แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงักรวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเขาสุกิมมีดังนี้

๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ โรงพยาบาลเขาสุกิม กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์เทคโนโลยีสารสนเทศ

๒.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ โรงพยาบาลเขาสุกิม กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรงต่อไปนี้

๒.๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password)เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๒.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์(e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๒.๓.๓ ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๒.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๒.๔.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๒.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPNหรือ XML Encryption เป็นต้น

๒.๒.๔.๕ ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๒.๔.๖ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่นส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน๒.๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๓.๓ ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า ๑ ชม.

การรักษาความปลอดภัยและความลับ

การจัดเก็บเวชระเบียน ความปลอดภัย :

- เวชระเบียนผู้ป่วยนอก จัดเก็บเวชระเบียนแบ่งออกเป็น ๓ ระบบ คือ รูปแบบเอกสาร มีการใส่ปกแข็งในกลุ่มโรคเรื้อรัง เพื่อให้ง่ายต่อการค้นหา การ Scan เอกสารเพื่อป้องกันการชำรุด สูญหาย และข้อมูลอิเล็กทรอนิกส์ไฟล์ถูกเก็บรักษาใน Server HOSxP สืบค้นโดยใช้ HN, เลขบัตรประชาชน และชื่อ –นามสกุล
- เวชระเบียนผู้ป่วยใน จัดเก็บโดยการ Scan เอกสารเวชระเบียนจัดเก็บเป็นไฟล์อิเล็กทรอนิกส์ เพื่อป้องกันการชำรุดสูญหาย และจัดเก็บใส่ซองเอกสารสีน้ำตาลแยกรายปี มีห้องสำหรับเก็บเวชระเบียนผู้ป่วยใน มีกุญแจล็อคมิดชิดป้องกันการเข้าถึงจากผู้ไม่มีส่วนเกี่ยวข้อง
- การเข้าถึงข้อมูลภายในฐานข้อมูล มีการกำหนดรหัสในการเข้าถึงข้อมูลเป็นรายบุคคล ตามหน้าที่ภาระงาน หน่วยงานต้นสังกัด และระดับความลับของข้อมูล โดยมีการกำหนดสิทธิการใช้ข้อมูลของเจ้าหน้า เป็นรหัสที่เป็นความลับของแต่ละบุคคล
- เวชระเบียนถูกเก็บรักษาไว้ ๑๐ ปี โดยมีการจัดทำหนังสือขอทำลายเอกสาร และติดประกาศทำลายภายใน ๖๐ วัน

การรักษาความลับของข้อมูลในเวชระเบียน :

- เนื่องจากการจัดเก็บและการรักษาความลับข้อมูลของผู้ป่วยนอกทางอิเล็กทรอนิกส์ใช้โปรแกรม HOSxP มีความเสี่ยงต่อการเข้าถึงได้ง่าย โดยผู้ที่ไม่มีสิทธิ จึงมีการปรับปรุงการจัดเก็บข้อมูลอย่างเป็นระบบ ๑) รักษาความลับเป็นระดับตามหน้าที่การใช้งานของโปรแกรม ๒) ระบบการเข้าถึงโดย Username และ Password สำหรับ Login และ Logout อัตโนมัติ ๕ นาทีหากไม่ได้ใช้งาน ๓) เปลี่ยนทุก ๙๐ วัน โดยประกาศเป็นระเบียบปฏิบัติ ทำให้ระบบมีความน่าเชื่อถือ ปลอดภัย และไม่พบข้อร้องเรียนเรื่องการเข้าถึงข้อมูลผู้ป่วยจากบุคคลที่ไม่เกี่ยวข้อง
- การกำหนดสิทธิการเข้าถึงเวชระเบียน แบ่งสิทธิตามวิชาชีพ กลุ่มวิชาชีพที่ ๑ แพทย์ พยาบาล เภสัชกรสามารถเข้าถึงข้อมูลเวชระเบียนการรักษา กลุ่มวิชาชีพที่ ๒ สหสาขาวิชาชีพ และกลุ่มที่ ๓ สนับสนุนบริการ สามารถเข้าถึงเฉพาะข้อมูลที่มีส่วนเกี่ยวข้อง

- เวชระเบียนอิเล็กทรอนิกส์ ระบบเครือข่ายภายนอก (Internet) มีการรักษาความปลอดภัยโดยติดตั้งอุปกรณ์ป้องกันการบุกรุกเครือข่าย (Fire Wall) ระบบป้องกันผู้บุกรุก (IPS) ระบบตรวจจับไวรัส และสปายแวร์ (Antivirus/Antispyware) และกำหนด Identity-based ควบคุมแอพพลิเคชั่นและควบคุมการทำงานของการเข้าถึงระบบเครือข่ายแบบ Endpoint Network Control (ENC) เพื่อป้องกันภัยคุกคามระบบเว็บไซต์มีการควบคุมการใช้งานระบบอินเตอร์เน็ตในโรงพยาบาล โดยกำหนดรหัสผู้ใช้และรหัสผ่านเพื่อระบุตัวตนมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานอินเตอร์เน็ตในโรงพยาบาล
- เวชระเบียนผู้ป่วย HIV, OSCC จะแยก OPD Card ไว้กับผู้รับผิดชอบโดยตรง กำหนดสิทธิดูได้เฉพาะแพทย์ และที่ปรึกษา จะบันทึกผลสื่อสารเป็นรหัส Code เท่านั้น ในส่วนของโปรแกรมทำประวัติใหม่โดยใช้รหัสแทนชื่อ จัดเก็บประวัติการถูกกระทำ/ถูกทารุณทางเพศ ผลการตรวจทางห้องปฏิบัติการ ไว้ในตู้เฉพาะที่มีกุญแจล็อค และกำหนดผู้เข้าถึงเวชระเบียนดังกล่าวที่ชัดเจน ไม่พบอุบัติการณ์การเปิดเผยข้อมูลของผู้ใช้บริการจะปกปิด Visit ที่ผู้ป่วยมารับบริการโดยบุคคลที่ไม่เกี่ยวข้องกับการรักษาจะไม่สามารถมองเห็น Visit บริการนั้น จากการดำเนินการไม่พบข้อร้องเรียนเกี่ยวกับการเปิดเผยความลับของผู้ป่วย
-

การให้ผู้ป่วยเข้าถึงข้อมูลของตนในเวชระเบียน :

โรงพยาบาลมีนโยบายการขอเปิดเผยประวัติ โดยผู้ป่วยสามารถขอเปิดเผยประวัติ โดยยื่นคำร้องขอสำเนาเวชระเบียนด้วยตนเอง หรือมอบอำนาจแก่ญาติสายตรงยื่นคำร้องแทน