



ประกาศโรงพยาบาลปราสาท
เรื่อง นโยบายการใช้งานเทคโนโลยีสารสนเทศที่เหมาะสม
(Acceptable Use Policy - AUP)

โรงพยาบาลปราสาท ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และความปลอดภัยไซเบอร์ จึงได้จัดทำนโยบายการใช้งานเทคโนโลยีสารสนเทศที่เหมาะสม (Acceptable Use Policy - AUP) ฉบับนี้ขึ้น เพื่อกำหนดหลักเกณฑ์ แนวทาง และมาตรการในการใช้งานระบบสารสนเทศของทุกภาคส่วนที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาล เพื่อให้การดำเนินงานด้านการรักษาความปลอดภัยสารสนเทศของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพ สอดคล้องตามกฎหมาย และเป็นมาตรฐานเดียวกันทั้งองค์กร

โรงพยาบาลปราสาทจึงกำหนดนโยบายการใช้งานเทคโนโลยีสารสนเทศที่เหมาะสม ดังต่อไปนี้

๑. วัตถุประสงค์

เพื่อให้บุคลากรใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศของโรงพยาบาลอย่างถูกต้อง ปลอดภัยและไม่ผิดกฎหมาย ตลอดจนป้องกันความเสียหายต่อระบบและชื่อเสียงของโรงพยาบาล

๒. ขอบเขต

บังคับใช้กับบุคลากรทุกประเภท ข้าราชการ พนักงาน ลูกจ้าง นักศึกษาฝึกงาน และบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งานระบบของโรงพยาบาล

๓. ข้อปฏิบัติในการใช้งานบัญชีผู้ใช้งาน (User Account) และ การกำหนดรหัสผ่าน (Password)

๓.๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งานต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งานของตนเองจากเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๓.๒ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อผู้บุคคลอื่น ห้ามโอนหรือจำหน่ายจ่ายแจกให้กับผู้อื่น

๓.๓ ผู้ใช้งานต้องลงบันทึกการเข้าใช้ (Login) โดยบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๓.๔ รหัสผ่านควรมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยผสมกันระหว่างตัวเลขและตัวอักษรภาษาอังกฤษที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักษรพิเศษ (เช่น @ # \$ %) และสัญลักษณ์ต่าง ๆ ด้วย

๓.๕ ไม่ควรกำหนดรหัสผ่านจากข้อมูลส่วนตัว เช่น ชื่อหรือนามสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ หรือวันเดือนปีเกิด เป็นต้น

๓.๖ เมื่อผู้ใช้งานได้รับรหัสผ่านจากระบบสารสนเทศหรือได้รับจากผู้ดูแลระบบ ให้ทำการเปลี่ยนรหัสผ่านทันทีเมื่อใช้งานระบบครั้งแรก และควรทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอเหตุว่าอาจรั่วไหล

๓.๗ ไม่ทำการบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ หรือในรูปแบบอื่น ๆ ที่ไม่ได้ป้องกันการเข้าถึง

๔. การใช้งานอินเทอร์เน็ตและโซเชียลมีเดีย

๔.๑ ห้ามเข้าถึงเว็บไซต์ที่ผิดกฎหมาย, เว็บไซต์ลามกอนาจาร หรือเว็บไซต์ที่มีการเล่นการพนัน

๔.๒ ห้ามโพสต์หรือแชร์ข้อมูลที่เป็นความลับของโรงพยาบาล หรือข้อมูลส่วนบุคคลของผู้ป่วยลงในโซเชียลมีเดียโดยเด็ดขาด

๔.๓ ห้ามใช้ช่องทางออนไลน์ของโรงพยาบาลในการโพสต์ข้อมูลที่เข้าข่ายหมิ่นประมาท หรือสร้างความแตกแยก

๕. การใช้งานอุปกรณ์ (Hardware & Software)

๕.๑ ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ รวมถึงซอฟต์แวร์ที่ไม่เกี่ยวข้องกับภารกิจของหน่วยงาน เช่น เกมส์ หรือโปรแกรมชุดเตรียมดิจิทัล ทั้งนี้ การติดตั้งซอฟต์แวร์ใด ๆ ต้องได้รับอนุญาตจากหน่วยงานหรือผู้ดูแลระบบก่อนดำเนินการ

๕.๒ กรณีนำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) มาเชื่อมต่อกับระบบเครือข่ายของโรงพยาบาล ต้องได้รับอนุญาตจากผู้มีอำนาจและต้องมีการติดตั้งโปรแกรมป้องกันไวรัสหรือระบบป้องกันภัยคุกคามที่เป็นปัจจุบัน

๕.๓ ให้ใช้ความระมัดระวังในการเชื่อมต่อหรือใช้งานสื่อบันทึกข้อมูลแบบพกพา เช่น USB Drive เพื่อป้องกันความเสี่ยงจากมัลแวร์หรือโปรแกรมไม่พึงประสงค์ที่อาจส่งผลกระทบต่อระบบเครือข่ายภายในหน่วยงาน

๖. หน้าที่ในการเฝ้าระวังและรายงาน

บุคลากรมีหน้าที่รายงานเมื่อพบความผิดปกติของระบบ หรือพบพฤติกรรมที่น่าสงสัยว่าอาจเกิดภัยคุกคามไซเบอร์ (Phishing Email, Ransomware)

๗. บทลงโทษ

การฝ่าฝืนนโยบายนี้อาจได้รับบทลงโทษทางวินัยตามระเบียบของทางราชการ และอาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๙

(นางสาวชอุษา มหรรทศนพงศ์)

ผู้อำนวยการโรงพยาบาลปราสาท