ประกาศเทศบาลนครนนทบุรี

เรื่อง แนวทางการปฏิบัติงานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑

.....

เพื่อให้ ข้อมูลสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของเทศบาลนครนนทบุรี มีความมั่นคงปลอดภัย สามารถดำเนินการได้อย่างต่อเนื่อง มีประสิทธิภาพ สอดคล้องตามหลักมาตรฐานสากล และเป็นการปฏิบัติตามกฎระเบียบอื่นๆ ที่เกี่ยวข้อง รวมทั้งเพื่อให้เกิดมาตรการในการป้องกันปัญหา อันอาจเกิดขึ้นจากการถูกภาวะคุกคามต่างๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อความเสียหายแก่เทศบาลนครนนทบุรีและหน่วยงานในสังกัด อีกทั้งเพื่อเป็นการป้องกันการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เทศบาลนครนนทบุรีจึงเห็นสมควรกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ความสำคัญในการทำความเข้าใจกับบุคลากรถึงขอบเขตการใช้งานทรัพยากรคอมพิวเตอร์และนำไปบังคับใช้ เพื่อให้ใช้ข้อมูลสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ รวมทั้งการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครนนทบุรี เกิดประโยชน์สูงสุด และมีความมั่นคงปลอดภัยโดยรวม

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

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศเทศบาลนครนนทบุรี เรื่อง แนวทางการปฏิบัติงานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ.๒๕๖๑”

ข้อ ๒. แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑ ตามประกาศนี้ ให้มีผลบังคับตั้งแต่วันถัดจากวันที่ประกาศ เป็นต้นไป

ข้อ ๓. เทศบาลนครนนทบุรี ได้กำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศ และการสื่อสารให้ครอบคลุมแนวทางการใช้งานระบบคอมพิวเตอร์และเครือข่าย รวมทั้งการใช้งานเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ และในการใช้บริการสื่อสารข้อมูลในเครือข่าย โดยมีวัตถุประสงค์ ดังต่อไปนี้

(๑) เพื่อให้บุคลากรได้ตระหนักถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ทั้งในการปฏิบัติงานภายในและนอกสำนักงานเทศบาลนครนนทบุรี ให้มีประสิทธิภาพสูงสุด รวมทั้งเสริมสร้างความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

(๒) เพื่อกำหนดมาตรการควบคุม และกำหนดแนวทางการใช้บริการบนระบบเครือข่าย ได้แก่ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) และแนวทางควบคุมการใช้งานอินเตอร์เน็ต ซึ่งผู้ใช้บริการจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการบนระบบเครือข่าย โดยจะต้องเข้าใจเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายกำหนด ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่สร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่กำหนดไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด อันจะทำให้การใช้บริการต่างๆ บนระบบเครือข่าย เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

(๓) เพื่อให้บุคลากรได้รับทราบถึงหน้าที่ และความรับผิดชอบในการใช้งานระบบคอมพิวเตอร์และเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของเทศบาลนครนนทบุรีให้ปลอดภัย มีความถูกต้อง และพร้อมใช้งานอยู่เสมอ

(๔) เพื่อพัฒนาคุณภาพบุคลากรในด้านการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารให้มีความรู้ความเข้าใจการใช้เทคโนโลยีที่ถูกต้อง พัฒนาทักษะการใช้งานซอฟต์แวร์ในสำนักงานอย่างต่อเนื่อง ให้สามารถใช้งานและแก้ไขปัญหาเฉพาะหน้า ในการใช้งานระบบซอฟแวร์ตามกระบวนงานได้ โดยมีแนวทางการใช้งานข้อมูลอย่างเป็นระบบ

(๕) เพื่อกำหนดแนวทางการใช้บริการระบบภูมิสารสนเทศผ่านระบบอินเตอร์เน็ต ซึ่งผู้ใช้บริการจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการบนระบบภูมิสารสนเทศฯ โดยจะต้องเข้าใจเกณฑ์ต่างๆ ที่ผู้ดูแลระบบภูมิสารสนเทศฯ กำหนด ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่สร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่กำหนดไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบภูมิสารสนเทศฯ อย่างเคร่งครัด อันจะทำให้การใช้บริการต่างๆ บนระบบเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

ข้อ ๔ แนวทางการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑ มีองค์ประกอบดังต่อไปนี้

(๑) กฎหมายและระเบียบที่เกี่ยวข้อง

(๒) คำนิยามที่เกี่ยวข้อง

(๓) แนวทางการใช้งานเครื่องคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของเทศบาลและที่เป็นทรัพย์สินส่วนบุคคล

๓.๑ แนวทางปฏิบัติเมื่อพบว่าเครื่องคอมพิวเตอร์ติดไวรัส (Virus Computer)

๓.๒ แนวทางปฏิบัติเกี่ยวกับรหัสผ่าน (Password)

๓.๓ แนวทางปฏิบัติการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

๓.๔ แนวทางปฏิบัติการสำรองข้อมูล (Data Backup)

๓.๕ แนวทางปฏิบัติการใช้งานและค้นหาข้อมูลบนระบบเครือข่าย (Internet)

๓.๖ แนวทางปฏิบัติในการติดตั้งโปรแกรมสำเร็จรูป (Software)

๓.๗ แนวทางปฏิบัติในการนำอุปกรณ์ส่วนตัวเชื่อมต่อเครือข่ายหน่วยงาน

๓.๘ แนวทางปฏิบัติเมื่อพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติ

๓.๙ แนวทางปฏิบัติในการใช้ Handy Drive

๓.๑๐ แนวทางปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

๓.๑๑ แนวทางปฏิบัติในการแลกเปลี่ยนข้อมูลผ่านเครือข่าย (Data Share)

๓.๑๒ แนวทางปฏิบัติในการเข้าถึงพื้นที่หวงห้าม

๓.๑๓ แนวทางปฏิบัติเมื่อพบว่า Website หน่วยงานถูกโจมตี

๓.๑๔ แนวทางปฏิบัติเมื่อเชื่อมต่อเครือข่ายนอกสถานที่

๓.๑๕ แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ข้อ ๕. ต้องจัดให้มีการทบทวนและปรับปรุงแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครนนทบุรี เป็นประจำและสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖. ต้องมีการสร้างความรู้ความเข้าใจกับผู้ใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครนนทบุรี เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่อาจเกิดการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ ด้วยวิธีการดังต่อไปนี้

(๑) เผยแพร่สารสนเทศ แนวทางการใช้งานเทคโนโลยีสารสนเทศ และการสื่อสารผ่านเว็บไซต์ (Website) เฟซบุ๊ก (Facebook) สื่อสังคมออนไลน์ (Social Media) และช่องทางการสื่อสารอื่นๆ ของเทศบาลนครนนทบุรี โดยให้ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) ให้ความรู้ เพื่อสร้างความเข้าใจแก่ผู้ใช้งาน ในสาระสำคัญที่เกี่ยวข้องกับการใช้ข้อมูล สารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ รวมทั้ง การใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของเทศบาลนครนนทบุรี ให้เกิดประโยชน์สูงสุดและมีความมั่นคงปลอดภัยโดยรวม ตามรายละเอียดของการปฏิบัติตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่ได้กำหนดไว้

ข้อ ๗. การกำหนดความรับผิดชอบ

(๑) ระดับนโยบาย

๑.๑ กำหนดให้ผู้บริหารระดับสูงสุดของเทศบาลนครนนทบุรีเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบเทคโนโลยีสารสนเทศและการสื่อสารเทศบาล หรือข้อมูลสารสนเทศของเทศบาลนครนนทบุรี เกิดความเสียหาย หรือเกิดอันตรายใดๆ ต่อเทศบาลนครนนทบุรี หรือต่อหน่วยงานของเทศบาลนครนนทบุรี หรือต่อผู้หนึ่งผู้ใด อันเนื่องมาจากความจงใจบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติ ตามแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่ได้ประกาศนี้

๑.๒ กำหนดให้ผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศ ของเทศบาลนครนนทบุรีเป็นผู้รับผิดชอบ ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ คำปรึกษาแก่เจ้าหน้าที่ระดับปฏิบัติ

(๒) ระดับปฏิบัติ

๒.๑ ผู้ดูแลระบบ (Administrator) เป็นผู้รับผิดชอบ กำกับ ดูแล ควบคุม ตรวจสอบ รายงาน และให้ข้อแสนอแนะ เพื่อให้การปฏิบัติงานของผู้ใช้ (User) เป็นไปตามข้อตามข้อกำหนดในแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑ ที่ได้ประกาศใช้นี้

๒.๒ ผู้ใช้ (User) เป็นผู้รับผิดชอบการปฏิบัติงาน ให้เป็นไปตามข้อกำหนดในแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ.๒๕๖๑ ที่ได้ประกาศใช้นี้

ข้อ ๙. การกำหนดชั้นความลับของข้อมูลและสารสนเทศ ให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๖๑ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือ ข้อกำหนดอื่นที่ได้ประกาศใช้ทดแทน

ข้อ ๑๐. องค์ประกอบของแนวทางใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑ ได้กำหนดขึ้นเพื่อให้มีมาตรการและแนวทางในการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้อยู่ในระดับที่ปลอดภัย ช่วยลดความเสี่ยงต่อการดำเนินงาน ทรัพย์สิน และบุคลากร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย จึงจัดเป็นส่วนหนึ่งของมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งบุคลากรทุกหน่วยงานของเทศบาลนครนนทบุรี รวมทั้งบุคลากรของหน่วยงานภายนอกอื่นที่เกี่ยวข้อง ต้องถือปฏิบัติตามอย่างเคร่งครัด

ข้อ ๑๑. จนกว่าจะได้มีการประกาศใช้ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของเทศบาลนครนนทบุรี ที่ต้องดำเนินการและจัดทำตามกฎหมายและประกาศที่เกี่ยวข้องกับเรื่องความมั่นคงปลอดภัยและความน่าเชื่อถือด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานรัฐบาล ให้งดเว้นการถือปฏิบัติและการบังคับใช้ออกไปก่อน เฉพาะแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ดังต่อไปนี้

(๑) แนวทางปฏิบัติเรื่องบัญชีผู้ใช้งาน (User Account)

(๒) แนวทางกำหนดรหัสผ่าน (Password)

(๓) แนวทางพิสูจน์ตัวตน (Authentication)

(๔) แนวทางการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System)

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๒ ตุลาคม พ.ศ. ๒๕๖๑

(นายสมนึก ธนเดชากุล)
นายกเทศมนตรีนครนนทบุรี

แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร
เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑

๑. หลักการและเหตุผล

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารเทศบาลนครนนทบุรี พ.ศ. ๒๕๕๙-๒๕๖๓ มีวัตถุประสงค์ให้เทศบาลนครนนทบุรี สามารถใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ให้เกิดประโยชน์สูงสุดกับการทำงานประจำ เพิ่มคุณภาพการบริการประชาชนในทุกภารกิจ อีกทั้ง ยังสามารถใช้ประโยชน์จากข้อมูลข่าวสาร ด้วยการนำข้อมูลที่เป็นทรัพย์สินมาก่อประโยชน์ให้กับสังคม เช่น การเปิดเผยข้อมูลเชิงลึก ให้เกิดประโยชน์และนำไปสู่การวางรากฐานให้เทศบาลนครนนทบุรีสามารถพัฒนาให้เป็นเมืองอัจฉริยะในอนาคต

ด้วยเหตุผลทั้งหมดข้างต้น เทศบาลนครนนทบุรีจึงเห็นสมควรกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ความสำคัญในการทำความเข้าใจกับบุคลากรถึงขอบเขตการใช้งานทรัพยากรคอมพิวเตอร์ และนำไปบังคับใช้ เพื่อให้ข้อมูลและระบบเครือข่ายคอมพิวเตอร์สามารถเกิดประโยชน์สูงสุดและมีความมั่นคงปลอดภัยโดยรวม

๒. วัตถุประสงค์และขอบเขต

เทศบาลนครนนทบุรีได้กำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารให้ครอบคลุมแนวทางการใช้งานระบบคอมพิวเตอร์และเครือข่ายทั้งในการใช้งานเครื่องและอุปกรณ์คอมพิวเตอร์และในการใช้บริการสื่อสารข้อมูลในเครือข่ายโดยมีวัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อพัฒนาคุณภาพบุคลากรในด้านการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารให้มีความรู้ความเข้าใจการใช้เทคโนโลยีที่ถูกต้อง พัฒนาทักษะในการใช้งานซอฟต์แวร์ในสำนักงานอย่างต่อเนื่อง ให้สามารถใช้งานและแก้ไขปัญหาเฉพาะหน้าในการใช้งานระบบซอฟต์แวร์ตามกระบวนงานได้ โดยมีแนวทางการใช้งานข้อมูลอย่างเป็นระบบ

๒.๒ เพื่อให้บุคลากรได้รับทราบถึงหน้าที่และ ความรับผิดชอบในการใช้งานระบบคอมพิวเตอร์และเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด เพื่อเป็นการป้องกันทรัพยากรและข้อมูลของเทศบาลนครนนทบุรี ให้ปลอดภัย มีความถูกต้อง และพร้อมใช้งานอยู่เสมอ

๒.๓ เพื่อให้บุคลากรได้ตระหนักถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ทั้งในการปฏิบัติงานภายในและภายนอกสำนักงานเทศบาล ให้มีประสิทธิภาพสูงสุด รวมทั้งเสริมสร้างความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ

๒.๔ เพื่อกำหนดมาตรการควบคุม และกำหนดแนวทางการใช้บริการบนระบบเครือข่าย ได้แก่ แนวทางการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) และแนวทางควบคุมการใช้อินเทอร์เน็ต (Internet) ซึ่งผู้ใช้บริการจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการบนระบบเครือข่าย โดยจะต้องเข้าใจกฎเกณฑ์ต่างๆที่ผู้ดูแลระบบเครือข่ายกำหนด ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่

เคารพกฎเกณฑ์ที่กำหนดไว้และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัดอันจะทำให้การใช้บริการต่างๆบนระบบเครือข่ายเป็นไปอย่างปลอดภัยและในประสิทธิภาพ

๓. องค์ประกอบ

แนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี พ.ศ. ๒๕๖๑ มีองค์ประกอบดังต่อไปนี้

๓.๑ กฎหมายและระเบียบที่เกี่ยวข้อง

๓.๒ คำนิยามที่เกี่ยวข้อง

๓.๓ แนวทางปฏิบัติงานเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งที่เป็นทรัพย์สินของเทศบาลและที่เป็นทรัพย์สินส่วนบุคคล

๓.๑ แนวทางปฏิบัติเมื่อพบว่าเครื่องคอมพิวเตอร์ติดไวรัส (Virus Computer)

๓.๒ แนวทางปฏิบัติเกี่ยวกับรหัสผ่าน (Password)

๓.๓ แนวทางปฏิบัติการใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

๓.๔ แนวทางปฏิบัติการสำรองข้อมูล (Data Backup)

๓.๕ แนวทางปฏิบัติการใช้งานและค้นหาข้อมูลบนระบบเครือข่าย (Internet)

๓.๖ แนวทางปฏิบัติในการติดตั้งโปรแกรมสำเร็จรูป (Software)

๓.๗ แนวทางปฏิบัติในการนำอุปกรณ์ส่วนตัวเชื่อมต่อเครือข่ายหน่วยงาน

๓.๘ แนวทางปฏิบัติเมื่อพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติ

๓.๙ แนวทางปฏิบัติในการใช้ Handy Drive

๓.๑๐ แนวทางปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

๓.๑๑ แนวทางปฏิบัติในการแลกเปลี่ยนข้อมูลผ่านเครือข่าย (Data Share)

๓.๑๒ แนวทางปฏิบัติในการเข้าถึงพื้นที่หวงห้าม

๓.๑๓ แนวทางปฏิบัติเมื่อพบว่า Website หน่วยงานถูกโจมตี

๓.๑๔ แนวทางปฏิบัติเมื่อเชื่อมต่อเครือข่ายนอกสถานที่

๓.๑๕ แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

กฎหมายและระเบียบที่เกี่ยวข้อง

การพิจารณาดำเนินการ เพื่อกำหนดแนวทางการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร ของเทศบาลนครนนทบุรีนั้น มีตัวบทกฎหมายและระเบียบ รวมทั้งประกาศที่เกี่ยวข้อง ดังต่อไปนี้

๑. พระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗ มีสาระสำคัญในการระบุฐานความผิดและบทลงโทษสำหรับการละเมิดลิขสิทธิ์

๒. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ระบุถึงบทบาทและหน้าที่ของการเปิดเผยข้อมูลข่าวสารของทางราชการ

๓. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ กฎหมายฉบับนี้ระบุถึงการรองรับทางกฎหมายของข้อความหรือนิติกรรมสัญญาที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ รวมทั้งลายมือชื่ออิเล็กทรอนิกส์ ให้มีผลทางกฎหมายที่แน่นอนเท่ากับนิติกรรมสัญญา หรือผลผูกพันที่ตกลงหรือทำการผ่านกระดาษ

๔. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ เป็นกฎหมายที่กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ ภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน เพื่อสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์

๕. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นกฎหมายที่กำหนดฐานความผิดและบทลงโทษ สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรืออาชญากรรมทางคอมพิวเตอร์

๖. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑ ฉบับแก้ไขเพิ่มเติมที่มีประเด็นสำคัญว่าด้วยเรื่องของลายมือชื่ออิเล็กทรอนิกส์

๗. ระเบียบเทศบาลนครนนทบุรี ว่าด้วยข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๕๒ ออกตามความในมาตรา ๙ แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการพ.ศ. ๒๕๔๐ เป็นระเบียบเพื่อให้การบริการข้อมูลข่าวสารของราชการที่อยู่ในความรับผิดชอบของเทศบาลนครนนทบุรี เป็นไปด้วยความเรียบร้อย รวดเร็ว และสอดคล้องกับเจตนารมณ์ของกฎหมาย ในการรับรองสิทธิของประชาชน ในการรับรู้ข้อมูลข่าวสารที่อยู่ในความครอบครองของหน่วยงานของรัฐ

๘. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๓๓ เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จัดทำประกาศขึ้น เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๙. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกตามความในมาตรา ๑๒/๑ วรรคสอง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒)

พ.ศ. ๒๕๕๑ ที่กำหนดให้การจัดทำหรือแปลงเอกสารและข้อความ ให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ให้เป็นไปตามหลักเกณฑ์และวิธีการตามประกาศนี้

๑๐. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ เป็นกฎหมายที่กำหนดหลักเกณฑ์และวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ ให้มีมาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมีการบริหารจัดการการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีการยอมรับและเชื่อมั่นในข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น รวมทั้งให้สอดรับกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ มาตรา ๒๕ ที่บัญญัติให้ธุรกรรมทางอิเล็กทรอนิกส์ใดที่กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาแล้ว ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

๑๑. ระเบียบเทศบาลนครนนทบุรี ว่าด้วยการใช้งานระบบคอมพิวเตอร์ พ.ศ. ๒๕๕๔ เป็นระเบียบที่เทศบาลนครนนทบุรีจัดทำขึ้น เพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างเหมาะสม และมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง

๑๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ อาศัยอำนาจตามความในมาตรา ๖ วรรคหนึ่ง แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๓๓ ออกประกาศเพื่อกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัยไว้

๑๓. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ เป็นประกาศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ที่กำหนดให้คณะกรรมการประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใด ที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนด เป็นวิธีการที่เชื่อถือได้

๑๔. พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ ๑๗) พ.ศ. ๒๕๕๙ เป็นกฎหมายว่าด้วยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑๕. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ สาระสำคัญของพระราชบัญญัติฉบับนี้ มีอาทิ

๑๕.๑ เพิ่มเติมความผิดของการส่งสแปมเมล์ (spam mail)

๑๕.๒ แก้ไขให้ไม่สามารถนำไปฟ้องฐานหมิ่นประมาทตามประมวลกฎหมายอาญาได้

๑๕.๓ แก้ไขให้ยกเว้นความผิดสำหรับผู้ให้บริการได้หากยอมลบข้อมูลที่ผิดกฎหมาย

๑๕.๔ เพิ่มเติมให้ผู้ใดที่มีข้อมูลซึ่งศาลสั่งให้ทำลายอยู่ในครอบครองจะต้องทำลายไม่เช่นนั้นจะได้รับโทษด้วย

๑๕.๕ เพิ่มเติมให้มีคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ขึ้นมาพิจารณาว่าข้อมูลคอมพิวเตอร์ใดที่จะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน สามารถส่งฟ้องศาลเพื่อระงับหรือลบข้อมูลดังกล่าวได้

แต่อย่างไรก็ตาม เนื้อหาหลายมาตราในพระราชบัญญัติฉบับนี้ จะต้องให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ออกกฎกระทรวงหรือประกาศ เพื่อกำหนดรายละเอียดการใช้บังคับต่อไป

คำนิยามที่เกี่ยวข้อง

๑. เทศบาล หมายถึง เทศบาลนครนนทบุรี
๒. หน่วยงาน หมายถึง สำนัก ศูนย์ กอง ส่วนฝ่าย หน่วย และงาน ที่อยู่ในสังกัดเทศบาลนครนนทบุรี
๓. หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอก ที่เทศบาลอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
๔. นายกเทศมนตรี หมายถึง นายกเทศมนตรีนครนนทบุรี
๕. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของเทศบาลนครนนทบุรี
๖. ผู้บริหาร หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ปลัดเทศบาล หัวหน้ากองหรือเทียบเท่าผู้อำนวยการสำนัก/กอง หัวหน้าฝ่าย เป็นต้น
๗. ผู้บริหารระดับสูง หมายถึง ปลัดเทศบาลหรือเทียบเท่า
๘. ผู้ดูแลระบบ (System Administrator) และ/หรือ ผู้ดูแลระบบคอมพิวเตอร์ (Computer System Admistrator) หมายถึงผู้ที่ได้รับมอบหมายจากเทศบาล ให้มีหน้าที่รับผิดชอบดูแลบำรุงรักษา และบริหารจัดการ ระคอมพิวเตอร์และระบบเครือข่าย ไม่ว่าส่วนหนึ่งส่วนใด รวมถึงผู้รับจ้างดูแลและซ่อมบำรุงระบบคอมพิวเตอร์และเครือข่าย ที่ปฏิบัติงานตามสัญญาจ้างที่ได้ทำไว้กับเทศบาลนครนนทบุรี
๙. ผู้ใช้ และ/หรือ ผู้ใช้งาน (User) หมายถึง คณะผู้บริหารสมาชิกสภาเทศบาล ข้าราชการ ลูกจ้าง พนักงานราชการ พนักงานเทศบาล พนักงานจ้าง ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน รวมทั้ง บุคคลอื่นที่เทศบาลมอบหมายให้ปฏิบัติงาน และให้หมายความรวมถึงบุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของเทศบาล โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งได้กำหนดไว้
๑๐. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงาน ให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น
๑๑. เจ้าของบัญชีผู้ใช้บริการ หมายถึงบัญชีผู้ใช้ (User Account) ที่อนุญาตให้เจ้าของบัญชีผู้ใช้นั้นๆ มีสิทธิ์ในการใช้บริการต่างๆโดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ยืนยันตัวบุคคลในการเข้าใช้งาน
๑๒. ผู้ทำหน้าที่ตรวจสอบ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บริหาร เพื่อทำการตรวจสอบความมั่นคงปลอดภัยของระบบสารสนเทศ
๑๓. เจ้าหน้าที่ที่ได้รับมอบหมายให้ตรวจสอบสินทรัพย์ หมายถึงผู้ที่ได้รับการมอบหมายจากผู้บริหาร ทำการตรวจสอบสินทรัพย์ในความครอบครองของเทศบาลนครนนทบุรี
๑๔. เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้รับผิดชอบในการจัดการดูแลระบบสาระสนเทศให้มีความมั่นคงปลอดภัย
๑๕. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์
๑๖. สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก(Notebook Computer) อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย เช่น

โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๑๗. สินทรัพย์ส่วนบุคคล หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เป็นสมบัติส่วนตัวของผู้ใช้งาน เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และเครื่องคอมพิวเตอร์ขนาดสมุดบันทึก (Notebook Computer) อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่าย เช่น โทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ (Smartphone) ฮาร์ดแวร์และซอฟต์แวร์ รวมถึง ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๑๘. ข้อมูล (Data) และ/หรือ ข้อมูลคอมพิวเตอร์ (Computer Data) หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเลคทรอนิกส์ด้วย

๑๙. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ ในการบริหารจัดการ การวางแผน การตัดสินใจ และอื่นๆ

๒๐. รหัสผ่าน (Password) หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูล ในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

๒๑. เครื่องคอมพิวเตอร์ หมายถึง ครุภัณฑ์คอมพิวเตอร์ ทั้งที่เป็นคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) และคอมพิวเตอร์โน้ตบุค (Notebook Computer) ของที่อยู่ในบัญชีครุภัณฑ์ และไม่อยู่ในบัญชีครุภัณฑ์ของเทศบาล แต่นำมาใช้เพื่องานราชการ

๒๒. ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๒๓. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง แนวทางปฏิบัติงาน หรือสิ่งอื่นใดให้อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมต่อกันนั้น ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๒๔. ระบบแลน(LAN) และ/หรือ ระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๒๕. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของหน่วยงาน หรือระหว่างหน่วยงานกับหน่วยงานภายนอกได้ เช่น ระบบเครือข่ายท้องถิ่นแบบมีสาย(Cabling LAN) ระบบเครือข่ายแบบไร้สาย(Wireless LAN หรือ WLAN) ระบบอินทราเน็ต(Intranet) ระบบอินเทอร์เน็ต(Internet) เป็นต้น

๒๖. จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง รูปที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่รับส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP,POP๓ และ IMAP เป็นต้น

๒๗. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศ

ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารจัดการ การสนับสนุนการให้บริการ การพัฒนาและการควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศเป็นต้น

๒๘. ความมั่นคงปลอดภัย (Security) หมายถึง สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

๒๙. ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึงการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน(Integrity) และสภาพพร้อมใช้งาน(Availability)ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง(authenticity) การตรวจสอบได้(accoutability)การห้ามปฏิเสธความรับผิด(non-repudiation)และความน่าเชื่อถือ(reliability)

๓๐. ความเสี่ยง (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ด้านสารสนเทศ อาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จ

๓๑. มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๓๒. ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๓๓. แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๓๔. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศโดยแบ่งเป็น

๓๔.๑. พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ที่ประจำโต๊ะทำงานและพื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)

๓๔.๒. พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) หมายถึง พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานระบบเครือข่ายทั้งหมด ไม่ว่าจะเป็นพื้นที่ใช้งานระบบเครือข่ายท้องถิ่นแบบนี้สาย (Cabling LAN coverage area) หรือพื้นที่ใช้งานระบบเครือข่ายท้องถิ่นแบบไร้สาย (Wireless LAN coverage area)

๓๕. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ(Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง การใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๓๖. ประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศรวมทั้งผลกระทบจากการสูญเสียสารสนเทศ หรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

๓๗. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) หมายถึง การเกิดเหตุการณ์สภาพของบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓๘. แผนการเตรียมพร้อม กรณีฉุกเฉิน หมายถึง แผนแก้ไขปัญหาจากการเกิดการความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศหรือมีการซักซ้อมการดำเนินการตาม

๓๙. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) อาจทำให้ระบบขององค์กรถูกบุกรุกหรือถูกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๔๐. ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมเกิดการขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

แนวทางปฏิบัติงานเทคโนโลยีสารสนเทศและการสื่อสาร เทศบาลนครนนทบุรี

แนวทางปฏิบัติเมื่อพบว่าเครื่องคอมพิวเตอร์ติดไวรัส

วัตถุประสงค์

เพื่อให้ผู้ใช้งานสามารถดำเนินการด้านการป้องกันตนเองจากไวรัสคอมพิวเตอร์และสามารถจัดการกับปัญหาไวรัสคอมพิวเตอร์เบื้องต้นได้อย่างมีประสิทธิภาพ ทำให้ไม่เกิดความเสียหายแก่ข้อมูลของผู้ใช้ และหน่วยงานที่ใช้เครือข่ายร่วมกัน

แนวปฏิบัติ

๑. หากเครื่องคอมพิวเตอร์ยังคงทำงานได้ ให้ทำการ สำรองข้อมูล ไว้ในอุปกรณ์ภายนอกเครื่อง เช่น Handy drive หรือ Hard disk External เป็นต้น และนำส่งให้เจ้าหน้าที่สารสนเทศทำการสแกนก่อนนำข้อมูลกลับมาใช้

๒. ทำการอัพเดต Anti-Virus แล้วทำการสแกนหาไวรัส

๓. หากดำเนินการแล้วพบว่าเครื่องคอมพิวเตอร์ยังติดไวรัสอยู่ ให้ติดต่อเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ เพื่อทำการติดตั้ง Remove tool

๔. ในกรณีที่ไม่สามารถแก้ไขได้ และยังสงสัยว่าไวรัสยังคงอยู่ ให้ทำการฟอร์แมตเครื่องและติดตั้งระบบปฏิบัติการใหม่ทั้งหมด และนำข้อมูลที่ได้สำรองไว้กลับมาติดตั้งยังเครื่องคอมพิวเตอร์ต่อไป

๕. เปลี่ยนพาสเวิร์ดในการล็อกอินระบบต่าง ๆ ภายหลังการ ติดตั้งระบบปฏิบัติการใหม่

หมายเหตุ

๑. ผู้ใช้ควรติดตั้งโปรแกรมป้องกันไวรัส และทำการ Update อย่างสม่ำเสมอ

๒. ไม่ควรติดตั้งซอฟแวร์ที่มาจากเว็บไซต์ที่ไม่น่าเชื่อถือ

แนวทางปฏิบัติเกี่ยวกับ Password

วัตถุประสงค์

เพื่อกำหนดมาตรการในการตั้ง Password ที่มีความปลอดภัยสูงและได้มาตรฐาน รวมไปถึงระยะเวลาที่เหมาะสมในการเปลี่ยน Password อยู่เสมอ เพื่อป้องกันการโจมตีด้วยวิธี brute force

แนวปฏิบัติ

๑. ไม่ใช้พาสเวิร์ดเดียวกันในทุกระบบที่ผู้ใช้มีสิทธิเข้าใช้

๒. มีความยาว ๘-๑๒ ตัวอักษร

๓. ผสมผสานทั้งตัวเลข เครื่องหมายพิเศษ ตัวอักษรใหญ่ และตัวอักษรเล็ก

๔. อาจใช้เทคนิค การพิมพ์พาสเวิร์ดภาษาอังกฤษด้วยคีย์บอร์ดภาษาไทย

๕. ไม่ใช้คำทั่วไป และคำที่มีความหมายเกี่ยวข้องกับผู้ใช้งานในการตั้งพาสเวิร์ด

๖. เปลี่ยนรหัสผ่านทุก ๆ ๖ เดือน

๗. ออกจากระบบทุกครั้งหลังใช้งาน

๘. ไม่ควรเลือกใช้งาน "จำรหัสผ่าน" บทเว็บไซต์หรือระบบงานต่าง ๆ

๙. ไม่ควรจดรหัสผ่านลงกระดาษที่ไม่มีการป้องกันการเข้าถึง

๑๐. ไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบ

๑๑. เมื่อจำเป็นต้องทำธุรกรรมออนไลน์ผ่านคอมพิวเตอร์สาธารณะ ให้เปลี่ยนรหัสผ่านทันทีที่มีโอกาส

๑๒. ไม่เขียนรหัสผ่านไว้บนกระดาษและแปะไว้ตามที่ต่างๆเพื่อเตือนความจำ

หมายเหตุ

ตัวอย่างของรหัสผ่านที่มีความปลอดภัยสูง “ED๙ts๓๗๗!”, “t!๒!m!o!h!i!t!o!๐๒๙๒”,”๒S๐๐N๒btrue!!”

แนวทางปฏิบัติ การใช้ E-mail

วัตถุประสงค์

เพื่อเป็นแนวทางในการใช้ระบบ E-Mail ที่ถูกต้องปลอดภัย ลดความเสียหายจากการใช้งาน E-mail ที่ไม่ปลอดภัยและมีความเสี่ยงต่อเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

แนวปฏิบัติ

๑. ผู้ใช้งานที่ต้องการใช้งาน E-Mail ของหน่วยงานต้องทำการกรอกข้อมูลคำขอเข้าใช้งาน และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Password)

๒. เมื่อได้รับรหัสผ่าน (Password) จะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันทีหลังจากการเข้าสู่ ระบบเป็นครั้งแรก

๓. ควรกำหนดรหัสผ่านที่ยากต่อการคาดเดา ให้มีตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิพม์ปกติตัวเลข และสัญลักษณ์เข้าด้วยกัน

๔. ผู้ใช้งานควรเปลี่ยนรหัสผ่านทุกๆ ๖ เดือน

๕. ต้องใช้ E-Mail ของหน่วยงานเพื่อติดต่องานของราชการเท่านั้น

๖. ไม่ควรใช้ E-Mail Address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอม จากเจ้าของ E-Mail และให้ถือว่าเจ้าของ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ใน E-Mail ของตน

๗. หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

๘. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๙. ควรตรวจสอบและลบ E-Mail ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบ E-Mail ให้เหลือจำนวนน้อยที่สุด

๑๐. ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๑๑. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

๑๒. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๑๓. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิ์ของบุคคลอื่น

๑๔. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๑๕. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๑๖. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๗. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทาง จดหมายอิเล็กทรอนิกส์

หมายเหตุ ระบบE-mail ที่ควรใช้ในการติดต่องานราชการควรเป็น ระบบ E-mail กลางภาครัฐ (Mail.go.th)

แนวทางปฏิบัติการสำรองข้อมูล

วัตถุประสงค์

เพื่อกำหนดมาตรการในการสำรองข้อมูลของผู้ใช้งาน ทำให้ลดความเสี่ยงในการสูญเสียข้อมูลที่มีความสำคัญในการทำงาน ส่งผลให้ผู้ใช้งานสามารถทำงานได้อย่างต่อเนื่อง

แนวปฏิบัติ

๑.ทำการสำรวจข้อมูลและจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล ตามตัวอย่างแบบฟอร์มดังนี้

ลำดับ	รายการ	ระดับความสำคัญ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรอง	ระยะเวลาในการสำรองข้อมูล	ระยะเวลาในการกู้คืนข้อมูล
๑	เอกสาร	สูง	File เอกสาร		๑เดือน	๑ ชม.
๒	ข้อมูลเผยแพร่บนเว็บไซต์	สูงมาก	File ข้อมูลชนิดต่าง ๆ	ก่อนและหลังการเปลี่ยนแปลง	๑เดือน	๒ ชม.

๒. ทำการสำรองข้อมูลด้วย Harddisk External หรือระบบ Cloud

๓. ควรสำรองข้อมูลไว้มากกว่า ๑ ชุด พร้อมจัดทำเอกสารวิธีการกู้คืน

๔. หากข้อมูลมีความสำคัญสูงมาก ควรใช้ Bitlocker ในการเข้ารหัสลับข้อมูล

๕. ข้อมูลที่มีความลับ และมีความสำคัญสูงไม่ควรสำรองไว้บนระบบ Cloud

๖. ตรวจสอบความถูกต้องของข้อมูลที่ทำการสำรองและทดสอบการกู้คืนเป็นระยะ

๗. ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีการกู้คืนระบบต่างๆไว้นอกสถานที่

๘. การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

๙. ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน recycle bin

๑๐. ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

แนวทางปฏิบัติการใช้งานและค้นหาข้อมูลจาก internet

วัตถุประสงค์

เพื่อกำหนดวิธีการใช้งาน internet และการค้นหาข้อมูลจาก internet ที่ทำให้ไม่เกิดความเสียหายและส่งผลกระทบต่อระบบเครือข่ายของหน่วยงาน

แนวปฏิบัติ

๑. ด้านการติดต่อสื่อสารกับเครือข่าย ประกอบด้วย

๑.๑ ในการเชื่อมต่อเข้าสู่เครือข่ายควรใช้ชื่อบัญชี (Internet Account Name) และรหัสผ่าน (Password) ของตนเอง ไม่ควรนำของผู้อื่นมาใช้ รวมทั้งนำไปกรอกแบบฟอร์มต่างๆ

๑.๒ ควรเก็บรักษารหัสผ่านของตนเองเป็นความลับ และทำการเปลี่ยนรหัสผ่านเป็นระยะๆ รวมทั้งไม่ควรแอบดูหรือถอดรหัสผ่านของผู้อื่น

๑.๓ ควรวางแผนการใช้งานล่วงหน้าก่อนการเชื่อมต่อกับเครือข่ายเพื่อเป็นการประหยัดเวลา

๑.๔ เลือกถ่ายโอนเฉพาะข้อมูลและโปรแกรมต่างๆ เท่าที่จำเป็นต่อการใช้งานจริง

๒. ด้านการใช้ข้อมูลบนเครือข่าย ประกอบด้วย

๒.๑ เลือกใช้ข้อมูลที่มีความน่าเชื่อถือ มีแหล่งที่มาของผู้เผยแพร่ และที่ติดต่อ

๒.๒ เมื่อนำข้อมูลจากเครือข่ายมาใช้ ควรอ้างอิงแหล่งที่มาของข้อมูลนั้น และไม่ควรแอบอ้างผลงานของผู้อื่นมาเป็นของตนเอง

๒.๓ ไม่ควรนำข้อมูลที่เป็นเรื่องส่วนตัวของผู้อื่นไปเผยแพร่ก่อนได้รับอนุญาต

๓.ด้านการติดต่อสื่อสารระหว่างผู้ใช้ ประกอบด้วย

๓.๑ ใช้ภาษาที่สุภาพในการติดต่อสื่อสาร และใช้คำให้ถูกความหมาย เขียนถูกต้องตามหลักไวยากรณ์

๓.๒ ใช้ข้อความที่สั้น กะทัดรัดเข้าใจง่าย

๓.๓ ไม่ควรนำความลับ หรือเรื่องส่วนตัวของผู้อื่นมาเป็นหัวข้อในการสนทนา รวมทั้งไม่ใส่ร้ายหรือทำให้บุคคลอื่นเสียหาย

๓.๔ หลีกเลี่ยงการใช้ภาษาที่ดูถูก เหยียดหยามศาสนา วัฒนธรรมและความเชื่อของผู้อื่น

๓.๕ ในการติดต่อสื่อสารกับผู้อื่นควรสอบถามความสมัครใจของผู้ที่ติดต่อด้วย ก่อนที่จะส่งแฟ้มข้อมูล หรือโปรแกรมที่มีขนาดใหญ่ไปยังผู้ที่เราติดต่อด้วย

๔. ด้านระยะเวลาในการใช้บริการ ประกอบด้วย

๔.๑ ควรคำนึงถึงระยะเวลาในการติดต่อกับเครือข่าย เพื่อเปิดโอกาสให้ผู้ใช้คนอื่นๆ บ้าง

๔.๒ ควรติดต่อกับเครือข่ายเฉพาะช่วงเวลาที่ต้องการใช้งานจริงเท่านั้น

๔.๓ พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ไม่ Download/ Upload ข้อมูลหรือสิ่งอื่นใดที่ไม่เกี่ยวข้องกับงาน หรือใช้ Website ที่ไม่เกี่ยวข้องกับงาน

๕. ด้านความปลอดภัย

๕.๑ ไม่ควรเปิดเผยข้อมูลส่วนตัว

๕.๒ ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น เช่น สำเนาบัตรประชาชน เอกสารต่างๆ รวมถึงรหัสบัตรต่างๆ เช่น เอทีเอ็ม บัตรเครดิต ฯลฯ

๕.๓ ไม่ควรโอนเงินให้ใครอย่างเด็ดขาด นอกจากจะเป็นญาติสนิทที่เชื่อใจได้จริงๆ

๕.๔ ไม่ควรบันทึกยูสเซอร์เนมและพาสเวิร์ดขณะใช้เครื่องคอมพิวเตอร์สาธารณะ

๕.๕ ไม่ควรบันทึกภาพวิดีโอ หรือเสียงที่ไมเหมาะสมบนคอมพิวเตอร์ หรือบนมือถือ

๕.๖ ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

แนวทางปฏิบัติในการติดตั้งโปรแกรมสำเร็จรูป

วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรการในการติดตั้งโปรแกรมสำเร็จรูปที่ถูกต้องและเหมาะสม เพื่อลดการละเมิดลิขสิทธิ์และลดความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศอันเกิดจากโปรแกรมไม่พึงประสงค์เช่น ไวรัสคอมพิวเตอร์ Ransom ware เป็นต้น

แนวปฏิบัติ

๑. ควรติดตั้งโปรแกรมสำเร็จรูปที่มีลิขสิทธิ์

๒. ไม่ควรติดตั้งโปรแกรมเกินความจำเป็น

๓. ไม่ควรติดตั้งโปรแกรมที่โหลดจาก internet ที่ไม่น่าเชื่อถือ

๔. ควรอ่านข้อจำกัด สิทธิ์ ระหว่างการติดตั้งโปรแกรมอย่างถี่ถ้วน

๕. การติดตั้งโปรแกรมสำเร็จรูปควรได้รับคำแนะนำจากผู้ดูแลระบบสารสนเทศของหน่วยงานก่อน

แนวทางปฏิบัติในการนำอุปกรณ์ส่วนตัวเชื่อมต่อเครือข่ายหน่วยงาน

วัตถุประสงค์

เพื่อเป็นการกำหนดแนวทางที่เหมาะสมในการใช้อุปกรณ์ส่วนตัวเชื่อมต่อระบบเครือข่ายของหน่วยงานเป็นไปตามนโยบายความมั่นคงปลอดภัยด้านเครือข่าย

แนวปฏิบัติ

๑. ติดต่อผู้ดูแลระบบเครือข่ายของหน่วยงานเพื่อขออนุญาตเข้าใช้เครือข่าย พร้อมทั้งให้ข้อมูลการยืนยันตัวตนแก่ผู้ดูแลระบบ

๒. ห้ามพนักงานใช้ระบบเครือข่ายและคอมพิวเตอร์ เพื่อการดังต่อไปนี้

๒.๑ การกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๒.๒ การกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๒.๓ การค้าหรือการแสวงหาผลกำไร หรือผลประโยชน์ส่วนตัว

๒.๔ การเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน

๒.๕ การกระทำเพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

๒.๖ การรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหาย

๒.๗ การขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์หรือทำให้เครือข่ายคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ

๒.๘ แสดงความเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของหน่วยงานไปยังที่อยู่เว็บไซต์(Website) ใดๆ ในลักษณะที่จะก่อให้เกิดหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง หรือก่อให้เกิดความเสียหายแก่บุคคลอื่น

แนวทางปฏิบัติเมื่อพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติ

วัตถุประสงค์

เพื่อเป็นมาตรการการแก้ไขปัญหาที่เกิดขึ้นกับเครื่องคอมพิวเตอร์เบื้องต้น ทำให้เพิ่มประสิทธิภาพในการทำงาน ลดความเสี่ยงในความเสียหายต่อข้อมูลและทรัพย์สินสารสนเทศ

แนวปฏิบัติ

๑. ผู้ใช้ควรเก็บข้อมูล และรายละเอียดอาการของเครื่องคอมพิวเตอร์ที่ทำงานผิดปกติ

๒. หากเปิดเครื่องไม่ติด ให้ตรวจดูสายไฟ และเครื่องสำรองไฟฟ้า ว่าอยู่ในสถานะพร้อมใช้งาน

๓. ถอนการติดตั้งโปรแกรม และลบ file ที่ไม่จำเป็น

๔. ทำการสำรองข้อมูลทันที

๕. ทำการสแกนไวรัส

๖. ติดต่อเจ้าหน้าที่สารสนเทศเพื่อทำการตรวจสอบและแก้ไข

๗. หากอุปกรณ์คอมพิวเตอร์เสียหายให้ดำเนินการจัดจ้างซ่อมตามระเบียบราชการต่อไป

แนวทางปฏิบัติในการใช้ Handy drive

วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งาน Handy drive ที่ถูกต้อง ทำให้ลดการแพร่กระจายของไวรัสคอมพิวเตอร์เข้าสู่เครื่องคอมพิวเตอร์และระบบเครือข่าย

แนวปฏิบัติ

๑. ปิด Auto Run (ติดต่อเจ้าหน้าที่ด้านสารสนเทศเพื่อดำเนินการ)

๒. ทำการสแกนไวรัส ด้วยโปรแกรม Anti-virus ที่ติดตั้งภายในเครื่อง

๓. ก่อนถอดออกจากเครื่องคอมพิวเตอร์ต้องสั่ง Eject Handy drive ทุกครั้ง

๔. เมื่อมีความจำเป็นต้องใช้ Handy drive กับเครื่องคอมพิวเตอร์ผู้อื่น หลังจากการใช้งานต้องทำการสแกนไวรัสทุกครั้ง

๕. ไม่ใช้ Handy drive เป็นอุปกรณ์สำรองข้อมูลหลัก

๖. หากพบว่า Handy drive ติดไวรัสคอมพิวเตอร์ ให้ทำการ Format ทันที

๗. หาก Handy drive เกิดความเสียหาย ควรทำลายด้วยการเผา หรือบดทำลาย

แนวทางปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

วัตถุประสงค์

เพื่อกำหนดการใช้งานคอมพิวเตอร์ร่วมกันอย่างถูกต้อง และเหมาะสม ในกรณีที่หน่วยงานมีทรัพยากรด้านสารสนเทศจำกัด ทำให้เกิดการใช้งานอย่างคุ้มค่าและทำงานได้อย่างต่อเนื่อง

แนวปฏิบัติ

๑. กำหนด Username และ Password แยกจากกันตามจำนวนผู้เข้าใช้เครื่องคอมพิวเตอร์

๒. เพิ่มความถี่ในการสำรองข้อมูล

๓. ต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์

๔. เคร่งครัดการติดตั้งโปรแกรมสำเร็จรูปที่เหมาะสม

๕. หากมีการใช้ระบบเครือข่าย Internet ต้องแจ้งผู้ดูแลระบบในการมอบสิทธิ์การเข้าใช้เครือข่ายแยกจากกัน

๖. หากพบความผิดปกติบนเครื่องคอมพิวเตอร์ ผู้ใช้ทำการสำรองข้อมูลของตัวเองก่อน จากนั้นแจ้งผู้ใช้คนอื่นในการสำรองข้อมูลของแต่ละคน หลังจากนั้นให้ติดต่อเจ้าหน้าที่ด้านสารสนเทศทำการแก้ไขต่อไป

แนวทางปฏิบัติในการแลกเปลี่ยนข้อมูลผ่านเครือข่าย

วัตถุประสงค์

เพื่อเป็นแนวทางมาตรฐานในการแลกเปลี่ยนข้อมูลที่ตรงตามแนวนโยบายความมั่นคงปลอดภัย โดยการแลกเปลี่ยนข้อมูลผ่านเครือข่ายมีความจำเป็นต้องมีความปลอดภัยสูงสุด

แนวปฏิบัติ

๑. ผู้ใช้ต้องติดต่อผู้ดูแลระบบในการกำหนดการใช้งาน

๒. การแลกเปลี่ยนข้อมูลผ่านเครือข่ายควรมีระบบการเข้ารหัส

๓. เครื่องคอมพิวเตอร์ทั้งรับ-ส่งข้อมูลที่ใช้ในการแลกเปลี่ยนต้องติดตั้งโปรแกรม Anti-virus

๔. มีการจำกัดสิทธิ์ในการเข้าใช้ระบบแลกเปลี่ยน

๕. ระบบการแลกเปลี่ยนควรเป็นระบบภายในองค์กรเท่านั้น (intranet)

๖. การอนุญาตให้ผู้ใช้ ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น

แนวทางปฏิบัติในการเข้าถึงพื้นที่หวงห้าม

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก

แนวปฏิบัติ

๑. ภายในองค์กร ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม กรรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒. ผู้รับผิดชอบด้านสารสนเทศต้องกำหนดสิทธิ์ ผู้ใช้ ที่มีสิทธิ์ผ่านเข้าออกและช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๓. การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ

๔. กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร ผู้ดูแลระบบจะต้องลงบันทึกในแบบฟอร์มการเข้าออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง

๕. เจ้าหน้าที่ ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่อเพื่อขออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกได้ถูกต้อง

๖. บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และ รปภ. ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

๗. ผู้ใช้ จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๘. ผู้ดูแลระบบจะต้องควบคุมการทำงานของผู้ใช้ภายในพื้นที่หวงห้ามอย่างเข้มงวด และหากมีการสำเนาข้อมูลออกนอกพื้นที่จะต้องได้รับอนุญาตจากเจ้าของระบบเป็นลายลักอักษร

แนวทางปฏิบัติเมื่อพบว่า Website หน่วยงานถูกโจมตี

วัตถุประสงค์

เพื่อเป็นมาตรการการปฏิบัติงานของผู้ดูแลระบบในการดำเนินการแก้ไข และดำเนินการจัดการกับเว็บไซต์ของหน่วยงานเมื่อถูกโจมตีจากผู้ไม่หวังดีทั้งภายในและภายนอก

แนวปฏิบัติ

๑. ผู้ดูแลระบบควรปิดกันการเข้าถึงเว็บไซต์ที่ถูกโจมตีทันที

๒. ผู้ดูแลระบบควรตรวจสอบ LOG จากระบบการรักษาความมั่นคงปลอดภัยเช่น Firewall หรือ IPS เป็นต้น เพื่อยืนยันช่องทางการเข้าโจมตีและประเมินสถานการณ์ ผลกระทบที่อาจเกิดขึ้น

๓. ผู้ดูแลระบบควรทำการแก้ไขช่องโหว่ที่พบในทันที และทำการเปิดบริการ Website หลังจากได้รับการแก้ไขช่องโหว่ที่พบแล้วเท่านั้น

๔. ทำการตรวจสอบข้อมูล ความเสียหาย หากพบว่าไม่สามารถแก้ไขได้ ผู้ดูแลระบบควรทำการ กู้คืนระบบจากระบบสำรองข้อมูล

๕. หากเป็นระบบที่พัฒนาจากหน่วยงานภายนอกผู้ดูแลระบบต้องแจ้งเจ้าของระบบงานดังกล่าวเพื่อดำเนินการแก้ไข ปิดช่องโหว่ที่พบก่อนเปิดให้บริการ

๖. เจ้าของระบบควร Update ระบบปฏิบัติการ และติดตั้ง antivirus ที่เครื่อง Web server

แนวทางปฏิบัติเมื่อเชื่อมต่อเครือข่ายนอกสถานที่

วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรการการเชื่อมต่อเครือข่ายจากภายนอกสถานที่เข้ามายังหน่วยงาน ซึ่งการใช้บริการจากหน่วยภายนอกอาจก่อให้เกิดความเสี่ยงได้เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

แนวทางปฏิบัติ

๑. บุคคลที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายองค์กรจากภายนอกสถานที่จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน

๒. จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอก ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

๒.๑ เหตุผลในการขอใช้

๒.๒ ระยะเวลาในการใช้

๒.๓ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๒.๔ การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๒.๕ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓. หน่วยงานภายนอก ที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๔. เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๕. สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๖. ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจว่า สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๗. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวปฏิบัติ

๑. ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี อย่างเป็นลายลักษณ์อักษร

๒. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓. ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔. ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๕. ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

๖. ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๗. ผู้ดูแลระบบ ควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๘. ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

๙. ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๑๐. ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๑๑. ผู้ดูแลระบบ ควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย