โรงพยาบาลนครพนม

นโยบาย

นโยบายเรื่อง : การรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

ชื่อหน่วยงาน : งานคอมพิวเตอร์	**วันที่** เมษายน ๒๕๖๑
ผู้ตรวจสอบ : ..... (นายจรุงธรรม ขันตี) ตำแหน่ง รองฯ ด้านพัฒนาระบบบริการสุขภาพ	**ผู้อนุมัติ** : ..... (นายยุทธชัย ตริสกุล) ผู้อำนวยการโรงพยาบาลนครพนม

นโยบายโรงพยาบาลนครพนม

เรื่อง การรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

โรงพยาบาลนครพนม กำหนดมาตรการความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ดังนี้

๑. ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มการบริการสารสนเทศตามผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

๒. ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับระบบเครือข่าย ต้องได้รับอนุญาตจากผู้บริหารสารสนเทศระดับสูง หรือหัวหน้างานคอมพิวเตอร์ - สารสนเทศ

๓. การขออนุญาตใช้งานพื้นที่ web service และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือหัวหน้างานคอมพิวเตอร์และสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของผู้ใช้บริการอื่นๆ หรือระบบเครือข่าย

๔. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๕. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๕.๑ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับการอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๒ ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นได้

๕.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอก

หน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๕.๔ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๕.๕ การเข้าสู่ระบบเครือข่ายภายนาหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็น จำเป็นต้องมีการลงบันทึกเข้า (login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๕.๖ เลขที่อยู่ ไอพี (IP Address) ของระบบเครือข่าย ภายในหน่วยงาน จำเป็นจำเป็นต้องมีการป้องกัน มิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๕.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะที่จำเป็น

๕.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ได้กำหนดขึ้นมา เพื่อเป็นมาตรการและแนวทางในการให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเจ้าหน้าที่ของโรงพยาบาลนครพนม จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ เมษายน ๒๕๖๑

(นายบุญเสริม ศรีธรรม)
ผู้อำนวยการโรงพยาบาลนครพนม