# นโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลท่ากระดานดำเนินการอย่างเหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัย รวมถึงสามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในลักษณะที่ไม่เหมาะสม รวมถึงการคุกคามจากภัยต่าง ๆ ที่อาจส่งผลกระทบต่อโรงพยาบาล ทีมงานด้านระบบสารสนเทศจึงได้จัดทำแนวทางในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยี โดยอิงตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งแบ่งออกเป็น ๘ หมวด ดังนี้

**หมวด ๑ การพิสูจน์ตัวตน (Accountability, Identification and Authentication)**

**๑.** ผู้ใช้งานมีหน้าที่ในการป้องกันและรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานเป็นของตนเอง ห้ามใช้ร่วมกับผู้อื่นและห้ามเผยแพร่รหัสผ่านให้ผู้อื่นทราบ

**๒.** ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีผู้ใช้งานของตน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

**๓.** ผู้ใช้งานต้องตั้งรหัสผ่านให้มีความเฉพาะเพื่อความปลอดภัย

**๔.** ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๖๐ วัน หรือเมื่อได้รับการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

**๕.** ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศของโรงพยาบาล หากมีปัญหาในการพิสูจน์ตัวตน เช่น รหัสผ่านถูกล็อค ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

**๕.๑** การใช้งานอินเทอร์เน็ตต้องพิสูจน์ตัวตนและมีการบันทึกข้อมูลที่สามารถบ่งบอกตัวตนได้

**๕.๒** คอมพิวเตอร์ทุกประเภทต้องพิสูจน์ตัวตนก่อนเข้าถึงระบบปฏิบัติการ

**๕.๓** การใช้งานระบบคอมพิวเตอร์จากอุปกรณ์อื่น ๆ ในเครือข่าย เช่น แท็บเล็ต ไอแพด และโทรศัพท์มือถือ เป็นต้น

**๕.๔** เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องล็อคหน้าจอทุกครั้งและพิสูจน์ตัวตนก่อนใช้งานในภายหลัง

**๕.๕** คอมพิวเตอร์ทุกเครื่องต้องตั้งเวลาพักหน้าจอ (Screen saver) ไว้ที่อย่างน้อย ๕ นาที

**หมวด ๒ การบริหารจัดการทรัพย์สิน (Assets Management)**

**๑.** ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลโดยไม่ได้รับอนุญาต

**๒.** ห้ามนำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่ายโดยไม่ได้รับอนุญาต

**๓.** ห้ามเชื่อมต่อเครื่องมือหรืออุปกรณ์อื่น ๆ กับเครื่องแม่ข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

**๔.** ห้ามใช้หรือลบแฟ้มของผู้อื่นไม่ว่ากรณีใด ๆ

**๕.** ห้ามคัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต

**๖.** ผู้ใช้งานต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลมอบให้เสมือนเป็นทรัพย์สินของตนเอง

**๗.** กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลทรัพย์สินของโรงพยาบาลตามที่ได้รับมอบหมาย

**๘.** ผู้ใช้งานต้องชดใช้ค่าเสียหายหากทรัพย์สินชำรุดหรือสูญหายเนื่องจากความประมาท

**๙.** ห้ามให้ผู้อื่นยืมคอมพิวเตอร์หรือโน้ตบุ๊กเว้นแต่ได้รับอนุญาต

**๑๐.** ทรัพย์สินและระบบสารสนเทศที่โรงพยาบาลจัดเตรียมไว้ให้ใช้งานต้องใช้ในกิจกรรมของโรงพยาบาลเท่านั้น

**๑๑.** ความเสียหายใด ๆ ที่เกิดจากการละเมิดในข้อ ๑๐ ถือเป็นความผิดส่วนบุคคล

**หมวด ๓ การบริหารจัดการข้อมูลองค์กร (Corporate Management)**

**๑.** ผู้ใช้งานต้องตระหนักถึงการใช้งานข้อมูลของโรงพยาบาลและข้อมูลของบุคคลภายนอก

**๒.** ข้อมูลภายในทรัพย์สินของโรงพยาบาลถือเป็นทรัพย์สินของโรงพยาบาลห้ามเผยแพร่ เปลี่ยนแปลงหรือทำลายโดยไม่ได้รับอนุญาต

**๓.** ผู้ใช้งานต้องมีส่วนร่วมในการปกป้องข้อมูลของโรงพยาบาลจากการสูญเสียหรือการใช้งานที่ผิด

**๔.** ผู้ใช้งานต้องปกป้องรักษาความลับและความถูกต้องของข้อมูล

**๕.** ผู้ใช้งานมีสิทธิ์ในการเก็บรักษาและปกป้องข้อมูลส่วนบุคคลตามที่เห็นสมควร โรงพยาบาลจะสนับสนุนและเคารพสิทธิส่วนบุคคล

**หมวด ๔ การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)**

**๑.** ผู้ใช้งานมีสิทธิ์ในการพัฒนาโปรแกรมหรือฮาร์ดแวร์ แต่ต้องไม่ทำลายกลไกรักษาความปลอดภัยของระบบ

**๒.** ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่ได้รับอนุญาต

**๓.** ห้ามใช้โปรแกรมออนไลน์เพื่อความบันเทิงระหว่างปฏิบัติงาน

**๔.** ห้ามใช้ทรัพยากรของโรงพยาบาลเพื่อเผยแพร่ข้อมูลที่ขัดต่อศีลธรรม

**๕.** ห้ามใช้ทรัพย์สินของโรงพยาบาลเพื่อหาประโยชน์ทางการค้า

**๖.** ห้ามดักข้อมูลในเครือข่ายระบบสารสนเทศของโรงพยาบาล

**๗.** ห้ามรบกวนหรือทำลายระบบสารสนเทศของโรงพยาบาล

**๘.** ห้ามใช้ระบบสารสนเทศของโรงพยาบาลในการควบคุมระบบภายนอกโดยไม่ได้รับอนุญาต

**หมวด ๕ การปฏิบัติตามกฎหมายข้อบังคับ (Law and Compliance)**

**๑.** ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายและระเบียบของโรงพยาบาลอย่างเคร่งครัด หากมีการกระทำผิดถือเป็นความผิดส่วนบุคคล

**หมวด ๖ ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and Intellectual Property)**

**๑.** โรงพยาบาลให้ความสำคัญต่อทรัพย์สินทางปัญญา ห้ามติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

**๒.** ห้ามติดตั้ง ถอดถอน หรือทำสำเนาซอฟต์แวร์เพื่อใช้งานที่อื่น

**หมวด ๗ การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)**

**๑.** คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตระบบปฏิบัติการตามที่กำหนด

**๒.** ข้อมูลที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสก่อนนำมาใช้งาน

**๓.** ผู้ใช้งานต้องทำการอัพเดตข้อมูลเพื่อป้องกันความเสียหาย

**๔.** เมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งผู้ดูแลระบบ

**๕.** หากพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ห้ามเชื่อมต่อกับเครือข่ายและต้องแจ้งผู้ดูแลระบบ

**๖.** ห้ามลักลอบทำสำเนาข้อมูลหรือทำลายข้อมูลที่เป็นทรัพย์สินของโรงพยาบาล

**๗.** ห้ามเผยแพร่ไวรัสหรือโปรแกรมอันตรายที่อาจสร้างความเสียหายต่อโรงพยาบาล

**หมวด ๘ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail)**

**๑.** ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy) ดังนี้

**๑.๑** ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

**๑.๒** ควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

**๑.๓** ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) ของผู้อื่นเพื่ออ่านหรือรับ ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (Email) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (Email) ของตน

**๑.๔** หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (Email) เสร็จสิ้น ควรลงบันทึกออก (Logout) ทุกครั้ง