

นโยบายและระเบียบด้านเทคโนโลยีสารสนเทศ

คำตอบ 92 ข้อ

● ยอมรับ



มาตรการ 6 ป.

ระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ “มาตรการ 6 ป.”

<p>“ ปกปิด ”</p> <p>ต้องเก็บ Username และ Password เป็นความลับ ไม่เปิดเผยต่อผู้อื่น เป็นสิทธิ์ใช้งานเฉพาะบุคคล</p>	<p>“ ปกป้อง ”</p> <p>ต้อง Login ก่อน และ Logout หลังเลิกใช้งานทุกครั้ง อย่าทิ้งหน้าจอไว้ให้ใครมาสวมรอย</p>	<p>“ ป้องกัน ”</p> <p>ต้องติดตั้ง Antivirus ทุกเครื่อง และอัปเดตเมื่อมีการใช้งานหรือปิดหน้าจอเพื่อป้องกันข้อมูลอันสำคัญ</p>	<p>โรงพยาบาลบ้านคา</p> <p>(.....) นายสุรฤทธิ เจริญศรี ตำแหน่ง นายแพทย์ชำนาญการ ผู้อำนวยการโรงพยาบาลบ้านคา</p>
<p>“ เปิดเผย ”</p> <p>ต้องได้รับการอนุมัติ เป็นลายลักษณ์อักษรก่อนการเผยแพร่ ข้อมูลในเว็บไซต์โรงพยาบาล</p>	<p>“ ปลดปลั๊ก ”</p> <p>ห้ามนำอุปกรณ์ใด ๆ มาเชื่อมต่อ กับระบบเน็ตเวิร์คของโรงพยาบาล โดยไม่ได้รับอนุญาต</p>	<p>“ ปลอดภัย ”</p> <p>ห้ามนำอาหารหรือเครื่องดื่มมาวาง บริเวณคอมพิวเตอร์ เพื่อความปลอดภัย และ ยืดอายุการใช้งาน</p>	



ประกาศโรงพยาบาลบ้านคา

เรื่อง ระเบียบปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศ
สำหรับบุคลากรในโรงพยาบาลบ้านคา

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านคา มีเสถียรภาพ ปลอดภัย สามารถใช้งานในระบบบริการและสนับสนุนบริการสุขภาพของโรงพยาบาลบ้านคาได้ต่อเนื่องตลอดเวลา รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลบ้านคา จึงเห็นสมควรกำหนดระเบียบปฏิบัติงานดังต่อไปนี้

1. ให้เจ้าหน้าที่ตั้งรหัสผ่าน (Password) ของตนเองในการใช้งานระบบคอมพิวเตอร์ของโรงพยาบาลโดยทำการเปลี่ยนรหัสผ่านอย่างน้อย ๑ เดือน หรือ จนกว่าจะมีการแจ้งเตือนของเครื่องคอมพิวเตอร์ ขั้นตอนการเปลี่ยนรหัสผ่าน ๓ ขั้นตอนตามเอกสารแนบ หรือ ติดต่อเจ้าหน้าที่ดูแลระบบ
2. ให้เจ้าหน้าที่ปกปิดรหัสผ่านเป็นความลับส่วนตัว ไม่เปิดเผยให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้และห้ามติดรหัสผ่าน (Password) ให้เข้าถึงได้ง่ายทางกายภาพที่โต๊ะทำงาน หรือ บนหน้าจอ
3. ให้เจ้าหน้าที่ลงชื่อออก (Log Out) ทุกครั้งเมื่อไม่ได้ใช้งานหน้าเครื่องคอมพิวเตอร์ และปิดเครื่องคอมพิวเตอร์ (Shut Down) เมื่อเลิกใช้งาน
4. ห้ามใช้เครื่องคอมพิวเตอร์ของโรงพยาบาลเปิดไฟทำงานจากภายนอกหากไม่ได้ตรวจหาไวรัสก่อนและหากผู้ใช้งานพบ หรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัส ให้ยกเลิกการเชื่อมต่อระบบเครือข่ายทันที และแจ้งผู้ดูแลระบบ
5. ห้ามเผยแพร่ ทำสำเนา ถ่ายภาพ เปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลผู้ป่วย ในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณี นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการโรงพยาบาล
6. ห้ามนำเครื่องคอมพิวเตอร์ อุปกรณ์อื่น ๆ รวมถึงอุปกรณ์จัดเก็บข้อมูลเช่น CD-ROM , USB Drive , External Hard Disk อุปกรณ์เครือข่าย เช่น Hub , Switch , Wi-Fi Router ฯลฯ มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของโรงพยาบาล ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ
7. ห้ามเจ้าหน้าที่ทำการเปิดใช้งาน Desktop ระยะไกล (Remote Desktop) จากภายนอกโรงพยาบาล นอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการโรงพยาบาล
8. ห้ามนำอาหารและเครื่องดื่ม วางใกล้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายของโรงพยาบาล

(นายสุรฤทธิ์ เจริญศรี)

นายแพทย์ชำนาญการ

รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลบ้านคา



นโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านคา

โรงพยาบาลบ้านคา ได้จัดทำนโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่น ต่อความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านคา จะสามารถดำเนินงานได้อย่างมีประสิทธิภาพ และ ประสิทธิภาพ ได้มีการเผยแพร่ให้เจ้าหน้าที่ทุกระดับได้รับทราบ และ เจ้าหน้าที่ทุกคนจะต้อง ปฏิบัติตาม นโยบายนี้อย่างเคร่งครัด โดยมีเนื้อหา ดังนี้

๓. การรักษาความมั่นคงปลอดภัยทางกายภาพ และ สิ่งแวดล้อมของศูนย์ข้อมูล (Data Center) เช่น ความมั่นคงปลอดภัยทางกายภาพ กำหนดให้ไม่มีผู้รับผิดชอบในการเข้าสิ่งเอกสาร อุปกรณ์คอมพิวเตอร์ / ฮาร์ดแวร์เก็บเอกสาร / ข้อมูลสารสนเทศ
๔. การควบคุมการเข้าออกศูนย์ข้อมูล เช่น ห้ามมิให้ผู้ไม่มีหน้าที่เกี่ยวข้องเข้าออกโดยพลการ เว้นแต่จะได้รับอนุญาตจากผู้รับผิดชอบ รวมถึงจัดการควบคุมการเข้าใช้งานจากระยะไกลต้องเป็นผู้ที่ได้รับอนุญาต และ มีกิจอันควรในการใช้งาน
๕. การบริการระบบเครือข่ายคอมพิวเตอร์อย่างต่อเนื่อง เช่น ความมั่นคงปลอดภัยของระบบเครือข่าย มาตราการทางเทคนิค ในการจำกัดการเข้าถึงระบบเครือข่าย การใช้อุปกรณ์ Firewall เพื่อป้องกันภัยคุกคาม ในระบบเครือข่ายการเข้ารหัสข้อมูลสำคัญ คิดตั้ง / ตั้งค่าอุปกรณ์ ให้ได้ตามมาตรฐาน เน้าระวังและบำรุงรักษา อย่างต่อเนื่อง
๖. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Access Control) เช่น การป้องกันการเข้าถึงความลับส่วนตัว ของข้อมูลส่วนบุคคลเกี่ยวกับบุคลากร และ ข้อมูลของผู้ป่วย ป้องกันการเปิดเผยความลับผู้ป่วย ของโรงพยาบาลบ้านคา
๗. กำหนดให้มีการพิสูจน์ตัวตน (Accountability) Identification and Authentication) เช่น การยืนยันตัวตนบุคคล ในการเข้าใช้งานระบบสารสนเทศทางการแพทย์ การกำหนดสิทธิ์การเข้าถึงข้อมูล และ การสร้างความตระหนักของผู้ใช้งานต่อความเสี่ยง ต่าง ๆ ส่วนบุคคล โดยเฉพาะข้อมูลสุขภาพของผู้ป่วย และ ข้อมูลบุคคลของบุคลากร
๘. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพา (Use of Personal Computer) เช่น ไมอนุญาตให้ผู้ใช้ทำการ ติดตั้ง/ถอดถอน/เปลี่ยนแปลงการตั้งค่าในเครื่องคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจาก ผู้มีอำนาจ ผู้ใช้ต้องไม่บันทึกข้อมูลไว้ที่ Drive C หรือ Desktop และ ไม่ควรนำอาหาร หรือ เครื่องดื่มมารับประทาน หรือ วางใกล้บริเวณเครื่องคอมพิวเตอร์
๙. การใช้งานอินเทอร์เน็ต (Use of the Internet) เช่น ผู้ใช้สามารถใช้งาน Internet เฉพาะ Website ที่เกี่ยวข้องกับภารกิจโรงพยาบาลบ้านคาเท่านั้น และ ไม่กระทำการใด ๆ ที่เป็นภาระเม็ดเงินหรือบ่งชี้ว่าด้วยการกระทำความเสี่ยงเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
๑๐. การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถ ให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพ เช่น ทุกหน่วยงานต้องมีแผนเตรียมความพร้อมในการเผชิญเหตุ และ การนำสารสนเทศ กลับคืนสู่ระบบเมื่อเข้าสู่ภาวะปกติ การสำรองข้อมูล ควบคุมการเข้าถึงฐานข้อมูลส่วนบุคคลที่สำคัญเป็นพิเศษ เช่น (ฐานข้อมูลเงินเคียนของบุคลากร ข้อมูลสุขภาพของผู้ป่วย) การทำลายเอกสารที่มีข้อมูล ส่วนบุคคลที่สำคัญอย่างปลอดภัยแบบตรวจสอบติดตามความมั่นคง