มาตรฐานด้านการสนับสนุนและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ

(Service Level Agreement and Work Instruction)

กลุ่มงานสุขภาพดิจิตอล

นโยบายความมั่นคงปลอดภัยสารสนเทศ

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ**โรงพยาบาลทุ่งฝน** จัดทำขึ้นเพื่อใช้เป็นกรอบแนวทางในการยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยอ้างอิงตามกรอบมาตรฐานสากล ISO/IEC 27001 แบ่งออกเป็น 2 กลุ่มหลัก คือ

1. **กลุ่มผู้ใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่าย**
2. **กลุ่มผู้ดูแลระบบสารสนเทศและเครือข่าย**

1. กลุ่มผู้ใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่าย

1.1 นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ 1 ผู้ใช้งานมีหน้าที่ป้องกันและรักษาบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับส่วนบุคคล

ข้อ 2 กำหนดให้รหัสผ่านมีอายุการใช้งาน 30 วัน และผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านใหม่ทุก 30 วัน

ข้อ 3 ผู้ใช้งานต้องทำการพิสูจน์ตัวตน (Authentication) ทุกครั้งก่อนเข้าใช้งานระบบเครือข่ายหรือระบบสารสนเทศของ**โรงพยาบาลทุ่งฝน**

ข้อ 4 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดขึ้นผ่านบัญชีผู้ใช้งานของตนเองในทุกกรณี

ข้อ 5 ห้ามผู้ใช้งานเข้าภายในห้องควบคุมคอมพิวเตอร์และเครือข่าย (Server Room) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 6 ห้ามกระทำการใดๆ เพื่อดักจับข้อมูล (Sniffing/Intercepting) ไม่ว่าจะเป็นข้อความหรือรูปแบบอื่นใดในเครือข่ายสารสนเทศของโรงพยาบาล

ข้อ 7 ห้ามลักลอบใช้งานบัญชี (User) และรหัสผ่าน (Password) ของผู้อื่นโดยเด็ดขาด

ข้อ 8 ห้ามติดตั้งอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เครือข่ายทุกประเภทเพื่อแทรกแซงระบบสารสนเทศของโรงพยาบาล โดยไม่ได้รับอนุญาตหรือขึ้นทะเบียนอย่างถูกต้อง

ข้อ 9 หากพบว่าเครื่องคอมพิวเตอร์ติดไวรัสหรือมัลแวร์ ผู้ใช้งานต้องตัดการเชื่อมต่อจากระบบเครือข่ายทันทีและรีบแจ้งผู้ดูแลระบบ

ข้อ 10 ห้ามเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่ก่อให้เกิดความเสียหายต่อทรัพย์สินของโรงพยาบาล

1.2 นโยบายความมั่นคงปลอดภัยของเครือข่ายและระบบเครื่องแม่ข่าย

ข้อ 1 ห้ามใช้ทรัพยากร เครื่องแม่ข่าย หรืออุปกรณ์ของโรงพยาบาลเพื่อเผยแพร่ข้อมูลที่ขัดต่อศีลธรรม กฎหมาย หรือความมั่นคงของประเทศ

ข้อ 2 ห้ามนำอุปกรณ์ส่วนตัวมาต่อพ่วงกับระบบเครือข่ายที่อาจส่งผลกระทบต่อระบบ หากมีความจำเป็นต้องใช้เครื่องคอมพิวเตอร์ส่วนตัวปฏิบัติงาน ต้องผ่านการตรวจสอบและขึ้นทะเบียนระบบกับเจ้าหน้าที่ไอที

1.3 นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล

ข้อ 1 ผู้ใช้งานควรทำการสำรองข้อมูลสำคัญ (Backup) ในเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบอย่างสม่ำเสมอ

ข้อ 2 ห้ามคัดลอกหรือสำรองข้อมูลที่เป็นความลับของโรงพยาบาลเพื่อนำไปเผยแพร่โดยไม่ได้รับอนุญาต

1.4 นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wi-Fi)

ข้อ 1 ผู้ใช้งานต้องลงทะเบียนอุปกรณ์กับงานเทคโนโลยีสารสนเทศก่อน จึงจะสามารถใช้งานระบบเครือข่ายไร้สายได้

ข้อ 2 ห้ามติดตั้งอุปกรณ์กระจายสัญญาณ (Access Point) ส่วนตัวในพื้นที่โรงพยาบาลโดยไม่ได้รับอนุญาต

1.5 นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต

ข้อ 1 ห้ามใช้อินเทอร์เน็ตของโรงพยาบาลเพื่อแสวงหาประโยชน์เชิงพาณิชย์ส่วนบุคคล หรือเข้าถึงเว็บไซต์ที่ไม่เหมาะสมและขัดต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์

ข้อ 2 การเข้าใช้งานอินเทอร์เน็ตต้องมีการพิสูจน์ตัวตนและบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ตามกฎหมาย

ข้อ 3 การใช้งานสื่อสังคมออนไลน์หรือกระดานสนทนา ห้ามเสนอความคิดเห็นที่ให้ร้ายหรือทำให้โรงพยาบาลเสียชื่อเสียง และห้ามเปิดเผยความลับของหน่วยงาน

ข้อ 4 การส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่มีเนื้อหาเป็นความลับ ไม่ควรระบุความสำคัญหรือเนื้อหาลับในหัวข้อจดหมาย

ข้อ 5 ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลภายในที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

1.6 นโยบายการบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ 1 สิทธิ์การเข้าถึงระบบจำกัดเฉพาะผู้บริหาร แพทย์ บุคลากร และบุคคลที่ได้รับอนุญาตเท่านั้น

ข้อ 2 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรใช้การเข้ารหัส (Encryption) ตามมาตรฐานสากล เช่น SSL หรือ VPN (หากมีการติดตั้งในอนาคต)

ข้อ 3 บุคลากรที่พ้นสภาพการเป็นเจ้าหน้าที่ จะถูกยกเลิกสิทธิ์การเข้าใช้งาน Username และ Password ทันที

1.7 การฝ่าฝืนและการลงโทษ

ข้อ 1 ผู้ฝ่าฝืนจะถูกระงับหรือยกเลิกบัญชีผู้ใช้งานทันที

ข้อ 2 พิจารณาโทษทางวินัยตามระเบียบของทางราชการ

ข้อ 3 หากการฝ่าฝืนก่อให้เกิดความผิดตามกฎหมาย (พ.ร.บ. คอมพิวเตอร์ฯ) โรงพยาบาลจะดำเนินคดีทั้งทางแพ่งและทางอาญา

ข้อ 4 โรงพยาบาลมีสิทธิ์เข้าตรวจสอบข้อมูลในเครื่องคอมพิวเตอร์หากมีเหตุอันควรสงสัยว่ามีการฝ่าฝืนนโยบาย

2. กลุ่มผู้ดูแลระบบสารสนเทศและเครือข่าย

2.1 นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ 1 ผู้ดูแลระบบมีอำนาจระงับการใช้งานเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ 2 ห้ามเปิดเผยข้อมูลความลับของระบบ เช่น รหัสผ่านอุปกรณ์ หรือโครงสร้างทางเทคนิคที่อาจก่อให้เกิดช่องโหว่

ข้อ 3 ผู้ดูแลระบบต้องผ่านการพิสูจน์ตัวตนในการเข้าใช้งานระบบเช่นเดียวกับผู้ใช้งานทั่วไป

ข้อ 4 ต้องจัดทำบันทึกการเปลี่ยนแปลง (Change Log) ทุกครั้งที่มีการตั้งค่าหรือแก้ไขอุปกรณ์และเครื่องแม่ข่าย

2.2 นโยบายความมั่นคงปลอดภัยของเครือข่ายและระบบเครื่องแม่ข่าย

ข้อ 1 กำหนดค่าการให้บริการ (Service) บนเครื่องแม่ข่ายเฉพาะพอร์ต (Port) ที่จำเป็นต่อการใช้งานเท่านั้น

ข้อ 2 การเข้าถึงอุปกรณ์ Server ต้องมีมาตรฐานการรักษาความปลอดภัยขั้นสูง

ข้อ 3 จัดทำและปรับปรุงแผนผังระบบเครือข่าย (Network Diagram) ให้เป็นปัจจุบันอยู่เสมอ

ข้อ 4 สำรองไฟล์กำหนดค่า (Configuration File) ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ

ข้อ 5 ตรวจสอบและรายงานสถานะความผิดปกติของอุปกรณ์เครือข่ายและเครื่องแม่ข่ายต่อผู้บริหารตามวงรอบ

2.3 นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล

ข้อ 1 จัดทำขั้นตอนการสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ที่ชัดเจนแยกตามระบบสารสนเทศ

ข้อ 2 สื่อบันทึกข้อมูลสำรองต้องมีการระบุชื่อระบบ วันที่ และผู้รับผิดชอบอย่างชัดเจน และควรจัดเก็บไว้ในสถานที่ที่ปลอดภัยหรือแยกจากอาคารหลัก (Off-site Storage) รวมถึงต้องมีการทดสอบการกู้คืนข้อมูลอย่างต่อเนื่อง

2.4 นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (สำหรับผู้ดูแลระบบ)

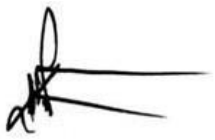
ข้อ 1 ควบคุมสัญญาณ Wi-Fi ไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานโดยไม่จำเป็น

ข้อ 2 ใช้มาตรการควบคุมสิทธิ์ผ่าน Mac Address ร่วมกับการพิสูจน์ตัวตนด้วย Username และ Password

ข้อ 3 ควบคุมและตรวจสอบไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาต เข้าถึงระบบเครือข่ายภายในและฐานข้อมูลของโรงพยาบาลผ่านเครือข่ายไร้สายโดยเด็ดขาด

ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ประกาศ ณ วันที่ 18 ธันวาคม 2566 เป็นต้นไป



(นายฉัตรชัย ประทุมทิพย์)

ผู้อำนวยการโรงพยาบาลทุ่งฝน