



แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

โรงพยาบาลเกาะกูด กำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงักรวมทั้งให้สามารถ ตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

๑. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑.๑ โรงพยาบาลเกาะกูดกำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้ดูแลระบบ

๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๑.๓ ผู้ดูแลระบบ มีการติดตั้งระบบบันทึก และติดตามการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๑.๔ ผู้ดูแลระบบมีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับการอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒. การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑ ผู้ดูแลระบบกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลเกาะกูด กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การกระทำความผิดตาม พรบ. การลาออก การโยกย้าย หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒ ผู้ดูแลระบบกำหนดการเข้าใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายภายใน เป็นต้น โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์อย่างสม่ำเสมอ

๒.๓ ผู้ดูแลระบบ บริหารจัดการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๓.๒ ส่งมอพรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๓.๓ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๔ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๓.๕ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการโรงพยาบาล หรือหัวหน้ากลุ่มงาน ประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับของข้อมูล

๒.๔.๑ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๔.๒ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลเช่น SSL VPN หรือ XML Encryption เป็นต้น

๒.๔.๓ กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๔.๔ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้บริการกรอกรหัสผ่านเครื่องในการเข้าใช้งานระบบปฏิบัติการของ เครื่องคอมพิวเตอร์ของหน่วยงาน

๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นรหัสผ่านของตนในการเข้าใช้เครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๓ ผู้ใช้บริการตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการลือคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๓.๔ ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า ๑ ชม.

ประกาศ ณ วันที่ ๑๖ มีนาคม พ.ศ. ๒๕๖๖

(นายณัฐภัทร ศรีอุดมพร)
นายแพทย์ปฏิบัติการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลเกาะกูด