

ระเบียบวิธีปฏิบัติ เรื่อง ความมั่นคงปลอดภัยของระบบสารสนเทศ

เรื่อง การเข้าถึงระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคง ปลอดภัย
2. เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก
3. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์
4. เพื่อให้ผู้ปฏิบัติได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วิธีปฏิบัติ

1. ผู้ดูแลระบบ ได้กำหนดสิทธิ์เบื้องต้นในการเข้าใช้งานตามมติ บอร์ดพัฒนาระบบสารสนเทศ
2. เมื่อผู้ใช้งานต้องการเพิ่มสิทธิ์ ให้ติดต่อ ที่ผู้ดูแลระบบ เพื่อทำบันทึกเป็นลายลักษณ์อักษรเพื่อ ขอเพิ่มสิทธิ์
3. ทบทวนเรื่องสิทธิ์ ปีละ 1 ครั้ง
4. ผู้ที่ได้รับสิทธิ์สูงสุด ต้องได้รับความเห็นชอบจากผู้อำนวยการโรงพยาบาล
5. กรณีทำงานใหม่ ให้ติดต่อผู้ดูแลระบบเพื่อเข้าใช้งานในระบบต่างๆ
6. ต้องมีการลงบันทึกการเข้าใช้งาน (login)และต้องมีการพิสูจน์ยืนยันตัวตนด้วยรหัสผ่านก่อนการเข้าใช้งาน สำหรับ ผู้ที่จะเข้าใช้งานต่อไปนี้
 - 6.1 ระบบ Hosxp
 - 6.2 ระบบ Internet
 - 6.3 ระบบ Hosoffice
 - 6.4 ระบบสารสนเทศการบริหารจัดการความเสี่ยงของสถานพยาบาล
7. ผู้ใช้งานต้องทำการลงบันทึกออกทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
8. เมื่อผู้ใช้งานระบบอินเทอร์เน็ต ต้องออกจากบราวเซอร์เพื่อป้องกันการใช้โดยบุคคลอื่นด้วยเสมอ
9. เมื่อมีการตรวจสอบว่า การบันทึกหรือการแก้ไขข้อมูล หรือการเข้าดูข้อมูล นั้นเกิดจาก user,password ใด บุคคลที่มีรายชื่อตามบัญชีรายชื่อผู้นั้น จะเป็นผู้รับผิดชอบ ในการบันทึก แก้ไข เข้าดูข้อมูลในครั้งนั้น
10. จัดระบบสำหรับการเข้าทำงานจากภายนอกโรงพยาบาล ผ่าน VPN
11. การบริหารจัดการรหัสผ่าน
 - 11.1 กรณีสำหรับระบบ HosXP ที่แรกเริ่มเดิมที เป็นรหัส demo ให้ผู้ใช้งานทำคนได้เปลี่ยนรหัส เป็น รหัส อย่างน้อย 6 ตัว และ ไม่ให้เป็นตัวเลข หรือ ตัวอักษร เรียงกัน หรือ จากคำศัพท์ในพจนานุกรม
 - 11.2 การเข้าถึงข้อมูลผู้ป่วยในระบบ HosXP โดยทะเบียนผู้ใช้งานระบบแบ่งออกตามกลุ่ม ดังต่อไปนี้

อนุญาตโดยประธาน บอร์ดพัฒนาระบบสารสนเทศ นำเสนอผู้อำนวยการโรงพยาบาลวังโป่งเพื่อทำการอนุมัติอีกครั้ง

16.1.1 กรณีบำรุงรักษาระบบ ต้องมีหนังสือจากองค์กร มาที่ผู้อำนวยการ และ admin จะเป็นผู้กรอก รหัสผ่านให้โดยไม่บอก กับบุคคลภายนอก และ อยู่ดูแล ควบคุม กำกับ กับ บุคคลภายนอกตลอดเวลา

16.1.2 กรณีขอเข้าดูประวัติผู้ป่วยผ่านระบบ ให้ทำเหมือนขอดูประวัติผู้ป่วยผ่านระบบเวชระเบียน

16.2 ควบคุม network port number อย่างรัดกุม

16.3 ผ่านระบบการพิสูจน์ตัวตนด้วยเช่นกัน

17. กรณีผู้ใช้งาน ได้ลาออก หรือ เปลี่ยนตำแหน่ง หน้าที่ความรับผิดชอบ ให้งานบริหารฝ่ายบุคลากร ทำการแจ้ง ผู้ดูแลระบบ เพื่อทำการปรับปรุงสิทธิการเข้าใช้ หรือ ยกเลิกการใช้งาน

18. จัดทำ log เก็บการใช้งานอินเทอร์เน็ต และมีระบบพิสูจน์ตัวตนในการเข้าถึงระบบ log