วยงานลาออก ให้แจ้ง งานควบคุมและบริการเทคโนโลยี ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณ ดำเนินการยกเลิกสิทธิ์ของผู้ที่ลาออก ออกจากระบบทันที

- กรณีผู้ใช้งานของหน่วยงานภายในหน่วยงาน มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งานให้หน่วยงานต้นสังกัด แจ้งงานควบคุมและบริการเทคโนโลยี ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณ เพื่อดำเนินการเปลี่ยนแปลงสิทธิ์การในการใช้งาน

- ผู้ใช้งานทุกคนของหน่วยงาน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

๕. หน้าที่ของผู้บังคับบัญชา

ชี้แจง และส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

๖. หน้าที่ของผู้ใช้งาน

- ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของเทศบาลนครขอนแก่นโดยเคร่งครัด

- ให้ความร่วมมืออย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของเทศบาลนครขอนแก่น สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของเทศบาลนครขอนแก่นให้มีความปลอดภัย

- รายงานต่อผู้บริหารทันที เมื่อพบว่าอุปกรณ์ หรือข้อมูลสารสนเทศสำคัญสูญหาย หรือพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรม รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อเทศบาลนครขอนแก่น

๗. การควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ

การกำหนดนโยบายปรับปรุงแก้ไขเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาต อาจมีผลให้เกิดความผิดพลาดในโปรแกรม หรือมีข้อมูลที่ไม่ถูกต้องในระบบสารสนเทศและรายงานต่างๆ และการแก้ไขเปลี่ยนแปลง แก้ไขฐานข้อมูลโดยตรง และอาจทำให้ระบบล้มเหลวหรือหยุดชะงักการทำงานได้ การเปลี่ยนแปลงแก้ไขระบบ หรือโปรแกรมที่ใช้อยู่ จึงควรมีการกำหนดเป็นขั้นตอน โดยมีการอนุมัติและจัดทำเอกสารประกอบด้วย

- การกำหนดระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขระบบที่เป็นลายลักษณ์อักษรและมีการอนุมัติจากเจ้าของระบบงานเป็นลายลักษณ์อักษร

- มีการศึกษาผลกระทบ ...

- มีการศึกษาผลกระทบต่างๆ ทั้งผลกระทบงานด้านเทคนิค ผลกระทบที่มีต่อระบบอื่นและความเสี่ยงจากการเปลี่ยนแปลง

- มีการทดสอบระบบที่แก้ไขแล้ว ก่อนนำมาใช้งาน

- จัดทำเอกสารคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด และมีการแก้ไขเอกสารที่เกี่ยวข้อง เช่น คู่มือการใช้งาน คู่มือการแก้ไขระบบงาน และตารางการทำงานของผู้เกี่ยวข้องของการปฏิบัติงาน เป็นต้น

- มีการประเมินผลและทดสอบระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง

๘. กรรมสิทธิ์และสิทธิในทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญาที่เกิดจากการประดิษฐ์ของเทศบาลนครขอนแก่น หรือผู้ที่เทศบาลนครขอนแก่นอนุญาตให้จัดทำระบบ ให้ถือเป็นกรรมสิทธิ์ของฝ่ายที่ได้ประดิษฐ์ขึ้น นับตั้งแต่วันที่เกิดทรัพย์สินทางปัญญาใหม่นั้นขึ้น โดยแต่ละฝ่ายมีสิทธิที่จะนำทรัพย์สินทางปัญญาใหม่ไปใช้เพื่อประโยชน์ภายในหน่วยงาน ในลักษณะที่มิใช่การใช้ประโยชน์เชิงพาณิชย์

ผู้ใช้บริการต้องไม่เปิดเผยข้อมูลที่เทศบาลนครขอนแก่นกำหนดให้เป็นความลับ โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจากเทศบาลนครขอนแก่น ผู้ใช้บริการจะต้องไม่ใช้ชื่อทางการค้า เครื่องหมายการค้า เครื่องหมายการบริการ ตราสัญลักษณ์ ชื่อโดเมนของเทศบาลนครขอนแก่น โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากเทศบาลนครขอนแก่น

๙. กฎหมายที่ใช้บังคับ

การตีความ และการบังคับตามเงื่อนไขการให้บริการฉบับนี้ ให้เป็นไปตามกฎหมายไทย จึงให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๖ มกราคม พ.ศ. ๒๕๖๗

(นายธีระศักดิ์ ฑีฆายุพันธุ์)
นายกเทศมนตรีนครขอนแก่น