แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

(Access Control Policy)

ฉบับปรับปรุง

๑.วัตถุประสงค์

ตามที่ทางสำนักงานคณะกรรมการรักษาความมั่นคงปลอดไซเบอร์แห่งชาติ(สกมช.)(NCSA) ต้องการให้ภาครัฐมีการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัยไม่ให้เกิดผลกระทบต่อองค์กรหรือหน่วยงาน โดยจะต้องมีการบริหารจัดการระบบเครือข่ายที่มีความปลอดภัยทั้งผู้ใช้งานระบบและผู้ให้บริการระบบภายนอก ทางศูนย์คอมพิวเตอร์ฯ เล็งเห็นถึงความสำคัญของการใช้งานระบบสารสนเทศของโรงพยาบาลในปัจจุบันที่ต้องเป็นมาตรฐานและสร้างความเชื่อมั่นให้กับผู้ใช้งานระบบได้ จึงมีการปรับปรุงเนื้อหาบางส่วนของ“แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ(Access Control Policy)” เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานและป้องกันการบุกรุกหรือจากโปรแกรมประสงค์ร้าย(Malware)ที่จะสร้างความเสียหายแก่ข้อมูลทางการแพทย์หรือการทำงานระบบสารสนเทศและระบบเครือข่ายทำให้หยุดชะงัก รวมทั้งการวางมาตรการป้องกันให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายภายในของหน่วยงานได้ถูกต้อง

ทั้งนี้ ทาง ศูนย์คอมพิวเตอร์ฯ มีความตั้งใจที่จะทำให้ระบบสารสนเทศของโรงพยาบาลมีความปลอดภัย โดยการสร้างความตระหนักรู้ ความเข้าใจกับผู้ใช้งานระบบและผู้ใช้บริการร่วมกับระบบงานของโรงพยาบาล ให้สามารถปฏิบัติตามข้อกำหนดที่ระบุไว้ข้างต้น และหวังเป็นอย่างยิ่งว่าจะได้ความร่วมมือจากทุกท่านเป็นอย่างดี

๒.แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลพระมงกุฎเกล้า

๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ โรงพยาบาลพระมงกุฎเกล้ากำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงาน หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อเจ้าหน้าที่ศูนย์คอมพิวเตอร์กอ.รพ.รร.๖

๒.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจสอบการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิต่างๆและการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ หน่วยงานผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่โดยมีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆในการใช้เข้างานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่นระบบคอมพิวเตอร์โปรแกรมประยุกต์(Application),ระบบเครือข่ายไร้สาย (Wireless LAN),ระบบเครือข่ายอินเทอร์เน็ต(Network Internet),ระบบเครือข่ายอินทราเน็ท(Intranet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

๒.๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๒.๒.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๒.๓.๓ ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๒.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้ รหัสผู้ใช้งานต่างๆจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

๒.๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๒.๔.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๒.๔.๔ ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๒.๔.๕ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

เพื่อให้การควบคุมการเข้าถึงระบบปฏิบัติการโดยอยู่ภายใต้ข้อบังคับตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่๒)พ.ศ.๒๕๖๐ ทางโรงพยาบาลพระมงกุฎเกล้าจึงได้กำหนดข้อควรปฏิบัติในการใช้งานระบบของโรงพยาบาลร่วมกันดังนี้

๒.๓.๑ ผู้ใช้บริการจะต้องแจ้งชื่อขอผู้ใช้งานUser nameและรหัสผ่านPasswordสำหรับการเข้าถึงระบบปฏิบัติการของเครื่องหรืออุปกรณ์ที่ให้บริการก่อนการผ่านเข้าสู่ระบบงานของโรงพยาบาลให้กับทางศูนย์คอมพิวเตอร์โรงพยาบาลเป็นผู้อนุญาตในการเข้าถึงระบบของโรงพยาบาลทุกครั้ง

๒.๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นนำรหัสผู้ใช้งานUser nameและรหัสผ่านPassword เข้าสู่ระบบปฏิบัติการของเครื่องคอมพิวเตอร์, เครื่องแสดงผลการรักษาทางการแพทย์,เครื่องบันทึกไฟล์ ภาพวิดีโอระบบPACS และอุปกรณ์อื่นๆที่เชื่อมต่อเข้ากับระบบงานของโรงพยาบาล ก่อนได้รับการอนุญาตทุกครั้ง

๒.๓.๓ ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเพื่อทำการLOgหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้น เมื่อต้องการเข้าใช้งานทุกครั้งผู้ใช้บริการต้องใส่รหัสผ่านที่ปลอดภัยและเป็นส่วนตัวในการเข้าใช้งานผ่านระบบเสมอ

๒.๓.๔ ผู้ใช้บริการควรทำการLogout ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า ๓๐ นาที ถึง ๑ ชั่วโมง

๒.๓.๕ผู้ใช้บริการจะต้องรับรองว่าอุปกรณ์ของบริษัทได้ผ่านมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์เรียบร้อยหรือได้รับการตรวจสอบความปลอดภัยจากทางศูนย์คอมพิวเตอร์โรงพยาบาลแล้วเท่านั้นถึงจะมีสิทธิเชื่อมต่อเข้ากับระบบงานของโรงพยาบาล

๒.๓.๖ ผู้ใช้บริการจะต้องมีการรับรองมาตรฐานสากลสำหรับการจัดการความปลอดภัยของข้อมูล ISO/IEC27001เพื่อให้มั่นใจว่าระบบสารสนเทศของโรงพยาบาลจะเป็นความลับ รวมถึงจะต้องมีแผนการอัพเดทระบบป้องกันภายในของอุปกรณ์ที่เชื่อมต่อเข้ามายังระบบงานโรงพยาบาล เพื่อไม่ให้เกิดการแพร่จายของไวรัสคอมพิวเตอร์ที่มาจากมัลแวร์ (Malware) จนเข้าไปสู่ระบบงานของโรงพยาบาลได้

๒.๓.๗ หากผู้ดูแลระบบตรวจพบว่า มีกิจกรรมใดที่ทำให้เกิดความเสี่ยงไม่ว่าจากบุคคลหรือจากเครือข่ายภายนอก จนทำให้ระบบงานของโรงพยาบาลหยุดชะงักและเกิดความเสียหายต่อข้อมูลบางส่วนหรือทั้งหมด ทางผู้ใช้บริการหรือหน่วยงานผู้เป็นเจ้าของระบบจะต้องรับผิดชอบ และทางโรงพยาบาลจะใช้ข้อกฎหมายตามพรบ.ข้างต้นประกอบการดำเนินคดี ซึ่งจะเป็นตามระเบียบของการพิจารณาที่ทางโรงพยาบาลกำหนดต่อไป

พ.อ.

(ธนกร เทียนศรี)

หน.ศูนย์คอมพิวเตอร์ กอ.รพ.รร.๖