ประกาศโรงพยาบาลท่าวังผา

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ด้วยโรงพยาบาลท่าวังผาได้ขับเคลื่อนนโยบายความปลอดภัยของผู้ป่วยและบุคลากรสาธารณสุข โดยมุ่งเน้นการทำงานที่มีความปลอดภัยในการดูแลผู้ป่วยและความปลอดภัยของผู้ให้บริการร่วมด้วย ความมั่นคงปลอดภัยระบบสารสนเทศเป็นหนึ่งในประเด็นการขับเคลื่อนของโรงพยาบาลท่าวังผา เพื่อให้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ โรงพยาบาลท่าวังผาจึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศดังต่อไปนี้

๑. กำหนดประเภทของข้อมูลของโรงพยาบาลเป็น ๖ ประเภทใหญ่ๆ และกำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพ ในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาลท่าวังผาในแต่ละประเภท ดังนี้

๑.๑. **ข้อมูลผู้ป่วย** หน่วยงานหลักคือ **ห้องบัตรและเวชระเบียน**

๑.๒. **ข้อมูลบุคลากรโรงพยาบาล** หน่วยงานหลัก**คือ ฝ่ายบริหารงาน (บุคลากร)**

๑.๓. **ข้อมูลการเงินและบัญชี** หน่วยงานหลักคือ **ฝ่ายงานบริหาร (การเงินและบัญชี)**

๑.๔. **ข้อมูลทางการรักษาโรค** หน่วยงานหลักคือ **แพทย์ พยาบาล และ เวชระเบียน**

๑.๕. **ข้อมูลทางการบริหาร** หน่วยงานหลักคือ **ฝ่ายบริหาร**

๑.๖. **ข้อมูลการจราจรทางคอมพิวเตอร์** หน่วยงานหลักคือ **กลุ่มงานสุขภาพดิจิทัล**

๒. กำหนดพื้นที่ควบคุมทางสารสนเทศโดยให้ผู้ที่ปฏิบัติงานสามารถเข้าออกพื้นที่ได้ ส่วนบุคคลอื่นต้องได้รับอนุญาตจากผู้รับผิดชอบหลัก ดังต่อไปนี้

๒.๑. **ห้องเก็บเวชระเบียนผู้ป่วยนอก** หน่วยงานหลักคือ **ห้องบัตรและเวชระเบียน**

๒.๒. **ห้องเก็บเวชระเบียนผู้ป่วยใน** หน่วยงานหลักคือ **กลุ่มงานสุขภาพดิจิทัล**

๒.๓. **ห้องเก็บเอกสารทางการเงินและบัญชี** หน่วยงานหลักคือ **ฝ่ายงานบริหาร (การเงินและบัญชี)**

๒.๔. **ห้องติดตั้งคอมพิวเตอร์แม่ข่าย (sever)** ผู้รับผิดชอบหลักคือ **กลุ่มงานสุขภาพดิจิทัล (ผู้ดูแลระบบ)**

๒.๕. **ห้องเก็บอุปกรณ์สำรองคอมพิวเตอร์** ผู้รับผิดชอบหลักคือ **กลุ่มงานสุขภาพดิจิทัล (ผู้ดูแลระบบ)**

๓. กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของโรงพยาบาล เป็น ๔ ระดับ ดังนี้

๓.๑ **ลับ** รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง ได้แก่ ข้อมูลผู้ป่วยเฉพาะโรค ข้อมูลการกระทำผิดทางวินัยของบุคลากร

๓.๒. **ใช้ภายในเท่านั้น** เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างกลุ่มทำงาน/หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในโรงพยาบาล ได้แก่ ข้อมูลผู้ป่วย ข้อมูลทางการรักษาโรค ข้อมูลทางการเงินและบัญชี

๓.๓. **ส่วนบุคล** ใช้เฉพาะตัวบุคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลขั้นตอนนั้น ได้แก่ ข้อมูลบุคลากร รหัสผ่านประจำตัวบุคลในการเข้าใช้งานระบบสารสนเทศ

๓.๔. **เปิดเผยได้** เป็นข้อมูลที่สามารถเปิดเผยได้ทั้งภายในและภานนอกโรงพยาบาล ได้แก่ ข้อมูลสถาณการณ์โรคต่าง ๆ ข้อมูลเอกสารทางวิชาการ

๔. การเข้าถึงข้อมูลและสารสนเทศโรงพยาบาล

๔.๑. กำหนดให้ผู้ดูแลระบบเป็นผู้บริหารจัดการ เป็นผู้ตรวจสอบ อนุมัติและกำหนดรหัสผ่านให้ผู้ใช้งานเข้าถึงข้อมูลตามสิทธิการเข้าถึงระบบสารสนเทศของโรงพยาบาล

๔.๒. การใช้งานที่ต้องกำหนกรหัสผ่านของโรงพยาบาล ได้แก่ โปรแกรมจัดการข้อมูลผู้ป่วย (HOSxP) และการเชื่อมต่อเครือข่ายไร้สาย โดยผู้ใช้งานจะต้องแจ้งขอเปิดสิทธิกับผู้ดูแลระบบ เพื่อรับรหัสใช้งานและรหัสผ่าน และจะต้องไม่ให้ผู้ใดใช้รหัสของตน

๔.๓. สิทธิการเข้าถึงโปรแกรมจัดการข้อมูลผู้ป่วย (HOSxP)

๔.๓.๑ **ผู้ใช้งาน (User)** จะเข้าถึงคงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย สามารถบันทึก แก้ไข ลบ ข้อมูลในความรับผิดชอบของตนเองได้ แต่จะไม่สามารถเข้าถึงข้อมูลบางอย่างที่ไม่ได้รับอนุญาต และฐานข้อมูลได้

๔.๓.๒. **ผู้ดูแลระบบ (Admin)** เข้าถึงตามภาระหน้าที่ได้รับมอบหมาย และสามารถบริหารจัดการ ตรวจสอบ อนุมัติ ลงทะเบียนให้สิทธิการเข้าใช้งานผู้ใช้งานอื่น ๆ และตัดสิทธิการเข้าใช้งานหากตรวจพบความผิดปกติ สามารถจัดการในระดับฐานข้อมูลได้

๕. การใช้เครื่องคอมพิวเตอร์สำนักงานและคอมพิวเตอร์พกพา

๕.๑. **คอมพิวเตอร์แม่ข่าย**

๕.๑.๑. ติดตั้งไว้ในห้องที่ปิดมิดชิด การเข้าออกต้องมีกุญแจ และต้องควบคุมให้อยู่ในอุณหภูมิที่ไม่เกิน ๒๕ องศาอยู่ตลอดเวลา

๕.๑.๒. กำหนดให้ผู้ดูแลระบบ (Admin) เป็นผู้รับผิดชอบดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพหากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย ให้รีบดำเนินการแก้ไข สามารถติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๕.๑.๓. ไม่อนุญาตให้ผู้อื่นเข้าออกห้องคอมพิวเตอร์แม่ข่าย นอกจากจะได้รับอนุญาตจากผู้ดูแลระบบ

๕.๒ **คอมพิวเตอร์สำนักงานและคอมพิวเตอร์โน้ตบุคที่จัดให้ใช้ร่วมกัน**

๕.๒.๑ จะถูกติดตั้ง IP ประจำเครื่องทุกเครื่อง เป็นแบบ fix IP และจะถูกติดตั้งโปรแกรมการใช้งานพื้นฐานที่จำเป็น เช่น โปรแกรมสแกนไวรัส Firewall ต่าง ๆ กำหนดให้มีผู้ดูแลประจำเครื่อง มีการลงทะเบียนคุมไว้ที่ผู้ดูแลระบบตามหมายเลข IP ประจำเครื่องและจุดติดตั้ง

๕.๒.๒. ห้ามผู้ใช้งานเปลี่ยน IP ประจำเครื่องโดยเด็ดขาด

๕.๒.๓. ห้ามผู้ใช้งานติดตั้งโปรแกรมที่นอกเหนือจากการทำงานโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๕.๒.๔. ผู้ใช้งานจะต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ ทุกครั้งที่นำมาเชื่อมต่ออุปกรณ์คอมพิวเตอร์ของโรงพยาบาล

๖. การใช้งานอินเตอร์เน็ตและระบบเครือข่ายไร้สาย

๖.๑. ไม่เปิดให้อุปกรณ์ภายนอกเชื่อมต่อเครือข่ายไร้สายของโรงพยาบาลได้อย่างอิสระ ยกเว้นมีการร้องขอเป็นกรณีพิเศษ เช่น เกิดเหตุการณ์ที่มีหน่วยงานอื่นเข้ามา และต้องมีการประสานงานผ่านเครือข่ายไร้สาย โดยจะเปิดให้เชื่อมต่อเฉพาะบริเวณที่อนุญาตเท่านั้น

๖.๒. กรณีเจ้าหน้าที่มีความประสงค์จะใช้อุปกรณ์ภายนอกเข้ามาเชื่อมต่ออินเตอร์เน็ตและระบบเครือข่ายไร้สายให้นำสำเนาบัตรประจำตัวประชาชน มาลงทะเบียน เพื่อขอรับรหัสใช้งาน และรหัสผ่าน กับผู้ดูแลระบบ ซึ่งจะกำหนดให้ใช้งานได้ตลอดจนกว่าจะมีการยกเลิกจากผู้ดูแลระบบ

๖.๓. กรณีผู้รับบริการหรือบุคคลภายนอกมีความประสงค์จะใช้อุปกรณ์ภายนอกเข้ามาเชื่อมต่ออินเตอร์เน็ตและระบบเครือข่ายไร้สาย ให้มาติดต่อกับผู้ดูแลระบบ เพื่อรับรหัสใช้งานและรหัสผ่าน ซึ่งจะมีระยะเวลากำหนดให้ใช้งานได้ไม่เกิน ๑ วัน

๗. ระบบรักษาความปลอดภัยของเครื่องแม่ข่ายคอมพิวเตอร์ (Firewall)

๗.๑. กำหนดให้ผู้ดูแลระบบติดตั้งโปรแกรม Firewall สำหรับอุปกรณ์คอมพิวเตอร์ทุกเครื่องที่ใช้ในโรงพยาบาล โดยทุกเส้นทางการเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะถูกบล็อก โดย Firewall

๗.๒. ผู้ดูแลระบบมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ระเบียบปฏิบัติของโรงพยาบาล กฎหมาย พรบ.คอมพิวเตอร์ หรืออาจจะทำให้เกิดความเสียหายต่อความปลอดภัยของระบบสารสนเทศ และความเสียหายต่อองค์กร จนกว่าจะได้รับการแก้ไข

๘. การสำรองข้อมูล

๘.๑. กำหนดให้มีเครื่องคอมพิวเตอร์แม่ข่ายสำรอง ๑ ตัว กรณีเครื่องแม่ข่ายหลักเกิดปัญหา และกำหนดให้มีการอัพเดทระบบ และสำรองข้อมูลผู้รับบริการทุก ๑ วัน โดยตั้งเวลาให้เครื่องคอมพิวเตอร์ทำงานโดยอัตโนมัติ ดูแลให้กระบวนการเป็นไปตามผู้ดูแลระบบ

๘.๒. ข้อมูลที่มีความสำคัญจะเก็บรูปแบบเอกสารร่วมกับอิเล็กทรอนิกส์ ซึ่งได้แก่ ข้อมูลด้านการเงินการคลัง ข้อมูลเวชระเบียนผู้ป่วยนอก ข้อมูลเวชระเบียนผู้ป่วยใน จะมีห้องจัดเก็บเฉพาะ อนุญาตให้เข้าออกได้เฉพาะผู้ปฏิบัติงาน กำหนดทำลายเอกสารเมื่อมีอายุเกิน ๑๐ ปี

๘.๓. การทำลายเอกสารต้องทำหนังสือแจ้งไปที่กองจดหมายเหตุแห่งชาติ และเมื่อได้รับการอนุมัติ ต้องประชาสัมพันธ์ให้ทราบโดยทั่วกัน เป็นระยะเวลาไม่น้อยกว่า ๓๐ วัน จึงจะเผาทำลายได้

๘.๔. กรณีข้อมูลของผู้ใช้งานถูกลบหรือถูกทำลาย สามารถติดต่อผู้ดูแลระบบเพื่อทำการกู้คืน ซึ่งอาจจะไม่สามารถกู้คืนได้ทั้งหมด

๙. กล้องวงจรปิด

๙.๑ กำหนดให้เจ้าหน้าที่งานสารสนเทศ เป็นผู้ดูแลบำรุงรักษาระบบกล้องวงจรปิด (CCTV) ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งานทุกวัน เวลา ๐๙.๐๐ น.

๙.๒. ผู้ดูแลระบบเป็นผู้กำหนดสิทธิการเข้าถึงกล้องวงจรปิด โดยความเห็นชอบของผู้อำนวยการและคณะกรรมการบริหาร

๙.๓. เมื่อมีการขอดูข้อมูลจากระบบกล้องวงจรปิด (CCTV) จะต้องกรอกแบบฟอร์มการขอดูหรือขอข้อมูลจากระบบกล้องวงจรปิด (CCTV) โดยจะต้องผ่านการอนุมัติจากผู้อำนวยการโรงพยาบาล คณะกรรมการบริหาร ผู้ดูแลระบบ ทั้งนี้ขึ้นอยู่กับเหตุการณ์หรือสถานการณ์เป็นกรณีไป

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ได้กำหนดขึ้นมาเพื่อเป็นมาตรการและแนวทางในการรักษาความมั่นคง ปลอดภัย ลดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ถือเป็นมาตรการความปลอดภัยของระบบสารสนเทศ และตามกฎหมาย พรบ.คอมพิวเตอร์ ซึ่งเจ้าหน้าที่ของโรงพยาบาลท่าวังผาและหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบสารสนเทศจะต้องปฏิบัติตามอย่างเคร่งครัด

จึงประกาศมาให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๗

(นายมงคล ลัคนาเลิศ)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลท่าวังผา