**<u>ระเบียบวิธีปฏิบัติ เรื่อง ความมั่นคงปลอดภัยของระบบสารสนเทศ</u>**

**เรื่อง การเข้าถึงระบบสารสนเทศ**

**วัตถุประสงค์**

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
๒. เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก
๓. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์
๔. เพื่อให้ผู้ปฏิบัติได้รับรู้เข้าใจ และ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

**วิธีปฏิบัติ**

๑. ผู้ดูแลระบบ ได้กำหนดสิทธิเบื้องต้นในการเข้าใช้งานตามมติ บอร์ดพัฒนาระบบสารสนเทศ
๒. เมื่อผู้ใช้งานต้องการเพิ่มสิทธิ์ ให้ติดต่อ ที่ผู้ดูแลระบบ เพื่อทำบันทึกเป็นลายลักษณ์อักษรเพื่อ ขอเพิ่มสิทธิ
๓. ทบทวนเรื่องสิทธิ ปีละ ๑ ครั้ง
๔. ผู้ที่ได้รับสิทธิ์สูงสุด ต้องได้รับความเห็นชอบจากผู้อำนวยการโรงพยาบาล
๕. กรณีผู้ทำงานใหม่ ให้ติดต่อผู้ดูแลระบบเพื่อเข้าใช้งานในระบบต่างๆ
๖. ต้องมีการลงบันทึกการเข้าใช้งาน (login)และต้องมีการพิสูจน์ยืนยันตัวตนด้วยรหัสผ่านก่อนการใช้งาน สำหรับผู้ที่จะเข้าใช้งานต่อไปนี้
   ๖.๑. ระบบ hosxp
   ๖.๒. ระบบ internet
   ๖.๓. ระบบ PAC
   ๖.๔. โปรแกรม RM
   ๖.๕. โปรแกรม SLA
   ๖.๖. ระบบ Smart Queue
๗. ผู้ใช้งานต้องทำการลงบันทึกออกทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
๘. เมื่อผู้ใช้งานระบบอินเตอร์เน็ต ต้องออกจากบราวเซอร์เพื่อป้องกันการใช้โดยบุคคลอื่นด้วยเสมอ
๙. เมื่อมีการตรวจสอบว่า การบันทึกหรือการแก้ไขข้อมูล หรือการเข้าดูข้อมูล นั้นเกิดจาก user,password ใด บุคคลที่มีรายชื่อตามบัญชีรายชื่อผู้นั้น จะเป็นผู้รับผิดชอบ ในการบันทึก แก้ไข เข้าดูข้อมูลในครั้งนั้น
๑๐. จัดระบบสำหรับการเข้าทำงานจากภายนอกโรงพยาบาล ผ่าน VPN

**๑๑.การบริหารจัดการรหัสผ่าน**

๑๑.๑ กรณีสำหรับระบบ hosxp ที่แรกเริ่มเดิมที เป็นรหัส ๑๒๓๔ ให้ผู้ใช้งานทำคนได้เปลี่ยนรหัส เป็น รหัสอย่างน้อย ๖ ตัว และ ไม่ให้เป็นตัวเลข หรือ ตัวอักษร เรียงกัน หรือ จากคำศัพท์ในพจนานุกรม

๑๑.๒ ผู้ใช้งานควรเปลี่ยนรหัสทุก ๓ เดือน

สำหรับกรณีผู้ใช้งานรายใหม่ ทาง ผู้ดูแลระบบจะได้กำหนดรหัสผ่านที่ไม่ใช่รหัสต้องห้ามไว้

๑๑.๓ ผู้ดูแลระบบทำการยกเลิกการใช้ user password เมื่อผู้ใช้งานได้ลาออก หรือ ย้ายออกจากโรงพยาบาล

๑๑.๔ ผู้ใช้งานต้องไม่ให้ใครล่วงรู้รหัสผ่านของตน

๑๑.๕ ไม่จด หรือ บันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑๑.๖ เมื่อมีความจำเป็นที่จะต้องบอกรหัสให้ผู้อื่น ให้ทำการเปลี่ยนรหัสทันที

๑๒. กำหนดไม่ให้มีการเก็บข้อมูลที่เป็นความลับ รวมทั้งรหัสผ่าน ให้เข้าถึงได้ง่ายทางกายภาพที่โต๊ะทำงานหรือบนหน้าจอ (clear desk, clear screen policy)

๑๓. ผู้ดูแลระบบ ทำการบันทึก การเข้าถึงข้อมูลของ user และ ติดตามเป็นประจำทุกเดือน และ รายงานประธานบอร์ดสารสนเทศทราบทุกเดือน

๑๔. กรณีส่งเครื่องคอมพิวเตอร์ซ่อมภายนอกโรงพยาบาล ให้ดำเนินการสำรองข้อมูลและลบข้อมูลที่เก็บไว้ออกก่อน

๑๕. ความผิดพลาดและปัญหาที่อาจจะเกิดขึ้นจากการไม่ปฏิบัติตามประกาศนี้ หรือจากการนำรหัสผู้ใช้งานและรหัสผ่านไปให้บุคคลอื่นใช้งาน ผู้ที่มีชื่อเป็นเจ้าของรหัสผู้ใช้งานและรหัสผ่านนั้นๆจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๑๖. **สำหรับกรณีบุคคลภายนอก**

๑๖.๑ ให้ติดต่อผู้ดูแลระบบ เพื่อทำบันทึก เพื่อขออนุญาต พร้อมเหตุผล ก่อนเข้าใช้ระบบ โดยระบุความเสี่ยงที่อาจจะเกิดขึ้นพร้อมกำหนดแนวทางป้องกันและแก้ไขความเสี่ยงนั้นก่อนเสนอให้รับการอนุญาตโดยประธานบอร์ดพัฒนาระบบสารสนเทศ นำเสนอผู้อำนวยการโรงพยาบาลวังโป่งเพื่อทำการอนุมัติอีกครั้ง

๑๖.๑.๑กรณีบำรุงรักษาระบบ ต้องมีหนังสือจากองค์กร มาที่ผู้อำนวยการ และ admin จะเป็นผู้กรอกรหัสผ่านให้โดยไม่บอก กับบุคคลภายนอก และ อยู่ดูแล ควบคุม กำกับ กับบุคคลภายนอกตลอดเวลา

๑๖.๑.๒ กรณีขอเข้าดูประวัติผู้ป่วยผ่านระบบ ให้ทำเหมือนขอดูประวัติผู้ป่วยผ่านระบบเวชระเบียน

๑๖.๒ ควบคุม network port number อย่างรัดกุม

๑๖.๓ ผ่านระบบการพิสูจน์ตัวตนด้วยเช่นกัน

๑๗. กรณีผู้ใช้งาน ได้ลาออก หรือ เปลี่ยนตำแหน่ง หน้าที่ความรับผิดชอบ ให้งานบริหารฝ่ายบุคลากร ทำการแจ้งผู้ดูแลระบบ เพื่อทำการปรับปรุงสิทธิการเข้าใช้ หรือ ยกเลิกการใช้งาน

๑๘. จัดทำ log เก็บการใช้งานอินเตอร์เน็ท และ มีระบบพิสูจน์ตัวตนในการเข้าถึงระบบ log