นโยบายควบคุมการเข้าถึง

(Access Control Policy)

นโยบายควบคุมการเข้าถึง (Access Control Policy)

๑. **การกำหนดผู้รับผิดชอบภายในโรงพยาบาลบ้านคา** และ ร่วมกันพิจารณาออกข้อกำหนดในการเข้าถึงระบบ และ มีการประกาศใช้อย่างเป็นทางการ เช่น กำหนดสิทธิในการเข้าใช้งานในอุปกรณ์คอมพิวเตอร์,กำหนดสิทธิในการเข้าใช้งานระบบ

๒. **การเข้าถึงเครือข่าย และ บริการเครือข่าย (Access to networks and network services)** การกำหนดให้มีการพิจารณาสิทธิในการเข้าถึงข้อมูลของผู้ใช้โดยกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ , มีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม

๓. **การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)** วัตถุประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

๓.๑ **การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)**

- การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งานระบบสารสนเทศ และ ระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพต้องยกเลิกออกจากระบบทันที

๓.๒ **การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)**

- ผู้ดูแลระบบต้องมีกระบวนการกำหนดสิทธิ์ให้ครอบคลุมผู้ใช้งานให้ครบทุกประเภท และ ทุกการบริการของระบบสารสนเทศ

๓.๓ **การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)**

- ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบ

๓.๔ **การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)**

- ผู้ดูแลระบบต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้อย่างน้อยปีละ ๑ ครั้ง

๓.๕ **การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal of adjustment of access rights)**

- เมื่อเจ้าหน้าที่ เปลี่ยนแปลง ปรับเปลี่ยน โยกย้าย การทำงานหรือสัญญาสิ้นสุดการจ้าง ผู้ดูแลระบบต้องทำการถอดถอนหรือปรับปรุงสิทธิให้ถูกต้อง

๔. **หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)** วัตถุประสงค์ เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

นโยบาย

๔.๑ **การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ**
(Use of secret authentication information)

- ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศองค์กร การกำหนดการเปลี่ยนแปลง การยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย
- รหัสผ่าน ถือเป็นข้อมูลลับ และ เป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย
- ผู้ใช้งาน ต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งาน และ รหัสผ่านของตนทั้งหมด
- รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และ เปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้

๕. **การควบคุมการเข้าถึงระบบ (System and application access Control)** วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบสารสนเทศและข้อมูลบนระบบสารสนเทศโดยไม่ได้รับอนุญาต

นโยบาย

๕.๑ **การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)**

- ต้องควบคุมการใช้งานสารสนเทศในระบบสารสนเทศกำหนดสิทธิในการใช้งาน ได้แก่ เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้งานที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งาน นั้น มีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน
- บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และ กำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๕.๒ **ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย**
(Secure tog-onprocedures)

- การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัยตาม แนวทางปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕.๓ **การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม**
(Access Control to program source code)

- มีการกำหนด ระดับความปลอดภัย ของเข้าใช้ซอร์สโค้ดของโปรแกรมเป็นลำดับขั้นความปลอดภัยเพื่อป้องกันเกี่ยวกับข้อมูลสูญหาย หรือ มีซอร์สโค้ดที่ไม่ได้รับการอัพเดตรายการแก้ไขเข้าไปอย่างถูกต้อง

นโยบายความมั่นคงปลอดภัย
ทางกายภาพ และ สภาพแวดล้อม

นโยบายความมั่นคงปลอดภัยทางกายภาพ และ สภาพแวดล้อม
(Physical and environmental security)

๑. **พื้นที่ ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Areas)** วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และ การแทรกแซง การทำงาน ที่มีต่อสารสนเทศ และ อุปกรณ์ประมวลผลสารสนเทศขององค์กร

<u>นโยบาย</u>

๑.๑ **ขอบเขตพื้นที่หรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)**

- ต้องแบ่งพื้นที่อย่างชัดเจน และ กำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์สารสนเทศที่มีความสำคัญ
- ต้องจัดทำแผนผังแสดงตำแหน่ง , พื้นที่แต่ละชนิด และ ประกาศให้ผู้เกี่ยวข้องทราบ

๑.๒ **การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)**

- ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ หรือ ผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่
- ต้องกำหนดสิทธิ และ ช่วงเวลาในการผ่านเข้าออกพื้นที่
- ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือ ยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดย เด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึง พื้นที่สำนักงาน และ พื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๑.๓ **การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงาน และ อุปกรณ์ (securing office, room and facilities)**

- ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับสำนักงาน ห้องทำงาน และ เครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์ หรือ ระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการ ผ่านเข้า ออกของบุคคลเป็นจำนวนมาก
- เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้ SWRVER ตู้เอกสาร ลิ้นชัก และ อุปกรณ์ต่าง ๆ ได้รับการปิดล็อคอย่างเหมาะสม และ กุญแจ ถูกเก็บรักษาไว้อย่างปลอดภัย
- ข้อมูล สื่อบันทึก วัสดุ และ อุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือ ในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด
- ข้อมูล สื่อบันทึก วัสดุ และ อุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการ ทำลายอย่างเหมาะสม โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูล หรือ กำจัดสื่อบันทึกข้อมูล
- เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรือ สื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ ที่ได้รับอนุญาตให้ดำเนินการ และ เป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๑.๔ **การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (protecting against external and environment threats)**

- ต้องมีวิธีป้องกันจากการทำลายของธรรมชาติ หรือ คนที่อาจจะเกิดขึ้น เช่น
  - ๑.๔.๑ มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม น้ำท่วม
  - ๑.๔.๒ มีอุปกรณ์ดับเพลิงตามมาตรฐาน
  - ๑.๔.๓ มีระบบปรับอากาศ และ ความคุมความชื้น
  - ๑.๔.๔ จัดทำแผน คู่มือ การซักซ้อม และ การสรุปผล การป้องกันต่อภัยคุกคามจากภายนอก และ ของสภาพแวดล้อม
  - ๑.๔.๕ แผนการใช้งานด้านระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ ด้านภัยพิบัติของสภาพแวดล้อมขึ้น

๑.๕ **การปฏิบัติงานในพื้นที่ ที่ต้องการรักษาความมั่นคงปลอดภัย (Working is secure areas)**
ขั้นตอนปฏิบัติสำหรับการปฏิบัติการในพื้นที่

- ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น “ห้ามเข้าก่อน ได้รับอนุญาต”

๒. **อุปกรณ์ (Equipment)** วัตถุประสงค์ เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือ การเป็นอันตรายต่อสินทรัพย์ และ ป้องกัน การหยุดชะงักต่อการดำเนินงานของ โรงพยาบาลบ้านคา

<u>นโยบาย</u>

๒.๑ **การจัดตั้ง และ ป้องกันอุปกรณ์ (Equipment sitting and protection)**

- การจัดตั้ง หรือ การจัดวางอุปกรณ์สินทรัพย์สารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวาง ในที่เข้าถึงได้ยาก

๒.๒ **ระบบ และ อุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)**

- อุปกรณ์ที่มีความสำคัญสูง ควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า
  - ๒.๒.๑ ความเสี่ยงสูง ต้องมีระบบสำรองไฟฟ้าทั้ง UPS และ เครื่องกำเนิดไฟฟ้า
  - ๒.๒.๒ ความเสี่ยงปานกลาง ต้องมีระบบสำรองไฟฟ้า UPS
  - ๒.๒.๓ ความเสี่ยงต่ำ ต้องมีระบบสำรองไฟฟ้า UPS

๒.๓ **ความมั่นคงปลอดภัยของการเดินสายสัญญาณ และ สายสื่อสาร (Cabling Security)**

- การเดินสายสัญญาณต้องคำนึงถึงผลกระทบต่อความเสี่ยงที่อาจเกิดขึ้นเพื่อป้องกันสัญญาณรบกวน เช่น
  - ๒.๓.๑ ความเสี่ยงสูง การเดินสายต้องใช้สายป้องกันการรบกวนสัญญาณ และ การเข้าถึงสายสัญญาณ
  - ๒.๓.๒ ความเสี่ยงปานกลาง การเดินสายต้องป้องกันการเข้าถึงสายสัญญาณ
  - ๒.๓.๓ ความเสี่ยงต่ำ ใช้สายสัญญาณธรรมดา

๒.๔ **การบำรุงรักษาอุปกรณ์ (Equipment maintenance)**

- ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือมากกว่าตามระดับความสำคัญ เช่น
  - ๒.๔.๑ ระบบที่มีความเสี่ยงสูง ต้องบำรุงรักษาทุก ๔ เดือน
  - ๒.๔.๒ ระบบที่มีความเสี่ยงปานกลาง ต้องบำรุงรักษาทุก ๖ เดือน
  - ๒.๔.๓ ระบบที่มีความเสี่ยงต่ำต้องบำรุงรักษาทุก ๑๒ เดือน

๒.๕ **การนำทรัพย์สินของ โรงพยาบาลบ้านคา ออกนอกสำนักงาน (Removal of assets)**

- ห้ามนำสินทรัพย์สารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีระบบ การควบคุมดูแลทรัพย์สิน การลงทะเบียนทรัพย์สิน / ครุภัณฑ์

๒.๖ **ความมั่นคงปลอดภัยของอุปกรณ์ และ ทรัพย์สินที่ใช้งานอยู่ภายนอกส่วนงาน (Security of equipment and assets off-premises)**

- ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง เช่น
  - ๒.๖.๑ กำหนดรหัสการเข้าถึงการใช้งานอุปกรณ์คอมพิวเตอร์
  - ๒.๖.๒ กำหนดผู้รับผิดชอบ และ ดูแลอุปกรณ์
  - ๒.๖.๓ กำหนดผู้รับผิดชอบ และ ดูแลอุปกรณ์ห้องแม่ข่าย
  - ๒.๖.๔ มีระบบป้องกันความปลอดภัย เช่น antivirus การกำหนดสิทธิ์ใช้งาน

๒.๗ **ความมั่นคงปลอดภัยสำหรับการกำจัด หรือ ทำลายอุปกรณ์ หรือ การนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)**

- ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายให้สิ้นซาก

๒.๘ **อุปกรณ์ของ ผู้ใช้งาน ที่ทิ้งไว้โดยไม่มี ผู้ดูแล (Unattended use equipment)**

- ต้องป้องกันให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สินทรัพย์สารสนเทศที่ไม่มีผู้ดูแล

๒.๙ **นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และ นโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)**

- เจ้าหน้าที่ต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บหรือบันทึกอยู่ไม่ให้ วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอ คอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน