



ประกาศเทศบาลนครนนทบุรี
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลนครนนทบุรี

ด้วยเทศบาลนครนนทบุรี ได้จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลนครนนทบุรี เพื่อให้ระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของเทศบาลนครนนทบุรี มีความมั่นคงปลอดภัย สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ สอดคล้องตามหลักมาตรฐานสากล และเป็นการปฏิบัติตามกฎระเบียบอื่น ๆ ที่เกี่ยวข้อง รวมทั้ง เพื่อให้เกิดมาตรการในการป้องกันปัญหา อันอาจเกิดขึ้นจากการถูกภาวะคุกคามต่าง ๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อความเสียหายแก่เทศบาลนครนนทบุรี และหน่วยงานในสังกัด อีกทั้ง เพื่อเป็นการป้องกันการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และฉบับที่ ๒ พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑ ธันวาคม พ.ศ. ๒๕๖๘

(นายสมนึก ธนเดชากุล)
นายกเทศมนตรีนครนนทบุรี



แนวปฏิบัติในการ

รักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ของเทศบาลนครนนทบุรี



เทศบาลนครนนทบุรี

งานสารสนเทศ ฝ่ายบริการและเผยแพร่วิชาการ กองยุทธศาสตร์และงบประมาณ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของเทศบาลนครนนทบุรี ประกอบด้วยแนวทางปฏิบัติในด้านต่าง ๆ ดังนี้

๑. แนวทางปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๑ กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารตามที่ได้รับมอบหมาย โดยกำหนดสิทธิให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้บริการ และสามารถเข้าใช้ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๑.๒ บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ให้บริการผู้ดูแลให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกัน หรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาแจ้งการใช้บริการของผู้ใช้บริการดังกล่าวทันที

๑.๓ ติดตั้ง และเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับมอบหมาย และทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยเดือนละครั้ง

๑.๔ บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วงให้มีความปลอดภัย

๑.๕ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของหน่วยงาน เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้อง ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑.๖ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้ระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๑.๗ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑.๘ คืนทรัพย์สินของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้บริหารของหน่วยงาน หรือผู้ที่ได้รับมอบหมาย เพื่อการตรวจสอบการคืนทรัพย์สิน

๑.๙ แจ้งเตือนทางเอกสารให้หน่วยงานภายในทราบถึงการโจมตี วิธีป้องกันการโจมตี และวิธีแก้ไข ปัญหา เมื่อได้รับรายงานถึงภัยคุกคาม และได้รับแจ้งจากหน่วยงานภายนอก

๒. แนวทางปฏิบัติกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑ กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒.๒ จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน โดยกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน ซึ่งแบ่งเป็น



๑) พื้นที่ทำงาน หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ

๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึงพื้นที่ติดตั้งและจัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ต่อพ่วงและให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายถึง พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

๓. แนวทางปฏิบัติการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๑ ผู้ดูแลระบบจัดทำเอกสาร “ทะเบียนการเข้าออกพื้นที่” ซึ่งระบุรายละเอียดอย่างน้อย ดังนี้ ชื่อนามสกุล, ตำแหน่ง, หน่วยงาน, พื้นที่ เครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ, รายละเอียดกิจกรรม, ระยะเวลาดำเนินการ และสิทธิที่ได้รับ

๓.๒ ผู้ดูแลระบบจัดทำแบบฟอร์มการบันทึกการเข้าออกพื้นที่ใช้งานฯ และบันทึกการเข้าออกพื้นที่ใช้งานฯอย่างสม่ำเสมอ

๓.๓ ผู้ดูแลระบบตรวจสอบการบันทึกการเข้าออกพื้นที่ทุกครั้งที่มีการใช้งาน รายการอุปกรณ์ให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา รวมทั้งตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำอย่างน้อย ๑ ครั้งต่อเดือน

๓.๔ ผู้ดูแลระบบกำหนดสิทธิการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เจ้าหน้าที่ที่มีหน้าที่รับผิดชอบเฉพาะ และต้องปฏิบัติงานที่เกี่ยวข้องกับพื้นที่ใช้งานฯ เป็นประจำ

๓.๕ ผู้ดูแลระบบควรมีระบบป้องกัน และตรวจสอบการเข้าออกพื้นที่อย่างปลอดภัย เช่น การใช้ระบบชีวภาพ (Biometric) หรือ สมาร์ทการ์ด (Smartcard) เป็นต้น

๓.๖ ผู้ใช้บริการที่ต้องการเข้าใช้พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร จะต้องขออนุญาต และบันทึกการเข้าออกพื้นที่ทุกครั้ง

๓.๗ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้บริการ ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้าหน่วยงานเจ้าของพื้นที่ หรือผู้ดูแลระบบต้องตรวจสอบเหตุผล และความจำเป็นก่อนอนุญาต และจดบันทึกการเข้าออกพื้นที่ฯ ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๔. แนวทางปฏิบัติการควบคุมสินทรัพย์สารสนเทศและใช้งานระบบคอมพิวเตอร์

๔.๑ ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

๔.๒ ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลักของหน่วยงาน เพื่อป้องกันไม่ให้เกิดทรัพย์สินเกิดความเสียหายใช้งานไม่ได้หรือสูญหาย

๔.๓ ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น



๕. แนวทางปฏิบัติการบริหารจัดการระบบเครือข่าย เทศบาลนครนนทบุรี

๕.๑ ผู้ดูแลระบบจัดทำแผนผังระบบเครือข่าย ประกอบด้วยรายละเอียดเกี่ยวกับขอบเขตของเครือข่าย ภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย การแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ การกำหนดเส้นทางบนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๒ ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้บริการ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ โดยเฉพาะระบบที่ไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ

๕.๓ ผู้ดูแลระบบต้องกำหนดหรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของอุปกรณ์ระบบเครือข่าย และอุปกรณ์ต่าง ๆ และทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยเดือนละครั้ง

๕.๔ ผู้ดูแลระบบต้องป้องกันพอร์ต โดยควบคุมการเข้าถึงพอร์ตดังกล่าวทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย

๕.๕ ผู้ดูแลระบบต้องตรวจสอบการโจมตีบุกรุก การใช้งานในลักษณะที่ผิดปกติ เพื่อความมั่นคงปลอดภัยของระบบเครือข่ายอย่างสม่ำเสมอ โดยบันทึกการใช้งาน และเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่าย

๕.๖ ผู้ดูแลระบบต้องติดตั้งอุปกรณ์หรือโปรแกรมป้องกันการบุกรุก ระหว่างระบบเครือข่ายภายใน หน่วยงานกับเครือข่ายภายนอก และระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๕.๗ การติดตั้ง เคลื่อนย้าย หรือทำการใด ๆ กับอุปกรณ์ระบบเครือข่ายต่าง ๆ เช่น อุปกรณ์จัดเส้นทาง (Router), อุปกรณ์กระจายสัญญาณข้อมูล (Switch), อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก เป็นต้น ต้องได้รับอนุญาตจากผู้ดูแลระบบ

๕.๘ ผู้ดูแลระบบที่ให้บริการระบบเครือข่ายไร้สายต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบ และบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๕.๙ ผู้ดูแลระบบที่ให้บริการระบบเครือข่ายไร้สายต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๕.๑๐ ผู้ดูแลระบบของหน่วยงานที่ให้บริการระบบเครือข่ายไร้สาย ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๕.๑๑ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสมกับพื้นที่ใช้งาน และควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๕.๑๒ ผู้ดูแลระบบ ควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายากเพื่อป้องกันผู้โจมตีไม่ไม่สามารถเดาหรือเจาะรหัสได้โดยง่าย



๕.๑๓ ผู้ดูแลระบบต้องบันทึกการทำงานของระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้บริการ บันทึกการบุกรุก บันทึกการเข้าออกระบบ บันทึกการใช้งาน และข้อมูลจราจรทางคอมพิวเตอร์

๖. แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

๖.๑ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบเครือข่าย ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ให้บริการภาษาไทย และภาษาอังกฤษ ชื่อหน่วยงาน

๖.๒ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยกำหนดขั้นตอน และแบบฟอร์มการใช้งานระบบเครือข่ายไร้สาย ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ให้บริการ เหตุผลในการขอใช้ระยะเวลาในการใช้บริการ

๖.๓ ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย ที่เชื่อมต่อกับระบบคอมพิวเตอร์หรือระบบสารสนเทศที่มีการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ และควบคุมการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ให้บริการสามารถใช้เส้นทางอื่น ๆ ได้

๖.๔ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบเครือข่าย โดยกำหนดให้ผู้ให้บริการสามารถใช้บริการได้ตามภารกิจของผู้ให้บริการ และได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๖.๕ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายจากระยะไกล (Remote access) โดยกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เช่น SSL, VPN เป็นต้น และผู้ให้บริการต้องขออนุมัติจากผู้ดูแลระบบตามแบบฟอร์มที่กำหนด ซึ่งแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการใช้บริการ

๖.๖ การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ต (Port) หรือโมเด็ม (Modem) โดยไม่จำเป็น จะต้องตัดการเชื่อมต่อทันทีเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๖.๗ ผู้ใช้บริการระบบเครือข่ายเทศบาลนครนนทบุรี ต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ

๗. แนวทางปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ

๗.๑ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ให้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ให้บริการสามารถใช้บริการได้ตามภารกิจของผู้ให้บริการ และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๗.๒ ผู้ดูแลระบบต้องตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้แก่ สถาบันมาตรวิทยาแห่งชาติ กรมอุตุนิยมวิทยา กองทัพเรือ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย

๗.๓ ผู้ดูแลระบบต้องกำหนดขั้นตอนการตรวจสอบระบบคอมพิวเตอร์ และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขให้ระบบคอมพิวเตอร์สามารถใช้งานได้



๗.๔ ผู้ดูแลระบบต้องบันทึกการทำงานของระบบคอมพิวเตอร์อย่างสม่ำเสมอ เช่น บันทึกการปฏิบัติงานของผู้ใช้บริการ บันทึกการทำงานของระบบคอมพิวเตอร์ บันทึกการให้บริการ บันทึกการทำงานของโปรแกรม บันทึกข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

๗.๕ ผู้ใช้บริการที่ต้องการใช้งานพื้นที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ Web Server, ชื่อโดเมนย่อย (Sub Domain Name) ของหน่วยงาน, บริการ (Service) ต้องทำหนังสือขออนุญาตต่องานสารสนเทศ และรับผิดชอบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในส่วนที่เกี่ยวข้อง และไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบ และผู้ใช้บริการอื่น ๆ

๗.๖ ผู้ดูแลระบบต้องเปิดบริการ (Service) เท่าที่จำเป็น เช่น บริการ telnet ftp หรือ ping เป็นต้น หากบริการใดที่จำเป็นต้องเปิดบริการมีความเสี่ยงต่อความมั่นคงปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๗.๗ ผู้ดูแลระบบต้องติดตั้งและปรับปรุงค่า parameter ต่าง ๆ ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ และทดสอบโปรแกรมระบบ เกี่ยวกับการรักษาความมั่นคงปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

๗.๘ หน่วยงานภายนอกที่ทำงานให้กับเทศบาลนครนนทบุรีทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในเทศบาลนครนนทบุรี หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของเทศบาล

๘. แนวทางปฏิบัติการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ และระบบสารสนเทศ

๘.๑ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอน และแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ

๘.๒ ผู้ดูแลระบบป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล๊อคที่ตัวเครื่อง การพินิจยืนยันตัวตน เป็นต้น

๘.๓ ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อทันทีเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

๘.๔ เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล, ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล, ระดับชั้นการเข้าถึง, เวลาที่ได้เข้าถึง, ช่องทางการเข้าถึง เป็นต้น

๘.๕ เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับสำหรับข้อมูลสำคัญ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

๒) ต้องกำหนดรายชื่อผู้ใช้บริการ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓) ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล



๕) ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๙. แนวทางปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้บริการ

๙.๑ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ให้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ให้บริการสามารถใช้บริการได้ตามภารกิจของผู้ให้บริการ และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๙.๒ ผู้ดูแลระบบต้องตรวจสอบบันทึกการปฏิบัติงานของผู้ให้บริการอย่างสม่ำเสมอ

๙.๓ ผู้ใช้บริการต้องรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และต้องปฏิบัติตามอย่างเคร่งครัด

๙.๔ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบ และรหัสผ่านของผู้ให้บริการ ดังต่อไปนี้

๑) เปลี่ยนแปลง และการยกเลิกรหัสผ่าน เมื่อผู้ให้บริการระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ให้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน และเมื่อผู้ให้บริการได้รับรหัสผ่านต้องตอบยืนยันการได้รับรหัสผ่าน

๓) กำหนดชื่อผู้ให้บริการ และรหัสผ่าน ต้องไม่ซ้ำกัน ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ให้บริการที่มีสิทธิสูงสุด ผู้ใช้บริการนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ให้บริการต่างจากรหัสผู้ให้บริการตามปกติ

๙.๕ เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลสำคัญตามประเภทชั้นความลับ เพื่อควบคุมป้องกันข้อมูลที่มีความสำคัญ ข้อมูลส่วนบุคคล โดยการกำหนดชั้นความลับของข้อมูล, วิธีปฏิบัติในการจัดเก็บข้อมูล และการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑) กำหนดรายชื่อผู้ให้บริการ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๓) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๔) สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนนำเครื่องคอมพิวเตอร์ไปให้บุคคลภายนอกใช้งาน หรือการส่งไปตรวจซ่อม

๑๐. แนวทางปฏิบัติการสำรอง และกู้คืนข้อมูล

๑๐.๑ ผู้ดูแลระบบกำหนดเจ้าหน้าที่รับผิดชอบดำเนินการสำรองข้อมูล โดยจัดทำเป็นลายลักษณ์อักษร และให้เจ้าหน้าที่ลงนามรับทราบ



๑๐.๒ ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติ ดำเนินการสำรองข้อมูล และการกู้คืนข้อมูล ที่เหมาะสม และรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้ระบบอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๑๐.๓ ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินตามระยะเวลาที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

๑๐.๔ ผู้ดูแลระบบต้องจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๑๐.๕ ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๑๐.๖ ผู้ดูแลระบบต้องจัดการกับอุปกรณ์สำหรับสำรองข้อมูลให้ปลอดภัยต่อการเข้าถึงโดยไม่ได้รับอนุญาต และสะดวกต่อการนำมาใช้กู้คืนข้อมูลในกรณีฉุกเฉินเมื่อข้อมูลที่จัดทำไว้เกิดการเสียหาย

๑๑. แนวทางปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑๑.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน

๑๑.๒ กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๑๑.๓ การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

- ๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
- ๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
- ๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๑๑.๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และการสื่อสารของหน่วยงาน

๑๑.๕ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๑.๖ ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยระบุผู้รับผิดชอบ และหน้าที่ความรับผิดชอบอย่างชัดเจน โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

๑๑.๗ ผู้ดูแลระบบทดสอบและปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง



๑๑.๘ ผู้ดูแลระบบต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อกรณีที่เหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

๑๒. แนวทางปฏิบัติของผู้ใช้บริการ

เพื่อให้ผู้ให้บริการมีความรู้ในการใช้ระบบคอมพิวเตอร์ ระบบเครือข่ายอย่างปลอดภัย และปฏิบัติตามอย่างเคร่งครัด ซึ่งประกอบด้วย การควบคุมการเข้าถึงระบบคอมพิวเตอร์, การใช้งานบัญชีผู้ให้บริการ (Account) และรหัสผ่าน (Password), การใช้งานระบบอินเทอร์เน็ต (Internet), การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) และการป้องกันจากโปรแกรมประสงค์ร้าย (Malware) ดังนั้น ผู้ใช้บริการจะต้องมีการปฏิบัติตามรายละเอียดดังนี้

๑๒.๑ การควบคุมการเข้าถึงระบบคอมพิวเตอร์ ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๑๒.๑.๑ ผู้ใช้บริการต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ให้บริการ และรหัสผ่านของตน ในการเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานร่วมกัน

๑๒.๑.๒ ผู้ใช้บริการตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๑๒.๒ การใช้งานบัญชีผู้ให้บริการ และรหัสผ่าน ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๑๒.๒.๑ ผู้ใช้บริการต้องเก็บรักษาหัสผ่าน โดยถือว่าเป็นความลับเฉพาะบุคคล จะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ และไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์โดยไม่ป้องกันการเข้าถึง

๑๒.๒.๒ ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ให้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งาน หรือหยุดการใช้งานชั่วคราว

๑๒.๒.๓ ผู้ใช้บริการควรกำหนดรหัสผ่าน ดังนี้

๑) รหัสผ่าน ควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักษรพิเศษและสัญลักษณ์ต่าง ๆ ด้วย

๒) ไม่ควรกำหนดรหัสผ่าน จากชื่อ หรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตน หรือคำศัพท์ที่ใช้ในพจนานุกรม หรือหมายเลขโทรศัพท์

๓) ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานอย่างน้อยทุก ๕ เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๑๒.๓ การใช้งานระบบอินเทอร์เน็ต (Internet) ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๑๒.๓.๑ ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบ อินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ให้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการขออนุญาตจากผู้อำนวยการกองยุทธศาสตร์และงบประมาณเป็นลายลักษณ์อักษรแล้ว

๑๒.๓.๒ ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุง (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา



๑๒.๓.๓ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้บริการทำการลงบันทึกออก (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๒.๔ การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

๑๒.๔.๑ ผู้ใช้บริการต้องใช้จดหมายอิเล็กทรอนิกส์กลางของภาครัฐในการติดต่อเรื่องที่เป็นงานราชการเท่านั้น

๑๒.๔.๒ ผู้ใช้บริการที่ต้องการขอลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงาน ยื่นคำขอ กับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิบัญชีผู้ใช้บริการรายใหม่ และรหัสผ่าน

๑๒.๔.๓ ผู้ใช้บริการที่ได้รับรหัสผ่านครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่านโดยทันที

๑๒.๔.๔ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้น ผู้ใช้บริการควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๑๒.๔.๕ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

๑๒.๕ การป้องกันจากโปรแกรมประสงค์ร้าย (Malware) ผู้ใช้บริการควรปฏิบัติ ดังต่อไปนี้

๑๒.๕.๑ ผู้ใช้บริการต้องติดตั้ง และใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๑๒.๕.๒ ผู้ใช้บริการควรทำการปรับปรุงระบบปฏิบัติการ (Windows Update) เว็บเบราว์เซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และป้องกันการโจมตีจากภัยคุกคาม

๑๒.๕.๓ ห้ามมิให้ผู้ให้บริการทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

๑๒.๕.๔ ผู้ใช้บริการที่มีเครื่องคอมพิวเตอร์ที่ติดโปรแกรมประสงค์ร้าย (Malware) ต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ดังกล่าวเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้าย (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ

๑๒.๕.๕ ผู้ใช้บริการควรตรวจสอบสื่อบันทึกพกพาก่อนการใช้งาน เช่น Thumb Drive และ External Storage เพื่อป้องกัน และกำจัดโปรแกรมประสงค์ร้าย (Malware)

