แนวทางปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๑.๑ กำหนดพื้นที่ควบคุมเพื่อจัดการการเข้าออกเฉพาะบุคคลที่ได้รับอนุญาตในการปฏิบัติงานในพื้นที่ควบคุม เพื่อป้องกันภัยคุกคามจากภายนอก รวมถึงการบริหารจัดการระบบสารสนเทศ, อุปกรณ์สนับสนุนการปฏิบัติงาน, และการบำรุงรักษาอุปกรณ์อย่างเหมาะสม

๒. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑ ผู้ดูแลระบบต้องตรวจสอบการอนุมัติและกำหนดรหัสผ่าน รวมถึงการลงทะเบียนผู้ใช้งาน เพื่อให้เฉพาะผู้ที่มีสิทธิ์ (User Authentication) เท่านั้นที่สามารถเข้าถึงระบบได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์

๒.๒ ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับความลับของผู้ใช้งาน รวมถึงการทบทวนสิทธิ์การใช้งานและการตรวจสอบการละเมิดความปลอดภัย

๒.๓ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อให้งานอินเทอร์เน็ตต้องผ่านระบบรักษาความปลอดภัยที่จัดเตรียมไว้ เช่น Firewall, IPS/IDS, Proxy และการตรวจสอบไวรัสคอมพิวเตอร์

๒.๔ ผู้ดูแลระบบต้องควบคุมการเข้าใช้งานจากภายนอก (Remote Access) โดยการกำหนดสิทธิ์การควบคุม (Port) ที่ใช้เข้าสู่ระบบอย่างรัดกุม พร้อมการแสดงตนของผู้ใช้และการพิสูจน์ยืนยันตัวตน (Authentication)

๓. การใช้เครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

๓.๑ กำหนดให้ใช้เครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของโรงพยาบาลท่ากระดาน รวมถึงโปรแกรมที่ใช้งานควรมีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับงานที่ปฏิบัติ

๓.๒ กำหนดให้ผู้ใช้งานต้องใช้ User และ Password ก่อนใช้งานเครื่อง รวมถึงการล็อกหน้าจอด้วยโปรแกรม Screen Saver ในระหว่างเวลาพักงาน หรือเมื่อหยุดการใช้เครื่องชั่วคราว

๓.๓ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลและกู้คืนข้อมูลบนสื่อเก็บข้อมูลที่มีความเหมาะสม และต้องเก็บรักษาไว้ในที่ปลอดภัย

๓.๔ การใช้คอมพิวเตอร์ส่วนตัวในโรงพยาบาลต้องแจ้งศูนย์คอมพิวเตอร์ทุกครั้งที่ต้องการใช้งานคอมพิวเตอร์ส่วนตัว

๔. การใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๔.๑ ผู้ดูแลระบบจะต้องกำหนดเฉพาะผู้ที่มีสิทธิ (User Authentication) จึงจะสามารถเชื่อมต่อระบบเพื่อใช้งานอินเทอร์เน็ตหรือจดหมายอิเล็กทรอนิกส์ได้

๔.๒ จัดให้มีระบบรักษาความปลอดภัยเพื่อตรวจสอบการใช้งานและภัยคุกคาม

๔.๓ กำหนดแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์อย่างถูกต้อง โดยไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่อาจสร้างปัญหาให้แก่ระบบหรือผู้ใช้อื่น

๔.๔ ในการติดต่อเรื่องงานราชการ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ของหน่วยงานหรือที่จัดเตรียมไว้ให้ใช้เท่านั้น ห้ามใช้ Free E-Mail

๔.๕ ต้องมีการเก็บข้อมูลการเข้าถึงระบบและข้อมูลจราจรทางคอมพิวเตอร์

๕. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๕.๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านและสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) และลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง พร้อมกำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสม เพื่อป้องกันไม่ให้บุคคลภายนอกที่ไม่เกี่ยวข้องหรือไม่ได้รับอนุญาตเข้าใช้งาน

๖. การป้องกันโปรแกรมไม่ประสงค์ดี

๖.๑ ผู้ดูแลระบบจะต้องตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่จะนำมาต่อกับระบบเครือข่ายของโรงพยาบาลท่ากระดาน เพื่อให้ติดตั้งโปรแกรมป้องกันไวรัส และผู้ใช้จะต้องตรวจสอบไวรัสคอมพิวเตอร์จากสื่อเก็บข้อมูลทุกชนิดก่อนนำมาใช้งานร่วมกับคอมพิวเตอร์หลัก

๗. สำรองข้อมูลสำคัญ

๗.๑ สำรองข้อมูลของโปรแกรม HOSXP แบบ Real-time ไปยังเครื่อง Back up โดยการสำรองแบบ Auto ทุกวัน เวลาเที่ยงคืนและตอน ๑๖.๓๐ น. มีระบบ Back up external โดยการ Back up ไฟล์ข้อมูลลง External Hard Drive ทุกวัน โดยเก็บนอกอาคารบริการ

แนวทางปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้ถูกกำหนดขึ้นเพื่อเป็นแนวทางในการรักษาความมั่นคงปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากร ทำให้สามารถดำเนินงานได้อย่างมั่นคงและปลอดภัย โดยเจ้าหน้าที่ของโรงพยาบาลท่ากระดานและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑ มีนาคม พ.ศ.๒๕๖๕

นายพิสุทธิ์ จรุงเรืองทรัพย์
นายแพทย์ชำนาญการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลท่ากระดาน