คำสั่งโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๙
ที่ ๓๐/๒๕๖๔
เรื่อง นโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับบุคลากร
โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๙

.....

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๙ เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC ๒๗๐๐๑ แบ่งออกเป็น ๒ กลุ่ม คือ

๑. กลุ่มผู้ใช้งานระบบสารสนเทศและเครือข่าย
๒. ผู้ดูแลระบบเทคโนโลยีสารสนเทศและเครือข่าย

๑. กลุ่มผู้ใช้งานสารสนเทศและเครือข่าย

๑.๑ นโยบายความมั่นคงปลอดภัยระบบบริการ HIS (HOSxp)

ข้อ ๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษารหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องตั้งรหัสผ่านประกอบด้วยตัวอักษรปนตัวเลขหรือตัวอักษรพิเศษไม่น้อยกว่า ๔ ตัวอักษร และทำการเปลี่ยนรหัสผ่าน (Password) ทุก ๓๐ วัน

ข้อ ๓ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๔ ผู้ใช้งานสามารถเข้าใช้ระบบ Hos xp ของโรงพยาบาล ๑ คนต่อ ๑ เครื่องเท่านั้น ไม่สามารถใช้รหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองเปิด Hosxp คอมพิวเตอร์ ๒ เครื่องได้

ข้อ ๕ ห้ามผู้ใช้งานกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้ Username และ Password ของผู้อื่น

ข้อ ๖ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๗ บุคลากรที่เข้าใช้งานระบบ Hosxp สามารถเข้าใช้งานได้เฉพาะหน่วยงานที่ตนสังกัดอยู่เท่านั้น

ข้อ ๘ ผู้ใช้งานที่พ้นสภาพการเป็นบุคลากรของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๙ งานการเจ้าหน้าที่ต้องแจ้งให้งานสารสนเทศทางการแพทย์ทราบ เพื่อยุติการเข้าใช้งานของบุคลากร

๑.๒ นโยบายการรักษาความลับและการเข้าถึงข้อมูลผู้รับบริการ

ข้อ ๑ ห้ามบุคลากรของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๙ ที่เข้าใช้ระบบ Hosxp ทำการคัดลอกประวัติของผู้รับบริการ โดยไม่ได้รับอนุญาตจากผู้รับบริการเช่น การถ่ายภาพจากหน้าจอคอมพิวเตอร์ การปริ้นสกรีน เป็นต้น ถ้าพบจะถูกดำเนินการตาม พรบ.คอมพิวเตอร์และระเบียบของโรงพยาบาล

ข้อ ๒ การขอ...

ข้อ ๒ การขอข้อมูลผู้ป่วยเพื่อไปทำผลงานวิชาการหรือเพื่อดำเนินการระหว่างรับต่อรัฐ ต้องทำเป็นลายลักษณ์อักษรตามแนวทางที่คณะกรรมการเทคโนโลยีสารสนเทศและเวชระเบียนกำหนด

ข้อ ๓ ห้ามเปิดเผยข้อมูลผู้ป่วยและผู้รับบริการผ่านสื่อสังคมออนไลน์และเครื่องมือสื่อสารทุกชนิด หากต้องการขอคำปรึกษาด้านการรักษาของผู้ป่วยหรือผู้รับบริการ ต้องปฏิบัติตามแนวทางที่คณะกรรมการเทคโนโลยีสารสนเทศและเวชระเบียนกำหนด

๑.๓ นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ตและเครือข่ายไร้สาย

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ตและเครือข่ายไร้สายของทางโรงพยาบาล เพื่อหาประโยชน์ในเชิงพาณิชย์ เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์

ข้อ ๒ การใช้งานอินเทอร์เน็ตและเครือข่ายไร้สายต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูล

ข้อ ๓ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงานหรือโรงพยาบาล ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาล หรือ บุคคลอื่น

ข้อ ๔ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

ข้อ ๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของทางโรงพยาบาล ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑.๔ นโยบายการบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ สิทธิในการเข้าถึงหรือใช้งานระบบเครือข่ายหรือสารสนเทศ เป็นสิทธิของผู้บริหาร แพทย์ บุคลากร เจ้าหน้าที่ หรือบุคคลอื่นที่ได้รับอนุญาตจากผู้บริหารหรือผู้มีอำนาจเท่านั้น

ข้อ ๒ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ เข้าหรือออกระบบเครือข่ายหรือระบบสารสนเทศควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN เป็นต้น

๑.๕ นโยบายความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่าย

ข้อ ๑ ห้ามเข้าห้อง SERVER ก่อนได้รับอนุญาต

ข้อ ๒ ห้ามบุคลากรเคลื่อนย้ายครุภัณฑ์คอมพิวเตอร์ ก่อนได้รับอนุญาตจากงานสารสนเทศทางการแพทย์

ข้อ ๓ บุคลากรที่เข้าใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง เช่น USB ต้องสแกนไวรัสก่อนทุกครั้ง

ข้อ ๔ บุคลากรที่เข้าใช้งานเครื่องคอมพิวเตอร์หากสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัสต้องแจ้งงานสารสนเทศทางการแพทย์ทันที

๒. กลุ่มผู้ดูแลระบบสารสนเทศและเครือข่าย

๒.๑ นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๒ ห้ามมิให้ผู้ดูแลระบบทำการบอกหรือเปิดเผยข้อมูลที่เป็นความลับทั้งข้อมูลของอุปกรณ์เครื่องแม่ข่าย รหัสผ่าน และข้อมูลอื่นๆ อันจะส่งเกิดผลเสียหายต่ออุปกรณ์ เครื่องแม่ข่าย หรือระบบเครือข่ายต่อผู้ใช้งานทั่วไป

ข้อ ๓ ผู้ดูแลระบบต้องพิสูจน์ตัวตนการใช้งานระบบเครือข่ายและสารสนเทศเช่นเดียวกับผู้ใช้งานทั่วไป

ข้อ ๔ ผู้ดูแล...

ข้อ ๔ ผู้ดูแลระบบต้องทำการเขียนเป็นบันทึกเมื่อทำการตั้งค่า แก้ไข กับอุปกรณ์หรือเครื่องแม่ข่าย ทุกครั้งที่มีการเปลี่ยนแปลง

๒.๒ นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ ๑ ให้ผู้ดูแลระบบกำหนดค่าการให้บริการของเครื่องแม่ข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จาเป็นต่อการให้บริการเท่านั้น

ข้อ ๒ การเข้าถึงตัวอุปกรณ์ เครื่องแม่ข่าย และห้องเซิฟเวอร์ต้องมีมาตรฐานรักษาความปลอดภัยและพิสูจน์ตัวตน

ข้อ ๓ ห้ามใช้ทรัพยากร เครื่องแม่ข่าย รวมถึงอุปกรณ์อื่นใดของโรงพยาบาล เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม กฎหมาย ความมั่นคงของประเทศ

ข้อ ๔ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๕ จัดสำรองไฟล์ระบบปฏิบัติบนอุปกรณ์เครือข่ายอย่างสม่ำเสมอ

ข้อ ๖ ผู้ดูแลระบบมีหน้าที่ต้องตรวจสอบและรายงานผลถึงข้อผิดพลาดของอุปกรณ์เครือข่าย ตลอดจนเครื่องแม่ข่าย และจัดทำรายงาน

๒.๓ นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล

ข้อ ๑ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ ๒ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔ นโยบายความมั่นคงปลอดภัยของอินเตอร์เน็ตและเครือข่ายไร้สาย

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และ Username และ Password ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๓ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายภายในและฐานข้อมูลภายในต่างๆ ของทางโรงพยาบาล โดยไม่ได้รับอนุญาต

การฝ่าฝืนและการลงโทษ

ข้อ ๑ ให้ดำเนินการพิจารณาโทษทางวินัยแก่ผู้ฝ่าฝืน

ข้อ ๒ หากการกระทำอันฝ่าฝืนเป็นความผิดตามกฎหมายทำให้โรงพยาบาลเสื่อมเสียชื่อเสียงสามารถให้โรงพยาบาล ดำเนินคดีทั้งทางอาญาและทางแพ่งกับผู้กระทำผิดอีกทางหนึ่งด้วย

ข้อ ๓ ทางโรงพยาบาล...

ข้อ ๓ ทางโรงพยาบาลสามารถเข้าไปตรวจสอบดูข้อมูลในเครื่องคอมพิวเตอร์ ในกรณีที่สงสัยว่าจะทำการฝ่าฝืนประกาศ

สั่ง ณ วันที่ / เดือน กุมภาพันธ์ พ.ศ.๒๕๖๔

(นายสมชาย ไวทิตานันท์)
ผู้อำนวยการโรงพยาบาลไทรโยค รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๙