คำสั่งโรงพยาบาลลำพูน

ที่ /๒๕๖๕

เรื่อง แจ้งวิธีปฏิบัติของผู้ใช้งานระบบเทคโนโลยสารสนเทศและการสื่อสารโรงพยาบาลลำพูน

.....

วิธีปฏิบัติของเจ้าหน้าผู้ใช้ระบบคอมพิวเตอร์และ internet ในโรงพยาบาลลำพูน

เพื่อให้มีความรู้ในการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายอย่างปลอดภัย และปฏิบัติตามอย่างเคร่งครัด ซึ่งประกอบด้วย การควบคุมการเข้าถึงระบบคอมพิวเตอร์ , การใช้งานบัญชีเจ้าหน้าที่โรงพยาบาล (Account) และ รหัสผ่าน (Password) , การใช้งานระบบอินเตอร์เน็ต (Internet) , และการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

การควบคุมการเข้าถึงระบบคอมพิวเตอร์ ควรปฏิบัติดังต่อไปนี้

๑. เจ้าหน้าที่โรงพยาบาลต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๒. เจ้าหน้าที่โรงพยาบาลต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อเจ้าหน้าที่โรงพยาบาลและรหัสผ่านของตนในการเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓. เจ้าหน้าที่โรงพยาบาลตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

การใช้งานบัญชีเจ้าหน้าที่โรงพยาบาล และ รหัสผ่าน เจ้าหน้าที่โรงพยาบาลควรปฏิบัติดังต่อไปนี้

๑. เจ้าหน้าที่โรงพยาบาลต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๒. เจ้าหน้าที่โรงพยาบาลต้องเก็บรักษารหัสผ่าน โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ และไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์โดยไม่ป้องกันการเข้าถึง

๓. เจ้าหน้าที่โรงพยาบาลจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีเจ้าหน้าที่โรงพยาบาลของตนเองและทำลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๔. เจ้าหน้าที่โรงพยาบาลควรกำหนดรหัสผ่าน ดังนี้

๔.๑ รหัสผ่าน ควรมีความยาวไม่น้อยกว่า ๔ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลขตัวอักษรและตัวเลข

๔.๒ ไม่ควรกำหนดรหัสผ่าน จากชื่อ หรือชื่อสกุลของเจ้าหน้าที่โรงพยาบาล ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือหมายเลขโทรศัพท์

๔.๓ ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานอย่างน้อยทุก ๖ เดือน หรือเปลี่ยนรหัสผ่าน ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

/การใช้งานระบบ...

การใช้งานระบบอินเตอร์เน็ต (Internet) เจ้าหน้าที่โรงพยาบาลควรปฏิบัติดังต่อไปนี้

๑. เจ้าหน้าที่โรงพยาบาลต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๒. เจ้าหน้าที่โรงพยาบาลต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเตอร์เน็ต ผ่านระบบรักษาความปลอดภัย (Firewall) ที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามเจ้าหน้าที่โรงพยาบาลทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้ช่วยผู้อำนวยการด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๓. เจ้าหน้าที่โรงพยาบาลต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุง (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๔. หลังจากใช้งานระบบอินเตอร์เน็ต (Internet) เสร็จแล้ว ให้เจ้าหน้าที่โรงพยาบาลทำการลงบันทึกออก (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

การป้องกันจากโปรแกรมประสงค์ร้าย (Malware) เจ้าหน้าที่โรงพยาบาลควรปฏิบัติดังต่อไปนี้

๑. เจ้าหน้าที่โรงพยาบาลต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๒. ศูนย์คอมพิวเตอร์จะต้องติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งการปรับปรุงให้ทันสมัยอยู่เสมอ

๓. ศูนย์คอมพิวเตอร์จะทำการปรับปรุงระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และป้องกันการโจมตีจากภัยคุกคาม

๔. ห้ามมิให้เจ้าหน้าที่โรงพยาบาลทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

๕. เจ้าหน้าที่โรงพยาบาลที่มีเครื่องคอมพิวเตอร์ที่ติดโปรแกรมประสงค์ร้าย ต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ดังกล่าวเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้ายไปยังเครื่องคอมพิวเตอร์อื่นๆ

๖. เจ้าหน้าที่โรงพยาบาลควรตรวจสอบสื่อบันทึกพกพาก่อนการใช้งาน เช่น Thumb Drive และ Data Storage เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย

สั่ง ณ วันที่ กรกฎาคม พ.ศ. ๒๕๖๕

(นายธีรพงษ์ ตติยพรกุล)
ผู้ช่วยผู้อำนวยการด้านเทคโนโลยีสารสนเทศและนวัตกรรม