



## นโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านคา

โรงพยาบาลบ้านคา ได้จัดทำนโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นต่อความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านคา จะสามารถดำเนินงานได้อย่างมีประสิทธิภาพ และ ประสิทธิภาพ ได้มีการเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบ และ เจ้าหน้าที่ทุกคนจะต้อง ปฏิบัติตามนโยบายนี้อย่างเคร่งครัด โดยมีเนื้อหา ดังนี้

๑. การรักษาความมั่นคงปลอดภัยทางกายภาพ และ สิ่งแวดล้อมของศูนย์ข้อมูล (Data Center) เช่น ความมั่นคงปลอดภัยทางกายภาพ กำหนดให้มีผู้รับผิดชอบในการเข้าถึงเอกสาร อุปกรณ์คอมพิวเตอร์ / สถานที่เก็บเอกสาร / ข้อมูลสารสนเทศ
๒. การควบคุมการเข้าออกศูนย์ข้อมูล เช่น ห้ามมิให้ผู้ไม่มีหน้าที่เกี่ยวข้องเข้าออกโดยพลการ เว้นแต่จะได้รับอนุญาตจากผู้รับผิดชอบ รวมถึงจัดการควบคุมการเข้าใช้งานจากระยะไกลต้องเป็นผู้ที่ได้รับอนุญาต และมีกิจอันควรในการใช้งาน
๓. การบริการระบบเครือข่ายคอมพิวเตอร์อย่างต่อเนื่อง เช่น ความมั่นคงปลอดภัยของระบบเครือข่าย มาตรการทางเทคนิค ในการจำกัดการเข้าถึงระบบเครือข่าย การใช้อุปกรณ์ Firewall เพื่อป้องกันภัยคุกคามในระบบเครือข่ายการเข้ารหัสข้อมูลสำคัญ ติดตั้ง / ตั้งค่าอุปกรณ์ ให้ได้มาตรฐาน ฝ้าระวังและบำรุงรักษาอย่างต่อเนื่อง
๔. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Access Control) เช่น การป้องกันการเข้าถึงความเป็นส่วนตัว ของข้อมูลส่วนบุคคลเกี่ยวกับบุคลากร และ ข้อมูลของผู้ป่วย ป้องกันการเปิดเผยความลับผู้ป่วย ของโรงพยาบาลบ้านคา
๕. กำหนดให้มีการพิสูจน์ตัวตน (Accountability, Identification and Authentication) เช่น การยืนยันตัวตนบุคคล ในการเข้าใช้งานระบบสารสนเทศทางการแพทย์ การกำหนดสิทธิการเข้าถึงข้อมูล และ การสร้างความตระหนักของผู้ใช้งานต่อความเสี่ยง ต่าง ๆ ส่วนบุคคล โดยเฉพาะข้อมูลสุขภาพของผู้ป่วย และ ข้อมูลบุคคลของบุคลากร
๖. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพา (Use of Personal Computer) เช่น ไม่อนุญาตให้ผู้ใช้ทำการ ติดตั้ง/ถอดถอน/เปลี่ยนแปลงการตั้งค่าในเครื่องคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจาก ผู้มีอำนาจ ผู้ใช้ต้องไม่บันทึกข้อมูลไว้ที่ Drive C หรือ Desktop และ ไม่ควรนำอาหาร หรือ เครื่องดื่มมารับประทาน หรือ วางใกล้บริเวณเครื่องคอมพิวเตอร์
๗. การใช้งานอินเทอร์เน็ต (Use of the Internet) เช่น ผู้ใช้สามารถใช้งาน Internet เฉพาะ Website ที่เกี่ยวข้องกับภารกิจโรงพยาบาลบ้านคาเท่านั้น และ ไม่กระทำการใด ๆ ที่เป็นการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
๘. การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถ ให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ เช่น ทุกหน่วยงานต้องมีแผนเตรียมความพร้อมในกรณีฉุกเฉิน และการนำสารสนเทศกลับคืนสู่ระบบเมื่อเข้าสู่ภาวะปกติ การสำรองข้อมูล ควบคุมการเข้าถึงฐานข้อมูลส่วนบุคคลที่สำคัญเป็นพิเศษ เช่น (ฐานข้อมูลเงินเดือนของบุคลากร ข้อมูลสุขภาพของผู้ป่วย) การทำลายเอกสารที่มีข้อมูล ส่วนบุคคลที่สำคัญอย่างปลอดภัยแผนตรวจสอบติดตามความมั่นคง

## คำนิยาม และ คำจำกัดความ

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

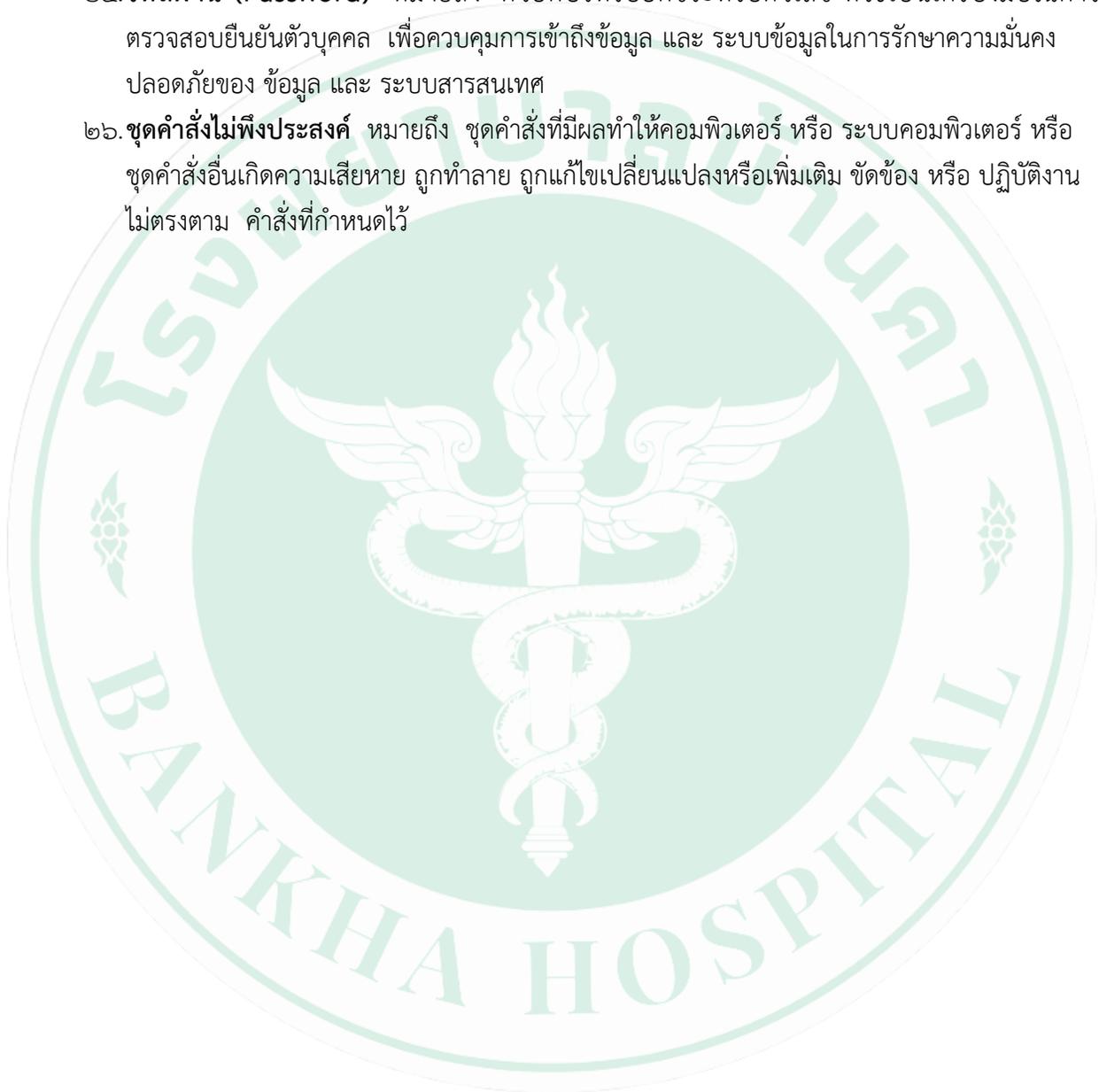
๑. **องค์กร** หมายถึง โรงพยาบาลบ้านคา
๒. **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารงานของ โรงพยาบาลบ้านคา
๓. **กลุ่มเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานบริหาร จัดการ และ ดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร เสนอแนะนโยบาย ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์ และ เครือข่ายของโรงพยาบาลบ้านคา
๔. **หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ** หมายถึง ผู้มีอำนาจ ในด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลบ้านคาซึ่งบทบาทหน้าที่ และ ความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบสารสนเทศ
๕. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของโรงพยาบาลบ้านคา
๖. **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้มองเห็นโดยตาม วัตถุประสงค์หรือเป้าหมาย
๗. **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
๘. **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
๙. **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแล รักษา ระบบสารสนเทศของโรงพยาบาลบ้านคา
๑๐. **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารระดับสูงของโรงพยาบาลบ้านคา
๑๑. **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ มีหน้าที่รับผิดชอบในการดูแลรักษา ระบบ และ เครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรม เครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลเครือข่ายคอมพิวเตอร์
๑๒. **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุขลูกจ้างประจำ ลูกจ้างชั่วคราว และ พนักงานเจ้าหน้าที่บริการ
๑๓. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลบ้านคา อนุญาตให้มีสิทธิ ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตาม อำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
๑๔. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือ สิ่งอื่นใด บรรดาที่อยู่ในระบบ คอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และ ให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๑๕. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และ อื่น ๆ
๑๖. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และ แนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
๑๗. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการ ส่งข้อมูล และ สารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของโรงพยาบาลบ้านคา ได้ เช่น ระบบ LAN, ระบบ Internet เป็นต้น
๑๘. **ระบบ LAN และ ระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ คอมพิวเตอร์ ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
๑๙. **ระบบ Internet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
๒๐. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยี สารสนเทศ ระบบคอมพิวเตอร์ และ ระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงาน สามารถนำมาใช้ ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และ ควบคุมการติดต่อสื่อสาร ซึ่ง มีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูล และสารสนเทศ เป็นต้น
๒๑. **พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงาน อนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น
- ๒๑.๑ **ห้องปฏิบัติงาน พื้นที่ทำงานทั่วไป (General Working area)** หมายถึง พื้นที่ติดตั้งเครื่อง คอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพา (Notebook) ที่ประจำโต๊ะทำงาน
  - ๒๑.๒ **พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)**
  - ๒๑.๓ **พื้นที่ติดตั้งอุปกรณ์ ระบบสารสนเทศ หรือ ระบบเครือข่าย (IT equipment or network area)**
  - ๒๑.๔ **พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)**
  - ๒๑.๕ **พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)**
๒๒. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
๒๓. **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และ ทรัพย์สินด้านเทคโนโลยีสารสนเทศ และ การสื่อสาร ของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๔. **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน ผ่านเครื่องคอมพิวเตอร์ และ เครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และ เสียง ผู้ส่งสามารถส่งข่าวสาร ไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๒๕. **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการ ตรวจสอบยืนยันตัวตนบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และ ระบบข้อมูลในการรักษาความมั่นคง ปลอดภัยของ ข้อมูล และ ระบบสารสนเทศ

๒๖. **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ หรือ ชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้อง หรือ ปฏิบัติงาน ไม่ตรงตาม คำสั่งที่กำหนดไว้



## นโยบายควบคุมการเข้าถึง (Access Control Policy)

๑. การกำหนดผู้รับผิดชอบภายในโรงพยาบาลบ้านคา และ ร่วมกันพิจารณาออกข้อกำหนดในการเข้าถึงระบบ และ มีการประกาศใช้อย่างเป็นทางการ เช่น กำหนดสิทธิในการเข้าใช้งานในอุปกรณ์คอมพิวเตอร์, กำหนดสิทธิในการเข้าใช้งานระบบ
๒. การเข้าถึงเครือข่าย และ บริการเครือข่าย (Access to networks and network services)  
การกำหนดให้มีการพิจารณาสิทธิในการเข้าถึงข้อมูลของผู้ใช้โดยกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ , มีการทบทวนสิทธิการเข้าถึงข้อมูลของเจ้าหน้าที่เดิม
๓. การบริหารจัดการการเข้าถึงของพนักงาน (User access management) วัตถุประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

### นโยบาย

- ๓.๑ การลงทะเบียนและการถอดถอนสิทธิพนักงาน (User registration and de-registration)
  - การลงทะเบียนพนักงานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งานระบบสารสนเทศ และ ระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่พนักงานสิ้นสุดสถานภาพต้องยกเลิกออกจากระบบทันที
- ๓.๒ การจัดการสิทธิการเข้าถึงของพนักงาน (User access provisioning)
  - ผู้ดูแลระบบต้องมีกระบวนการกำหนดสิทธิ์ให้ครอบคลุมพนักงานให้ครบทุกประเภท และ ทุกการบริการของระบบสารสนเทศ
- ๓.๓ การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)
  - ผู้ดูแลระบบต้องกำหนดสิทธิพนักงานในการเข้าถึงระบบสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบ
- ๓.๔ การทบทวนสิทธิการเข้าถึงของพนักงาน (Review of user access right)
  - ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้อย่างน้อยปีละ ๑ ครั้ง
- ๓.๕ การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or 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 การกำหนดการเปลี่ยนแปลงการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย
- รหัสผ่าน ถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษาหัสผ่านอย่างมั่นคงปลอดภัย
- 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 มีเฉพาะข้อมูลที่ต้องใช้งาน
- บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และ กำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

#### ๕.๒ ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

##### (Secure log-on procedures)

- การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัยตาม แนวทางปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

#### ๕.๓ การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม

##### (Access Control to program source code)

- มีการกำหนด ระดับความปลอดภัย ของเข้าใช้ซอร์สโค้ดของโปรแกรมเป็นลำดับขั้นความปลอดภัยเพื่อป้องกันเกี่ยวกับข้อมูลสูญหาย หรือ มีซอร์สโค้ดที่ไม่ได้รับการอัปเดตรายการแก้ไขเข้าไปอย่างถูกต้อง

## นโยบายความมั่นคงปลอดภัยทางกายภาพ และ สภาพแวดล้อม (Physical and environmental security)

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

### นโยบาย

#### 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 ยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด 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 ได้รับการปิดล็อกอย่างเหมาะสม และ กุญแจ ถูกเก็บรักษาไว้อย่างปลอดภัย
- ข้อมูล สื่อบันทึก วัสดุ และ อุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือ ในตู้ที่ไม่ได้ล็อกกุญแจโดยเด็ดขาด
- 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 กรณีไฟไหม้ 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 in secure areas)

ขั้นตอนปฏิบัติสำหรับการปฏิบัติการในพื้นที่

- ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น “ห้ามเข้าก่อน ได้รับอนุญาต”

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

##### นโยบาย

##### 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 ออกจากสำนักงาน (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 วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอ คอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน

