ประกาศโรงพยาบาลปากพนัง

เรื่อง นโยบายความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

๑. หลักการและเหตุผล เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปากพนัง มีความมั่นคงปลอดภัย (Security) เชื่อถือได้ (Reliability) และมีความพร้อมใช้ (Availability) ในการให้บริการทางการแพทย์ การบริหารจัดการข้อมูลภายในโรงพยาบาลปากพนัง และการเชื่อมโยงข้อมูลระหว่างโรงพยาบาลภายใต้สังกัดกระทรวงสาธารณสุข รวมทั้งเพื่อคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยและบุคลากรให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. วัตถุประสงค์

๑. เพื่อป้องกันความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับข้อมูลของผู้ป่วย และระบบการใช้งานภายในโรงพยาบาลปากพนัง

๒. เพื่อกำหนดแนวปฏิบัติให้บุคลากรภายในโรงพยาบาลปากพนัง ใช้งานระบบคอมพิวเตอร์ภายในหน่วยงานและระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย

๓. เพื่อให้สามารถกู้คืนระบบที่ใช้งานและข้อมูลได้ทันท่วงทีหากเกิดเหตุฉุกเฉิน

๓. ขอบเขตการบังคับใช้ นโยบายนี้ครอบคลุมถึงระบบเครือข่ายเครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์ลูกข่าย (Computer) อุปกรณ์พกพา (NoteBook , Tablet , โทรศัพท์) เป็นต้น ตลอดจนข้อมูลอิเล็กทรอนิกส์ทั้งหมด และบุคลากรทุกคนของโรงพยาบาลปากพนัง รวมถึงบุคคลภายนอกที่เข้ามาปฏิบัติงานในโรงพยาบาลปากพนัง

๔. แนวทางปฏิบัติ (Policy Guidelines)

๔.๑ การควบคุมการเข้าถึง (Access Control)

- **รหัสผ่าน (Password) :** บุคลากรต้องตั้งรหัสผ่านที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร ประกอบด้วยตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข อักขระพิเศษ และต้องเปลี่ยนรหัสผ่านทุก ๙๐ วัน (ห้ามบอกรหัสผ่านแก่ผู้อื่นโดยเด็ดขาด)
- **สิทธิ์การใช้งาน :** กำหนดสิทธิ์การเข้าถึงข้อมูลตามความจำเป็นของตำแหน่งและหน้าที่การทำงาน (Need-to-Know Basis) เมื่อบุคลากรลาออกหรือย้ายสถานที่ทำงาน ต้องดำเนินการระงับสิทธิ์การเข้าถึงข้อมูลต่างๆ ภายในองค์กรทันที
- **การล็อกหน้าจอ :** ต้องล็อกหน้าจอคอมพิวเตอร์ (Log off / Lock Screen) ทุกครั้งที่ไม่ใช้งาน หรือใช้งานเสร็จเรียบร้อยแล้ว

๔.๒ ความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย

- **ซอฟต์แวร์ลิขสิทธิ์ :** ห้ามติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ หรือโปรแกรมที่ไม่เกี่ยวข้องกับการทำงานลงในเครื่องคอมพิวเตอร์ทุกเครื่องของโรงพยาบาลปากพนัง
- **Antivirus :** เครื่องคอมพิวเตอร์ทุกเครื่องต้องติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ

- **การเชื่อมต่ออุปกรณ์ภายนอก :** ระมัดระวังการเสียบ Flash Drive หรือ External Hard Disk จากภายนอก ต้องสแกนไวรัสก่อนใช้งานทุกครั้ง
- **Wi-Fi โรงพยาบาลปากพนัง :** แยกวงเครือข่ายระหว่างเจ้าหน้าที่ (Staff) และผู้รับบริการ (Guest) ออกจากกันอย่างชัดเจน

๔.๓ การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy & PDPA)

- **ข้อมูลผู้ป่วย :** ข้อมูลเวชระเบียนและประวัติการรักษาถือเป็นข้อมูลอ่อนไหว ห้ามนำข้อมูลผู้ป่วยไปเผยแพร่ในสื่อสังคมออนไลน์ (Social Media) ทุกช่องทาง หรือส่งต่อผ่านแอปพลิเคชั่น แชทสาธารณะ (เช่น LINE) โดยไม่มีมาตรการเข้ารหัสหรือปกปิดตัวตน
- **การส่งออกข้อมูล :** การนำข้อมูลออกจากโรงพยาบาลปากพนัง เพื่อการวิจัยหรือส่งต่อหน่วยงานอื่น ต้องได้รับการอนุมัติจากผู้อำนวยการโรงพยาบาลปากพนังและมีการทำลายชื่อ (Anonymization) ก่อนทุกครั้ง

๔.๔ การสำรองและกู้คืนข้อมูล (Backup & Recovery)

- งานคอมพิวเตอร์ต้องทำการสำรองข้อมูลสำคัญ (Backup) เป็นประจำทุกวัน (Daily) และทุกสัปดาห์ (Weekly)
- ต้องมีการทดสอบการกู้คืนข้อมูล (Restore Test) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าข้อมูลที่ทำการสำรองไว้สามารถนำกลับมาใช้งานได้จริง

๕. การตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Incident Response)

หากพบเหตุผิดปกติ เช่น เครื่องติดไวรัส เรียกค่าไถ่ (Ransomware) หรือข้อมูลรั่วไหล ให้ปฏิบัติดังนี้

- **หยุด :** ตัดการเชื่อมต่ออินเทอร์เน็ต/เครือข่ายทันที (ถอดสาย LAN หรือปิด Wi-Fi) ห้ามปิดเครื่อง
- **แจ้ง :** แจ้งผู้ดูแลระบบ (Admin) หรือหัวหน้ากลุ่มงานสุขภาพดิจิทัลทันที
- **บันทึก :** ถ่ายภาพหน้าจอ หรือจดบันทึกอาการที่พบเพื่อเป็นหลักฐาน

๖. บทลงโทษ

ผู้ใดฝ่าฝืนนโยบายฉบับนี้ จนเป็นเหตุให้เกิดความเสียหายแก่โรงพยาบาลปากพนัง หรือข้อมูลผู้ป่วยรั่วไหล จะถูกพิจารณาโทษทางวินัยตามระเบียบของโรงพยาบาลปากพนัง และอาจต้องรับโทษตามกฎหมายที่เกี่ยวข้อง

จึงประกาศให้ทราบและถือปฏิบัติโดยทั่วกัน

ทราบ/อนุมัติ

(นายสมเกียรติ วรยุทธการ)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลปากพนัง