ประกาศโรงพยาบาลวาปีปทุม

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ของโรงพยาบาลวาปีปทุม เป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัย และสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงนโยบายและมาตรฐานความปลอดภัยของกระทรวงสาธารณสุข

โรงพยาบาลวาปีปทุม จึงขอประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้บุคลากรและหน่วยงานที่เกี่ยวข้องถือปฏิบัติ ดังนี้

ข้อ ๑ การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management) ให้มีการจัดทำทะเบียนคุมอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ (Asset Inventory) ของหน่วยงาน และตรวจสอบสถานะให้เป็นปัจจุบัน รวมถึงบริหารจัดการให้มีการใช้ซอฟต์แวร์ที่ถูกลิขสิทธิ์และมีความปลอดภัย

ข้อ ๒ การควบคุมการเข้าถึงระบบ (Access Control) ๒.๑ กำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศตามความจำเป็นของหน้าที่ความรับผิดชอบ (Least Privilege) ๒.๒ กำหนดให้ผู้ใช้งานต้องตั้งรหัสผ่าน (Password) ที่มีความมั่นคงปลอดภัย โดยมีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร และประกอบด้วยอักขระที่หลากหลาย ๒.๓ สำหรับผู้ดูแลระบบ (Administrator) และการเข้าถึงจากภายนอกเครือข่าย (VPN) ต้องมีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: ๒FA/MFA)

ข้อ ๓ การปกป้องและคุ้มครองข้อมูล (Data Protection) ๓.๑ ให้มีการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัส (Antivirus/EDR) บนเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายอย่างสม่ำเสมอ ๓.๒ ให้มีการสำรองข้อมูล (Backup) ที่สำคัญอย่างน้อยวันละ ๑ ครั้ง และจัดเก็บตามหลักการ ๓-๒-๑ เพื่อให้พร้อมกู้คืนข้อมูลได้เมื่อเกิดเหตุฉุกเฉิน

ข้อ ๔ การบริหารจัดการช่องโหว่ (Vulnerability Management) ให้มีการประเมินความเสี่ยง ตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งดำเนินการปรับปรุงแก้ไข (Patch) ระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันปัจจุบัน เพื่อลดความเสี่ยง

ข้อ ๕ การเฝ้าระวังและการรับมือภัยคุกคาม (Monitoring & Incident Response) ๕.๑ ให้มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log files) ไม่น้อยกว่า ๙๐ วัน ตามกฎหมาย ๕.๒ ให้มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (BCP) และแผนกู้คืนระบบ (DRP) พร้อมทั้งมีการซ้อมแผนอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ การพัฒนาบุคลากร (Personnel Development) ส่งเสริมและสนับสนุนให้บุคลากรได้รับการอบรม สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) และการคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ให้เจ้าหน้าที่ทุกคนตระหนักและถือปฏิบัติตามประกาศนี้อย่างเคร่งครัด เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อระบบสารสนเทศของทางราชการ

ประกาศ ณ วันที่ ๑๒ มกราคม พ.ศ. ๒๕๖๙

(นางเบญจพร อินทกรอุดม)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)
รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลวาปีปทุม