ประกาศโรงพยาบาลสตูล
เรื่อง ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศโรงพยาบาลสตูล
(สำหรับผู้ดูแลระบบ)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสตูล เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้ง ป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุมคามจากภัยต่างๆ โรงพยาบาลสตูลจึงเห็นควรกำหนดแนวปฏิบัติให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศต่างๆ ดังนี้

๑. **การตรวจสอบระบบความมั่นคงปลอดภัย**
   - ตรวจสอบระบบสารสนเทศเป็นประจำเพื่อตรวจพบช่องโหว่งและปัญหาที่อาจทำให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัย
   - ทำการประสานงานระหว่างทีมผู้ดูแลระบบและผู้ใช้งานเพื่อเข้าใจความต้องการและปัญหาที่เกิดขึ้น

๒. **การบริหารจัดการสิทธิ์และการเข้าถึงข้อมูล**
   - กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบให้เหมาะสมกับบทบาทและความจำเป็นของผู้ใช้งาน
   - ตรวจสอบและปรับปรุงสิทธิ์เป็นระยะเป็นระยะ

๓. **การรักษาความลับของข้อมูล**
   - กำหนดมาตรฐานเทคโนโลยีการเข้ารหัสข้อมูลเพื่อรักษาความลับ
   - จำกัดการเข้าถึงข้อมูลที่มีความสำคัญ

๔. **การสำรองข้อมูล (Backup)**
   - ทำการสำรองข้อมูลอย่างสม่ำเสมอตามกฎ ๓-๒-๑
   - ทดสอบการคืนค่าข้อมูลจากระบบสำรองเพื่อให้แน่ใจว่ามีความพร้อมในกรณีเกิดภัยคุกคาม

๕. **การป้องกันไวรัสและซอฟแวร์**
   - ติดตั้งโปรแกรมป้องกันไวรัสและซอฟแวร์ (Firewall) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
   - ทำการอัปเดทซอฟแวร์อย่างสม่ำเสมอ

๖. **การตรวจสอบและการบันทึก**
   - ตรวจสอบไฟล์บันทึก (Log) เพื่อตรวจสอบกิจกรรมที่เป็นไปในระบบ
   - บันทึกและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

๗. **การตอบสนองต่อเหตุการณ์ฉุกเฉิน**
   - จัดทำแผนที่จำปฏิบัติในกรณีเกิดเหตุการณ์ที่ไม่คาดฝัน เช่น การโจมตีไซเบอร์หรือภัยธรรมชาติ
   - ทดสอบและปรับปรุงแผนการตอบสนองเหตุการณ์ฉุกเฉินอย่างสม่ำเสมอ

จึงประกาศมาให้ทราบ และถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๕ มกราคม ๒๕๖๗

(นางสาววันทนา ไทรงาม)
ผู้อำนวยการโรงพยาบาลสตูล