ประกาศเทศบาลนครปากเกร็ด

เรื่อง แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐

.....

เพื่อให้ ข้อมูล สารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของเทศบาลนครปากเกร็ด มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ สอดคล้องตามหลักมาตรฐานสากล และเป็นการปฏิบัติตามกฎหมายและระเบียบอื่นๆ ที่เกี่ยวข้อง รวมทั้งเพื่อให้เกิดมาตรการในการป้องกันปัญหา อันอาจเกิดขึ้นจากการถูกภาวะคุกคามต่างๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อความเสียหายแก่เทศบาลนครปากเกร็ดและหน่วยงานในสังกัด อีกทั้งเพื่อเป็นการป้องกันการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เทศบาลนครปากเกร็ดจึงเห็นสมควรกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ความสำคัญในการทำความเข้าใจกับบุคลากรถึงขอบเขตการใช้งานทรัพยากรคอมพิวเตอร์และนำไปบังคับใช้ เพื่อให้การใช้ ข้อมูล สารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ รวมทั้งการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครปากเกร็ด เกิดประโยชน์สูงสุด และมีความมั่นคงปลอดภัยโดยรวม

อาศัยอำนาจตามพระราชบัญญัติเทศบาล พ.ศ. ๒๔๙๖ มาตรา ๔๘ เตรส (๔) เทศบาลนครปากเกร็ดจึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศเทศบาลนครปากเกร็ด เรื่อง แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐”

ข้อ ๒. แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ ตามประกาศนี้ ให้มีผลใช้บังคับตั้งแต่วันถัดจากวันที่ประกาศ เป็นต้นไป

ข้อ ๓. เทศบาลนครปากเกร็ด ได้กำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ให้ครอบคลุมแนวทางการใช้งานระบบคอมพิวเตอร์และเครือข่าย ทั้งในการใช้งานเครื่องและอุปกรณ์คอมพิวเตอร์และในการใช้บริการสื่อสารข้อมูลในเครือข่าย โดยมีวัตถุประสงค์ ดังต่อไปนี้

/(๑) เพื่อพัฒนา . .

(๑) เพื่อพัฒนาคุณภาพบุคลากรในด้านการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความรู้ความเข้าใจการใช้เทคโนโลยีที่ถูกต้อง พัฒนาทักษะการใช้งานซอฟต์แวร์ในสำนักงานอย่างต่อเนื่อง ให้สามารถใช้งาน และแก้ไขปัญหาเฉพาะหน้า ในการใช้งานระบบซอฟต์แวร์ตามกระบวนงานได้ โดยมีแนวทางการใช้งานข้อมูลอย่างเป็นระบบ

(๒) เพื่อให้บุคลากรได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานระบบคอมพิวเตอร์และเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของเทศบาลนครปากเกร็ดให้ปลอดภัย มีความถูกต้อง และพร้อมใช้งานอยู่เสมอ

(๓) เพื่อให้บุคลากรได้ตระหนักถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยง ในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ทั้งในการปฏิบัติงานภายในและภายนอกสำนักงานเทศบาล ให้มีประสิทธิภาพสูงสุด รวมทั้งเสริมสร้างความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ

(๔) เพื่อกำหนดมาตรการควบคุม และกำหนดแนวทางการใช้บริการบนระบบเครือข่าย ได้แก่ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) และแนวทางควบคุมการใช้อินเทอร์เน็ต ซึ่งผู้ใช้บริการจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการบนระบบเครือข่าย โดยจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายกำหนด ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่กำหนดไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด อันจะทำให้การใช้บริการต่างๆ บนระบบเครือข่าย เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

ข้อ ๔. แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ มีองค์ประกอบดังต่อไปนี้

(๑) กฎหมายและระเบียบที่เกี่ยวข้อง

(๒) คำนิยามที่เกี่ยวข้อง

(๓) แนวทางการใช้งานเครื่องคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของเทศบาล และที่เป็นทรัพย์สินส่วนบุคคล

๓.๑ การใช้งานทั่วไป

๓.๒ ความปลอดภัยทางด้านกายภาพ สำหรับเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer)

๓.๓ แนวทางปฏิบัติเรื่องบัญชีผู้ใช้งาน (User Account)

๓.๔ แนวทางกำหนดรหัสผ่าน (Password)

๓.๕ แนวทางการพิสูจน์ตัวตน (Authentication)

/๓.๖ แนวทาง . .

๓.๖ แนวทางควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System)

๓.๗ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๓.๘ การสำรองข้อมูลและการกู้คืน (Data Backup and Recovery)

(๔) แนวทางการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

๔.๑ แนวทางการใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ดูแลระบบ (Administrator)

๔.๒ แนวทางการใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ใช้ (User)

(๕) แนวทางควบคุมการใช้อินเทอร์เน็ต (Internet)

๕.๑ แนวทางควบคุมการใช้อินเทอร์เน็ตสำหรับผู้ดูแลระบบ (Administrator)

๕.๒ แนวทางควบคุมการใช้อินเทอร์เน็ตสำหรับผู้ใช้ (User)

ข้อ ๕. ต้องจัดให้มีการตรวจสอบและควบคุมประสิทธิภาพของการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ด้วยการตรวจประเมินผลการปฏิบัติตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครปากเกร็ด เป็นประจำและสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖. ต้องจัดให้มีการทบทวนและปรับปรุงแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครปากเกร็ด เป็นประจำและสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗. ต้องมีการสร้างความรู้ความเข้าใจกับผู้ใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครปากเกร็ด เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่อาจเกิดจากการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการดังต่อไปนี้

(๑) เผยแพร่สารสนเทศ แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารผ่านเว็บไซต์ (Website) เฟซบุ๊ก (Facebook) สื่อสังคมออนไลน์ (Social Media) และช่องทางการสื่อสารอื่นๆ ของเทศบาลนครปากเกร็ด โดยให้ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) จัดอบรมให้ความรู้ เพื่อสร้างความเข้าใจแก่ผู้ใช้งาน ในสาระสำคัญที่เกี่ยวข้องกับการใช้ ข้อมูล สารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ รวมทั้ง การใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครปากเกร็ด ให้เกิดประโยชน์สูงสุดและมีความมั่นคงปลอดภัยโดยรวม ตามรายละเอียดของการปฏิบัติตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่ได้กำหนดไว้

/ข้อ ๘. การกำหนด . .

ข้อ ๘. การกำหนดความรับผิดชอบ

(๑) ระดับนโยบาย

๑.๑ กำหนดให้ผู้บริหารระดับสูงสุดของเทศบาลนครปากเกร็ด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือข้อมูลสารสนเทศของเทศบาลนครปากเกร็ด เกิดความเสียหาย หรือเกิดอันตรายใดๆ ต่อเทศบาลนครปากเกร็ด หรือต่อหน่วยงานของเทศบาลนครปากเกร็ด หรือต่อผู้หนึ่งผู้ใด อันเนื่องมาจากความจงใจ บกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติ ตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่ได้ประกาศนี้

๑.๒ กำหนดให้ผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศ ของเทศบาลนครปากเกร็ด เป็นผู้รับผิดชอบ ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

(๒) ระดับปฏิบัติ

๒.๑ ผู้ดูแลระบบ (Administrator) เป็นผู้รับผิดชอบ กำกับ ดูแล ควบคุม ตรวจสอบ รายงาน และให้ข้อเสนอแนะ เพื่อให้การปฏิบัติงานของผู้ใช้ (User) เป็นไปตามข้อกำหนดในแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ ที่ได้ประกาศใช้นี้

๒.๒ ผู้ใช้ (User) เป็นผู้รับผิดชอบการปฏิบัติงาน ให้เป็นไปตามข้อกำหนดในแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ ที่ได้ประกาศใช้นี้

ข้อ ๙. การกำหนดชั้นความลับของข้อมูลและสารสนเทศ ให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่นที่ได้ประกาศใช้ทดแทน

ข้อ ๑๐. องค์ประกอบของแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ ได้กำหนดขึ้นเพื่อให้มีมาตรการและแนวทางในการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้อยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย จึงจัดเป็นส่วนหนึ่งของมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งบุคลากรทุกหน่วยงานของเทศบาลนครปากเกร็ด รวมทั้งบุคลากรของหน่วยงานภายนอกอื่นที่เกี่ยวข้อง ต้องถือปฏิบัติตามอย่างเคร่งครัด

/ข้อ ๑๑. เทศบาล . .

ข้อ ๑๑. เทศบาลนครปากเกร็ดจะดำเนินการทางวินัยหรือทางกฎหมายกับผู้ที่จงใจ บกพร่องละเลย หรือฝ่าฝืน ไม่ปฏิบัติตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ ตามที่ประกาศนี้ จนเป็นเหตุให้ก่อหรืออาจก่อให้เกิดความเสียหาย หรืออันตรายใดๆ ต่อข้อมูลสารสนเทศ หรือต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครปากเกร็ด หรือต่อหน่วยงานของเทศบาลนครปากเกร็ด หรือต่อผู้หนึ่งผู้ใด

ข้อ ๑๒. รายละเอียดของการปฏิบัติตามแนวทางการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐ ตามที่แนบท้ายประกาศนี้

ข้อ ๑๓. จนกว่าจะได้มีการประกาศใช้ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเทศบาลนครปากเกร็ด ที่ต้องดำเนินการและจัดทำตามกฎหมายและประกาศที่เกี่ยวข้องกับเรื่องความมั่นคงปลอดภัยและความน่าเชื่อถือด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานของรัฐ ให้งดเว้นการถือปฏิบัติและการบังคับใช้ออกไปก่อน เฉพาะแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ดังต่อไปนี้

(๑) แนวทางปฏิบัติเรื่องบัญชีผู้ใช้งาน (User Account)

(๒) แนวทางกำหนดรหัสผ่าน (Password)

(๓) แนวทางการพิสูจน์ตัวตน (Authentication)

(๔) แนวทางการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System)

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๕ สิงหาคม พ.ศ. ๒๕๖๐

(นายวิชัย บรรดาศักดิ์)
นายกเทศมนตรีนครปากเกร็ด

เอกสารแนบ ๑

เอกสารแนบท้ายประกาศ

แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร

เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐

แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร

เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐

ตามแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร

เทศบาลนครปากเกร็ด พ.ศ. ๒๕๕๙ – ๒๕๖๓

สารบัญ

แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. ๒๕๖๐

1. หลักการและเหตุผล

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ.2559-2563 มีวัตถุประสงค์ให้เทศบาลนครปากเกร็ด สามารถใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ให้เกิดประโยชน์สูงสุดกับการทำงานประจำ เพิ่มคุณภาพการบริการประชาชนในทุกภารกิจ อีกทั้ง ยังสามารถใช้ประโยชน์จากข้อมูลข่าวสาร ด้วยการนำข้อมูลที่เป็นทรัพย์สินมาก่อประโยชน์ให้กับสังคม เช่น การเปิดเผยข้อมูลเชิงลึก ให้เกิดประโยชน์และนำไปสู่การวางรากฐานให้เทศบาลนครปากเกร็ดสามารถพัฒนาให้เป็นเมืองอัจฉริยะในอนาคต

ด้วยเหตุผลทั้งหมดข้างต้น เทศบาลนครปากเกร็ดจึงเห็นสมควรกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ความสำคัญในการทำความเข้าใจกับบุคลากรถึงขอบเขตการใช้งานทรัพยากรคอมพิวเตอร์ และนำไปบังคับใช้ เพื่อให้ข้อมูลและระบบเครือข่ายคอมพิวเตอร์สามารถเกิดประโยชน์สูงสุดและมีความมั่นคงปลอดภัยโดยรวม

2. วัตถุประสงค์และขอบเขต

เทศบาลนครปากเกร็ด ได้กำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ให้ครอบคลุมแนวทางการใช้งานระบบคอมพิวเตอร์และเครือข่าย ทั้งในการใช้งานเครื่องและอุปกรณ์คอมพิวเตอร์ และในการใช้บริการสื่อสารข้อมูลในเครือข่าย โดยมีวัตถุประสงค์ ดังต่อไปนี้

2.1. เพื่อพัฒนาคุณภาพบุคลากรในด้านการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความรู้ความเข้าใจการใช้เทคโนโลยีที่ถูกต้อง พัฒนาทักษะในการใช้งานซอฟต์แวร์ในสำนักงานอย่างต่อเนื่อง ให้สามารถใช้งานและแก้ไขปัญหาเฉพาะหน้า ในการใช้งานระบบซอฟต์แวร์ตามกระบวนงานได้ โดยมีแนวทางการใช้งานข้อมูลอย่างเป็นระบบ

2.2. เพื่อให้บุคลากรได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานระบบคอมพิวเตอร์และเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของเทศบาลนครปากเกร็ด ให้ปลอดภัย มีความถูกต้อง และพร้อมใช้งานอยู่เสมอ

2.3. เพื่อให้บุคลากรได้ตระหนักถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ทั้งในการปฏิบัติงานภายในและภายนอกสำนักงานเทศบาล ให้มีประสิทธิภาพสูงสุด รวมทั้งเสริมสร้างความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ

2.4. เพื่อกำหนดมาตรการควบคุม และกำหนดแนวทางการใช้บริการบนระบบเครือข่าย ได้แก่ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) และแนวทางควบคุมการใช้อินเทอร์เน็ต (Internet) ซึ่งผู้ใช้บริการจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการบนระบบเครือข่าย โดยจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายกำหนด ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่กำหนดไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด อันจะทำให้การใช้บริการต่างๆ บนระบบเครือข่าย เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

3. องค์ประกอบ

แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครปากเกร็ด พ.ศ. 2560 มีองค์ประกอบดังต่อไปนี้

3.1. กฎหมายและระเบียบที่เกี่ยวข้อง

3.2. คำนิยามที่เกี่ยวข้อง

3.3. แนวทางการใช้งานเครื่องคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของเทศบาล และที่เป็นทรัพย์สินส่วนบุคคล

3.3.1. การใช้งานทั่วไป

3.3.2. ความปลอดภัยทางด้านกายภาพ สำหรับเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer)

3.3.3. แนวทางปฏิบัติเรื่องบัญชีผู้ใช้งาน (User Account)

3.3.4. แนวทางกำหนดรหัสผ่าน (Password)

3.3.5. แนวทางการพิสูจน์ตัวตน (Authentication)

3.3.6. แนวทางควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System)

3.3.7. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

3.3.8. การสำรองข้อมูลและการกู้คืน (Data Backup and Recovery)

3.4. แนวทางการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

3.4.1. แนวทางการใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ดูแลระบบ (Administrator)

3.4.2. แนวทางการใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ใช้ (User)

3.5. แนวทางควบคุมการใช้อินเทอร์เน็ต (Internet)

3.5.1. แนวทางควบคุมการใช้อินเทอร์เน็ตสำหรับผู้ดูแลระบบ (Administrator)

3.5.2. แนวทางควบคุมการใช้อินเทอร์เน็ตสำหรับผู้ใช้ (User)

กฎหมายและระเบียบที่เกี่ยวข้อง

การพิจารณาดำเนินการ เพื่อกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ของเทศบาลนครปากเกร็ดนั้น มีตัวบทกฎหมายและระเบียบ รวมทั้งประกาศที่เกี่ยวข้อง ดังต่อไปนี้

1. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 มีสาระสำคัญในการระบุฐานความผิดและบทลงโทษสำหรับการละเมิดลิขสิทธิ์
2. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ระบุถึงบทบาทและหน้าที่ของการเปิดเผยข้อมูลข่าวสารของทางราชการ
3. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 กฎหมายฉบับนี้ระบุถึงการรองรับทางกฎหมายของข้อความหรือนิติกรรมสัญญาที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ รวมทั้งลายมือชื่ออิเล็กทรอนิกส์ ให้มีผลทางกฎหมายที่แน่นอนเท่ากับนิติกรรมสัญญา หรือผลผูกพันที่ตกลงหรือทำการผ่านกระดาษ
4. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 เป็นกฎหมายที่กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ ภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน เพื่อสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์
5. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่กำหนดฐานความผิดและบทลงโทษ สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรืออาชญากรรมทางคอมพิวเตอร์
6. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 ฉบับแก้ไขเพิ่มเติมที่มีประเด็นสำคัญว่าด้วยเรื่องของลายมือชื่ออิเล็กทรอนิกส์
7. ระเบียบเทศบาลนครปากเกร็ด ว่าด้วยข้อมูลข่าวสารของราชการ พ.ศ. 2552 ออกตามความในมาตรา 9 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นระเบียบเพื่อให้การบริการข้อมูลข่าวสารของราชการที่อยู่ในความรับผิดชอบของเทศบาลนครปากเกร็ด เป็นไปด้วยความเรียบร้อย รวดเร็ว และสอดคล้องกับเจตนารมณ์ของกฎหมาย ในการรับรองสิทธิของประชาชน ในการรับรู้ข้อมูลข่าวสารที่อยู่ในความครอบครองของหน่วยงานของรัฐ
8. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 จัดทำประกาศขึ้น เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

9. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553 เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกตามความในมาตรา 12/1 วรรคสอง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 ที่กำหนดให้การจัดทำหรือแปลงเอกสารและข้อความ ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ให้เป็นไปตามหลักเกณฑ์และวิธีการตามประกาศนี้
10. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 เป็นกฎหมายที่กำหนดหลักเกณฑ์และวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ ให้มีมาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมีการบริหารจัดการการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีการยอมรับและเชื่อมั่นในข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น รวมทั้งให้สอดรับกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 25 ที่บัญญัติให้ธุรกรรมทางอิเล็กทรอนิกส์ใดที่กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาแล้ว ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้
11. ระเบียบเทศบาลนครปากเกร็ด ว่าด้วยการใช้งานระบบคอมพิวเตอร์ พ.ศ. 2554 เป็นระเบียบที่เทศบาลนครปากเกร็ดจัดทำขึ้น เพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างเหมาะสม และมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง
12. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ อาศัยอำนาจตามความในมาตรา 6 วรรคหนึ่ง แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2553 ออกประกาศเพื่อกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยไว้
13. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ อาศัยอำนาจตามความในมาตรา 7 แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2553 ที่กำหนดให้คณะกรรมการประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใด ที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนด เป็นวิธีการที่เชื่อถือได้

14. พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ. 2559 เป็นกฎหมายว่าด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
15. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 สาระสำคัญของพระราชบัญญัติฉบับนี้ มีอาทิ
    - เพิ่มเติมความผิดของการส่งสแปมเมล์ (spam mail)
    - แก้ไขให้ไม่สามารถนำไปฟ้องฐานหมิ่นประมาทตามประมวลกฎหมายอาญาได้
    - แก้ไขให้ยกเว้นความผิดสำหรับผู้ให้บริการได้หากยอมลบข้อมูลที่ผิดกฎหมาย
    - เพิ่มเติมให้ผู้ใดที่มีข้อมูลซึ่งศาลสั่งให้ทำลายอยู่ในครอบครองจะต้องทำลายไม่เช่นนั้นจะได้รับโทษด้วย
    - เพิ่มเติมให้มีคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ขึ้นมาพิจารณาว่าข้อมูลคอมพิวเตอร์ใดที่จะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน สามารถส่งฟ้องศาลเพื่อระงับหรือลบข้อมูลดังกล่าวได้

แต่อย่างไรก็ตาม เนื้อหาหลายมาตราในพระราชบัญญัติฉบับนี้ จะต้องให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ออกกฎกระทรวงหรือประกาศ เพื่อกำหนดรายละเอียดการใช้บังคับต่อไป

คำนิยามที่เกี่ยวข้อง

1. เทศบาล หมายถึง เทศบาลนครปากเกร็ด
2. หน่วยงาน หมายถึง สำนัก ศูนย์ กอง ส่วน ฝ่าย หน่วย และงาน ที่อยู่ในสังกัดเทศบาลนครปากเกร็ด
3. หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอก ที่เทศบาลอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
4. นายกเทศมนตรี หมายถึง นายกเทศมนตรีนครปากเกร็ด
5. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของเทศบาลนครปากเกร็ด
6. ผู้บริหาร หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ปลัดเทศบาล หัวหน้ากองหรือเทียบเท่า ผู้อำนวยการสำนัก/กอง หัวหน้าฝ่าย เป็นต้น
7. ผู้บริหารระดับสูง หมายถึง ปลัดเทศบาลหรือเทียบเท่า
8. ผู้ดูแลระบบ (System Administrator) และ/หรือ ผู้ดูแลระบบคอมพิวเตอร์ (Computer System Administrator) หมายถึงผู้ที่ได้รับมอบหมายจากเทศบาล ให้มีหน้าที่รับผิดชอบดูแลบำรุงรักษา และบริหารจัดการ ระบบคอมพิวเตอร์และระบบเครือข่าย ไม่ว่าส่วนหนึ่งส่วนใด รวมถึงผู้รับจ้างดูแลและซ่อมบำรุงระบบคอมพิวเตอร์และเครือข่าย ที่ปฏิบัติงานตามสัญญาจ้างที่ได้ทำไว้กับเทศบาลนครปากเกร็ด
9. ผู้ใช้ และ/หรือ ผู้ใช้งาน (User) หมายถึง คณะผู้บริหาร สมาชิกสภาเทศบาล ข้าราชการ ลูกจ้าง พนักงานราชการ พนักงานเทศบาล พนักงานจ้าง ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน รวมทั้ง บุคคลอื่นที่เทศบาลมอบหมายให้ปฏิบัติงาน และให้หมายรวมถึงบุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของเทศบาล โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งได้กำหนดไว้
10. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงาน ให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น
11. เจ้าของบัญชีผู้ใช้บริการ หมายถึง บัญชีผู้ใช้ (User Account) ที่อนุญาตให้เจ้าของบัญชีผู้ใช้นั้นๆ มีสิทธิ์ในการใช้บริการต่างๆ โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ยืนยันตัวบุคคลในการเข้าใช้งาน
12. ผู้ทำหน้าที่ตรวจสอบ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บริหาร เพื่อทำการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศ

13. <u>เจ้าหน้าที่ที่ได้รับมอบหมายให้ตรวจสอบสินทรัพย์</u> หมายถึงผู้ที่ได้รับการมอบหมายจากผู้บริหาร ให้ทำการตรวจสอบสินทรัพย์ในความครอบครองของเทศบาลนครปากเกร็ด
14. <u>เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ</u> หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้รับผิดชอบในการจัดการดูแลระบบสารสนเทศให้มีความมั่นคงปลอดภัย
15. <u>สิทธิของผู้ใช้งาน</u> หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์
16. <u>สินทรัพย์</u> หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer) อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย เช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
17. <u>สินทรัพย์ส่วนบุคคล</u> หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เป็นสมบัติส่วนตัวของผู้ใช้งาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer) อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย เช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
18. <u>ข้อมูล (Data) และ/หรือ ข้อมูลคอมพิวเตอร์ (Computer Data)</u> หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
19. <u>สารสนเทศ (Information)</u> หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ ในการบริหารจัดการ การวางแผน การตัดสินใจ และอื่นๆ
20. <u>รหัสผ่าน (Password)</u> หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูล ในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ
21. <u>เครื่องคอมพิวเตอร์</u> หมายถึง ครุภัณฑ์คอมพิวเตอร์ ทั้งที่เป็นคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer) ที่อยู่ในบัญชีครุภัณฑ์ และที่ไม่อยู่ในบัญชีครุภัณฑ์ของเทศบาล แต่นำมาใช้เพื่องานราชการ

22. ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
23. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง แนวทางปฏิบัติงาน หรือสิ่งอื่นใด ให้อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมต่อกันนั้น ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
24. ระบบแลน (LAN) และ/หรือ ระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
25. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงาน หรือระหว่างหน่วยงานกับหน่วยงานภายนอกได้ เช่น ระบบเครือข่ายท้องถิ่นแบบมีสาย (Cabling LAN) ระบบเครือข่ายแบบไร้สาย (Wireless LAN หรือ WLAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
26. จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่รับส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
27. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารจัดการ การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
28. ความมั่นคงปลอดภัย (Security) หมายถึง สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ
29. ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) การตรวจสอบได้ (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

30. ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ด้านสารสนเทศ ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จ
31. มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
32. ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
33. แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
34. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น
    34.1. พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ที่ประจำโต๊ะทำงาน และพื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
    34.2. พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) หมายถึง พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานระบบเครือข่ายทั้งหมด ไม่ว่าจะเป็นพื้นที่ใช้งานระบบเครือข่ายท้องถิ่นแบบมีสาย (Cabling LAN coverage area) หรือพื้นที่ใช้งานระบบเครือข่ายท้องถิ่นแบบไร้สาย (Wireless LAN coverage area)
35. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
36. ประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป
37. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) หมายถึง การเกิดเหตุการณ์สภาพของบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

38. แผนการเตรียมพร้อมกรณีฉุกเฉิน หมายถึง แผนแก้ไขปัญหาจากการเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูล สารสนเทศ หรือมีการซักซ้อมการดำเนินการตามแผน
39. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
40. ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม เกิดการขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

แนวทางการใช้งานเครื่องคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของเทศบาล และที่เป็นทรัพย์สินส่วนบุคคล

การกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ของเทศบาลนครปากเกร็ด ให้ครอบคลุมแนวทางการใช้งานระบบคอมพิวเตอร์และเครือข่าย ในการใช้งานเครื่องและอุปกรณ์คอมพิวเตอร์ มีความสำคัญในการทำความเข้าใจกับบุคลากร ถึงขอบเขตการใช้งานทรัพยากรคอมพิวเตอร์ และนำไปบังคับใช้ เพื่อให้ข้อมูลและระบบเครือข่ายคอมพิวเตอร์สามารถเกิดประโยชน์สูงสุด และมีความมั่นคงปลอดภัยโดยรวม โดยได้กำหนดแนวทางการใช้งานเครื่องคอมพิวเตอร์ ที่ครอบคลุมเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer) ทั้งที่เป็นทรัพย์สินของเทศบาล และที่เป็นทรัพย์สินส่วนบุคคล

1. วัตถุประสงค์

แนวทางการใช้งานเครื่องคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของเทศบาลและที่เป็นทรัพย์สินส่วนบุคคล ได้ถูกจัดทำขึ้นโดยมีวัตถุประสงค์ดังต่อไปนี้

1.1. เพื่อให้ผู้ใช้ได้รับทราบถึงหน้าที่ และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ ซึ่งผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของเทศบาลนครปากเกร็ด ให้ปลอดภัย มีความถูกต้อง และพร้อมใช้งานอยู่เสมอ

1.2. เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์ ในการนำไปปฏิบัติงานทั้งภายในและภายนอกหน่วยงาน และเพื่อเป็นการป้องกันข้อมูลและอุปกรณ์เครื่องคอมพิวเตอร์ของเทศบาล ให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนด และมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์ให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1. ผู้ใช้งาน ต้องยอมรับทราบ กฎระเบียบ หรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

2.2. เครื่องคอมพิวเตอร์ที่เทศบาลอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของเทศบาล ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ ด้วยการใช้งานที่เหมาะสม ประหยัดทรัพยากร คุ้มค่า คุ้มราคา ถนอมรักษาให้มีอายุการใช้งานที่ยาวนาน และเป็นการใช้เพื่อการปฏิบัติงานของเทศบาล

2.3. ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้ง และแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของเทศบาล

2.4. ก่อนการใช้งานสื่อบันทึกข้อมูลแบบพกพาต่างๆ ต้องมีการสแกน (Scan) ตรวจสอบเพื่อหาไวรัส โดยโปรแกรมป้องกันไวรัส

2.5. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของเทศบาล ต้องเป็นโปรแกรมที่เทศบาลได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน โดยผิดกฎหมาย

2.6. การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่ของเทศบาล หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ที่ได้ทำสัญญากับเทศบาลเท่านั้น

2.7. ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

2.8. ห้ามนำเครื่องคอมพิวเตอร์ที่ไม่ใช่ทรัพย์สินของเทศบาล มาใช้กับระบบเครือข่ายของเทศบาล ยกเว้น จะได้รับการอนุญาตจากผู้บังคับบัญชาหรือผู้บริหาร

2.9. ไม่เก็บข้อมูลสำคัญของเทศบาล ไว้บนเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินส่วนบุคคล

2.10. ไม่สร้าง short-cut หรือปุ่มกดง่าย บน desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของเทศบาล

2.11. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่ของเทศบาลเท่านั้น

2.12. ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.13. ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

2.14. การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

2.15. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แตกเสียหายได้

2.16. ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.17. ไม่ใช้หรือวางเครื่องคอมพิวเตอร์ ใกล้สิ่งที่เป็นของเหลว หรือมีความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

2.18. ไม่เคลื่อนย้ายเครื่องคอมพิวเตอร์ในขณะที่ Hard Disk กำลังทำงาน

2.19. ไม่ใช้หรือวางเครื่องคอมพิวเตอร์ ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.20. ไม่วางเครื่องคอมพิวเตอร์ ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.21. ไม่ติดตั้งหรือวางคอมพิวเตอร์ ในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

2.22. การเช็ดทำความสะอาดหน้าจอภาพ ควรเช็ดอย่างเบามือที่สุด และเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

3. ความปลอดภัยทางด้านกายภาพสำหรับเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer)

3.1. ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อค (Lock) เครื่อง ขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2. ผู้ใช้ ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์ ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3.3. ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่ (Battery)

3.4. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก ต้องใส่กระเป๋าที่ทำเฉพาะสำหรับเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

3.5. ในกรณีที่มีการเดินทาง ห้ามใส่เครื่องคอมพิวเตอร์ขนาดสมุดบันทึกไปในกระเป๋าเดินทาง เพราะเสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับ หรือกระเป๋าเดินทางอาจถูกจับโยนได้

3.6. การเคลื่อนย้ายเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก ในขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

4. แนวทางปฏิบัติเรื่องบัญชีผู้ใช้งาน (User Account)

4.1. ผู้ดูแลระบบ จะต้องกำหนดบัญชีผู้ใช้งาน (User Account) ซึ่งประกอบด้วย ชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน โดยกำหนดชื่อผู้ใช้งานให้เป็นไปในแนวทางเดียวกันทั้งหน่วยงาน

4.2. การกำหนดรหัสผ่านครั้งแรกให้กับบัญชีผู้ใช้งานใหม่ (New Account) หรือการรีเซท (Reset) รหัสผ่าน จะต้องกำหนดรหัสผ่านให้ยากต่อการคาดเดา และต้องส่งมอบรหัสผ่านให้กับผู้ใช้งานอย่างรัดกุมปลอดภัย

4.3. ผู้ดูแลระบบต้องตั้งค่าระบบ บังคับให้ผู้ใช้เปลี่ยนรหัสผ่านที่กำหนดให้ในทันที ที่ผู้ใช้งาน Log in เข้าระบบในครั้งแรก ด้วยบัญชีผู้ใช้ใหม่ หรือด้วยรหัสผ่านชั่วคราวที่ได้กำหนดให้จากการ Reset Password

4.4. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน ไม่ว่าการกระทำนั้นๆ จะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

4.5. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่าน โดยต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

5. แนวทางกำหนดรหัสผ่าน (Password)

5.1. ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยการกำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรไม่น้อยกว่า 6 ตัวอักษร ซึ่งต้องประกอบด้วย ตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

5.2. ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว

5.3. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

5.4. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ทุก 3–6 เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

6. แนวทางการพิสูจน์ตัวตน (Authentication)

6.1. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของเทศบาล

6.2. หากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่าน หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

6.3. คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

6.4. การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

6.5. การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนของบุคคลผู้ใช้งานได้

6.6. เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

7. แนวทางการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System)

7.1. ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

7.2. ผู้ใช้ ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที เพื่อให้ทำการล็อค (Lock) หน้าจอ เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้ต้องใส่รหัสผ่าน

7.3. ผู้ใช้ ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

7.4. ในระหว่างเวลาพักกลางวัน หรือเมื่อไม่อยู่ที่หน้าจอเป็นเวลานาน ผู้ใช้ต้อง Log out ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

7.5. เมื่อเลิกงาน ผู้ใช้ต้อง Log out ออกจากระบบ และปิดเครื่องทุกครั้ง

8. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

8.1. ผู้ใช้ มีหน้าที่รับผิดชอบในการอัปเดต (Update) โปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

8.2. ผู้ใช้ ต้องให้โปรแกรมตรวจสอบไวรัส ทำการตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่างๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

8.3. ผู้ใช้ ต้องรับผิดชอบตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

8.4. ผู้ใช้ต้องสังเกตและตรวจสอบเครื่องคอมพิวเตอร์ที่ใช้งาน ที่อาจมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หากตรวจพบเจอ ให้รีบแจ้งผู้ดูแลระบบเพื่อดำเนินการแก้ไข

9. การสำรองข้อมูลและการกู้คืน (Data Backup and Recovery)

9.1. ผู้ใช้ ต้องประเมินความเสี่ยงว่า ข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของเทศบาล

9.2. ผู้ใช้ ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ ไว้บนสื่อบันทึกข้อมูลอื่นๆ เช่น CD, DVD, Thumb drive, External Hard Disk เป็นต้น

9.3. ผู้ใช้ มีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรอง (Data Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหล การสูญหาย หรือการเสียหายของข้อมูลที่เก็บไว้ในสื่อบันทึกข้อมูลสำรอง

9.4. สื่อบันทึกข้อมูลสำรองที่เก็บไว้ จะต้องทำการทดสอบการกู้คืนข้อมูล (Data recovery) ที่สำรองไว้อย่างสม่ำเสมอ

9.5. สื่อบันทึกข้อมูลสำรองที่ไม่ใช้งานแล้ว ต้องทำลายทิ้ง ไม่ให้สามารถนำกลับมาใช้งานได้อีก

แนวทางการใช้
จดหมายอิเล็กทรอนิกส์ (E-mail)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์ และต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์ ไม่กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด อันจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย เป็นไปอย่างปลอดภัย และมีประสิทธิภาพ

2. แนวทางการใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ดูแลระบบ (Administrator)

2.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของเทศบาล ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ และเหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์ บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริง ของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของเทศบาล

2.3 ผู้ดูแลระบบต้องกำหนดให้ระบบบังคับให้มีการเปลี่ยนรหัสผ่านโดยทันที เมื่อผู้ใช้รายใหม่ (New user) ที่ได้รับรหัสผ่านเป็นค่าเริ่มต้น (Default Password) ได้ทำการ Log in เข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก

2.4 ผู้ดูแลระบบต้องกำหนดให้การใส่รหัสผ่าน เพื่อ Log in เข้าระบบจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่าน ต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น ✕ หรือ ● ในการพิมพ์แต่ละตัวอักษร

2.5 ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง

2.6 ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ มีการ Log out ออกจากหน้าจอ ตัดการใช้งานของผู้ใช้ออกจากระบบ (Session Timeout) เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที และเมื่อต้องการเข้าใช้งานต่อ ต้องใส่ชื่อผู้ใช้และรหัสผ่าน (Log in) ใหม่

2.7. เมื่อผู้ดูแลระบบทำการ Reset Password และกำหนดรหัสผ่านชั่วคราวให้ผู้ใช้ ต้องกำหนดให้ระบบบังคับให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับมา ในทันทีที่ Log in เข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ด้วยรหัสผ่านชั่วคราวนั้น

2.8 ผู้ดูแลระบบต้องกำหนดเป็นนโยบายของระบบ (System Policy) ให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านเป็นประจำสม่ำเสมอ ทุก 3 - 6 เดือน

3. แนวทางการใช้จดหมายอิเล็กทรอนิกส์สำหรับผู้ใช้ (User)

3.1 ผู้ใช้ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์ และต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์

3.2 ผู้ใช้ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ตามระยะเวลาที่ระบบกำหนดไว้

3.3 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกที่เป็นค่าเริ่มต้น (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น จะต้องมีเปลี่ยนรหัสผ่านตามที่ระบบบังคับไว้โดยทันที

3.4 การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติ ตามที่ระบุไว้ในหัวข้อ “แนวทางกำหนดรหัสผ่าน”

3.5 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail Account) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ของหน่วยงาน และยื่นคำขอกับผู้รับผิดชอบของแต่ละหน่วยงาน โดยเสนอให้ผู้บริหารอนุมัติ และส่งรายชื่อมายังผู้ดูแลระบบ เพื่อดำเนินการลงทะเบียนการใช้บริการ

3.6 ผู้ใช้ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อองค์กร หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของเทศบาล

3.7 ห้ามมิให้ผู้ใช้ ใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-mail Account) ของผู้อื่น เพื่ออ่าน และ/หรือ รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

3.8 ผู้ใช้ ต้องใช้ บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-mail Account) และที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของเทศบาล เพื่อการทำงานของเทศบาลเท่านั้น

3.9 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Log out ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์

3.10 ผู้ใช้ต้องทำการตรวจสอบไฟล์เอกสารแนบ (Attachment file) ที่แนบมากับจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ด้วยการตรวจสอบโดยใช้โปรแกรมป้องกันไวรัส เพื่อเป็นการป้องกันความปลอดภัยและลดความเสี่ยงในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

3.11 ผู้ใช้ ต้องระมัดระวังในการเปิดรับ หรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

3.12 ผู้ใช้ต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือมีข้อมูลอันอาจทำให้เสียชื่อเสียงของเทศบาล ทำให้เกิดความแตกแยกระหว่างองค์กรหรือหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

3.13 ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

3.14 ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

3.15 ผู้ใช้ต้องไม่โอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

3.16 ผู้ใช้ต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับมาจากผู้ดูแลระบบ เมื่อร้องขอการ Reset Password โดยต้องเปลี่ยนรหัสผ่านชั่วคราว ในทันทีตามที่ระบบบังคับไว้ เมื่อได้ Log in เข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ด้วยรหัสผ่านชั่วคราวที่ได้รับมานั้น

3.17 การส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูล ลงในหัวข้อจดหมายอิเล็กทรอนิกส์ เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล (Data Encryption) และต้องใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิดตัวผู้รับ

3.18 ห้ามส่ง จดหมายอิเล็กทรอนิกส์ ที่มีลักษณะเป็น จดหมายขยะ (Spam Mail) หรือ จดหมายลูกโซ่ (Chain Letter) หรือ ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

3.19 ห้ามส่งจดหมายอิเล็กทรอนิกส์ ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

3.20 ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ ทุกฉบับที่ส่งไป

3.21 ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ ตามความจำเป็นอย่างสม่ำเสมอ

แนวทางควบคุม
การใช้อินเทอร์เน็ต (Internet)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล การส่งข้อความ การส่งคำสั่ง/ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข หรือการทำให้ระบบคอมพิวเตอร์ของเทศบาล ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวน จนไม่สามารถทำงานตามปกติได้

2. แนวทางควบคุมการใช้อินเทอร์เน็ตสำหรับผู้ดูแลระบบ (Administrator)

2.1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต โดยต้องเชื่อมต่อด้วยช่องทางผ่านระบบรักษาความปลอดภัยที่เทศบาลจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems) เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem เว้นแต่มีเหตุผลความจำเป็น และได้ทำการขออนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษรแล้ว

2.2 เครื่องคอมพิวเตอร์ที่จะใช้งานอินเทอร์เน็ต ก่อนที่จะทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

2.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการตรวจสอบหาไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

2.4 ผู้ดูแลระบบ เป็นผู้ดูแลรับผิดชอบการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงแหล่งข้อมูลในเครือข่ายอินเทอร์เน็ตตามหน้าที่ความรับผิดชอบที่ผู้ใช้ได้รับมอบหมาย เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยของข้อมูลของเทศบาล

3. แนวทางควบคุมการใช้อินเทอร์เน็ตสำหรับผู้ใช้ (User)

3.1 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของเทศบาล เผยแพร่ข้อมูล ที่ไม่เหมาะสมทางศีลธรรมจรรยา ที่เป็นการหาประโยชน์ส่วนตัว ที่ละเมิดสิทธิ์ของผู้อื่น หรือเป็นข้อมูลที่อาจก่อความเสียหายให้กับเทศบาล

3.2 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของเทศบาล เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม อาทิ เว็บไซต์ที่มีเนื้อหาที่ขัดต่อความมั่นคงปลอดภัยของชาติ ศาสนา พระมหากษัตริย์ หรือขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี หรือเว็บไซต์ที่เป็นภัยต่อสังคม

3.3 ผู้ใช้ได้รับอนุญาตให้ใช้เครือข่ายอินเทอร์เน็ตของเทศบาล ในการเข้าถึงแหล่งข้อมูลต่างๆ ตามหน้าที่ความรับผิดชอบของตน ตามที่ได้รับมอบหมายเท่านั้น ทั้งนี้เพื่อประสิทธิภาพของเครือข่าย และความปลอดภัยของข้อมูลของเทศบาล

3.4 ห้ามมิให้ผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของเทศบาล ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านสื่อสังคมออนไลน์ (Social Media) เว็บบอร์ด (Web Board) หรือสื่อต่างๆ ในระบบอินเทอร์เน็ต

3.5 ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว ผ่านเครือข่ายอินเทอร์เน็ต

3.6 ผู้ใช้ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เพิ่มเติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่อาจจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

3.7 ผู้ใช้มีหน้าที่รับผิดชอบ ตรวจสอบความถูกต้อง และความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลคอมพิวเตอร์นั้นไปใช้งานหรือเผยแพร่ต่อ

3.8 ผู้ใช้ต้องระมัดระวังการดาวน์โหลด (Download) โปรแกรมใช้งานจากอินเทอร์เน็ต และการดาวน์โหลดการอัปเดต (Update) ซึ่งรวมถึงแพตช์ (Patch) หรือฟิกซ์ (Fix) ต่างๆ โดยต้องระมัดระวังให้การดาวน์โหลดดังกล่าวนั้น ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

3.9 ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของเทศบาล หรือเป็นการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

3.10 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

3.11 การใช้งานระบบคอมพิวเตอร์เพื่อใช้อินเทอร์เน็ต ต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560