



ประกาศโรงพยาบาลบางบ่อ

เรื่อง ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๘

หมวด ๓ ผู้ใช้ระบบสารสนเทศ

หมวดที่ ๓ ผู้ใช้ระบบสารสนเทศ

๑. วัตถุประสงค์

ระเบียบปฏิบัติงานนี้เพื่อเป็นแนวทางการบริหารความมั่นคงปลอดภัย การควบคุม และการปฏิบัติงาน ด้านเทคโนโลยีสารสนเทศโรงพยาบาลบางบ่อ

๒. ขอบข่าย

ระเบียบปฏิบัติตามเอกสารฉบับนี้ใช้สำหรับเจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศของโรงพยาบาลบางบ่อ

๓. ความรับผิดชอบ

เจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศของโรงพยาบาลบางบ่อ ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ โรงพยาบาล ต้องปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

- ๓.๑ ศึกษา ทำความเข้าใจ และปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ๓.๒ เมื่อมีข้อสงสัยเกี่ยวกับการปฏิบัติ ให้ปรึกษาผู้บังคับบัญชา หรือกลุ่มภารกิจสุขภาพดิจิทัล
- ๓.๓ เมื่อพบปัญหา การปฏิบัติตามระเบียบปฏิบัติความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้รายงาน ข้อมูลได้ทุกช่องทาง ได้แก่ รายงานผู้บังคับบัญชาโดยตรง การเขียนรายงานอุบัติการณ์ เป็นต้น

๔. คำจำกัดความที่เกี่ยวข้อง

- ๔.๑ เจ้าหน้าที่ผู้ใช้งานระบบสารสนเทศ หมายถึง เจ้าหน้าที่ของโรงพยาบาลบางบ่อ ที่มีบัญชีการใช้งาน ระบบสารสนเทศของโรงพยาบาล

๕. ระบบสารสนเทศโรงพยาบาล

หมายถึง ระบบคอมพิวเตอร์ที่ใช้สำหรับบริหารงานโรงพยาบาล ซึ่งประกอบไปด้วย ข้อมูลผู้ป่วย ข้อมูลการรักษา และข้อมูลอื่นๆ ที่เกี่ยวข้องกันรายละเอียด

๕.๑ ผู้ใช้งานระบบ

๕.๑.๑. การรักษาหัสผ่าน การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- ๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
- ๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)
- ๓) หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อ หรือนามสกุลของ ตนเองหรือตรงกับคำในพจนานุกรม
- ๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- ๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- ๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับ ผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- ๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้ เปลี่ยนรหัสผ่าน

๕.๑.๒. การรักษาข้อมูลผู้ป่วย การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบกระทรวงสาธารณสุข ว่าด้วยการคุ้มครอง และจัดการข้อมูลด้านสุขภาพของบุคคล พ.ศ. ๒๕๖๑

๕.๑.๓. การใช้งานระบบสารสนเทศโรงพยาบาล ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สิทธิ์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ติ หรือเกิดจากความผิดพลาดใด ๆ ก็ติ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- ๑) คอมพิวเตอร์ทุกประเภท การเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

- ๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
- ๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
- ๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตน ก่อนการใช้งานทุกครั้ง
- ๕) ผู้ใช้งานต้องตั้งเวลาพักหน้าจอ (Screen Saver) หลังจากไม่ได้ใช้งานเป็นเวลา ๑๐ นาที และต้องใส่ รหัสผ่าน (Password) ให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

ประกาศ ณ วันที่ ๓ มีนาคม ๒๕๖๘



(นายวี โรจนศิริประภา)

นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลบางบ่อ