การจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลบ้านคา

จัดทำโดย

ศูนย์คอมพิวเตอร์ โรงพยาบาลบ้านคา

กลุ่มภารกิจพัฒนาระบบบริการ และ สนับสนุนบริการสุขภาพ

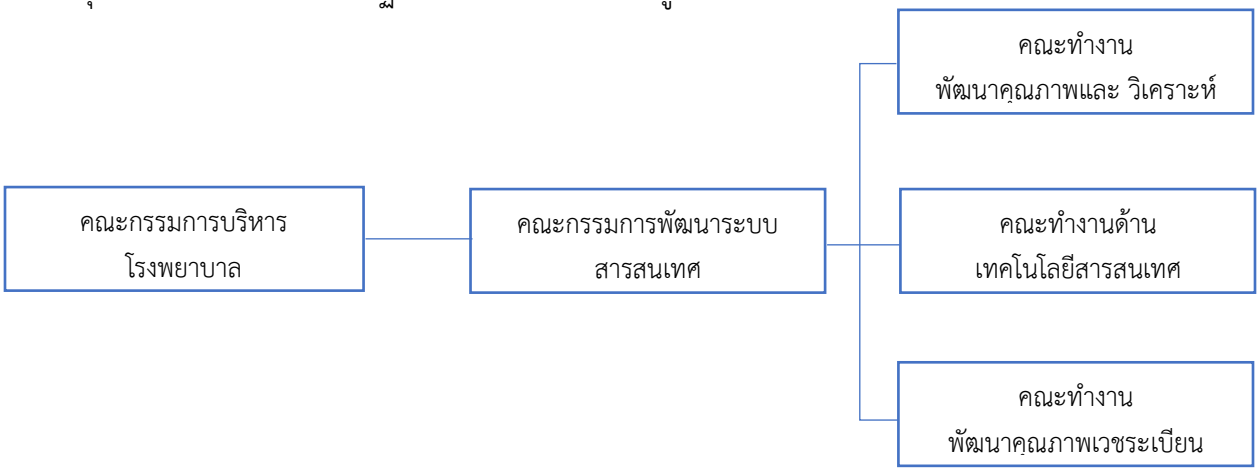
สารบัญ

เรื่อง **หน้า**

คำสั่งแต่งตั้ง
คณะกรรมการพัฒนา
คุณภาพสารสนเทศ

คำสั่งโรงพยาบาลบ้านคา
ที่ ๘ / ๒๕๖๗
เรื่อง แต่งตั้งคณะกรรมการพัฒนาคุณภาพสารสนเทศ

เพื่อให้โรงพยาบาลบ้านคามีการพัฒนาอย่างต่อเนื่องและยั่งยืน สู่การเป็นโรงพยาบาลชุมชั้นนำระดับประเทศ ส่งเสริมบุคลากรเรียนรู้และพัฒนาโดยใช้ข้อมูลเป็นพื้นฐาน มีและใช้เทคโนโลยีให้เกิดประโยชน์สูงสุดต่อผู้ป่วย/ผู้รับบริการ และชุมชน ในการนี้จึงขอแต่งตั้งคณะกรรมการพัฒนาคุณภาพสารสนเทศ พร้อมคณะทำงานจำนวน ๓ คณะได้แก่ คณะทำงานพัฒนาข้อมูล คณะทำงานด้านเทคโนโลยีสารสนเทศ คณะทำงานพัฒนาคุณภาพเวชระเบียน โดยปฏิบัติงานภายใต้การกำกับดูแลของคณะกรรมการบริหารโรงพยาบาลบ้านคา



๑. คณะกรรมการพัฒนาระบบสารสนเทศ

๑.๑ นายสุรฤทธิ์ เจริญศรี	นายแพทย์ชำนาญการ	ประธาน
๑.๒ นายธนัฐกรณ์ โภคินกรณ์พงศ์	พยาบาลวิชาชีพชำนาญการพิเศษ	รองประธาน
๑.๓ นางสาววรางคณา แท่นตั้งเจริญชัย	ทันตแพทย์ชำนาญการพิเศษ	กรรมการ
๑.๔ นางสาวอาริยา เลิศวิไล	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๑.๕ นางสาวชนาพร เพ็งจันทร์	นักจัดการงานทั่วไปปฏิบัติการ	กรรมการ
๑.๖ นางสาวอัจฉรา เพียภักดิ์	นักวิชาการสาธารณสุขปฏิบัติการ	กรรมการ
๑.๗ นายสันติ แววสกุล	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๑.๘ นางสาวบุญเรือง สว่างอารมณ์	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๑.๙ นางสาวดารณี ชาวโพธิ์สระ	เจ้าพนักงานเวชสถิติ	กรรมการ
๑.๑๐นายสุริยา บุญเลิศฟ้า	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ และ เลขานุการ

บทบาทหน้าที่

- ❖ จัดทำแผนแม่บท และแผนปฏิบัติการด้านสารสนเทศ
- ❖ จัดทำร่างนโยบายด้านความมั่นคงระบบสารสนเทศ เสนอคณะกรรมการบริหารโรงพยาบาลบ้านคา พร้อมทั้งเผยแพร่ให้บุคลากรรับทราบ
- ❖ บริหารจัดการความเสี่ยงด้านสารสนเทศ เทคโนโลยีคอมพิวเตอร์ และเวชระเบียน
- ❖ จัดให้มีการติดตามควบคุม กำกับการปฏิบัติตามนโยบายความมั่นคงระบบสารสนเทศ
- ❖ วิเคราะห์ ทบทวน อุบัติการณ์ด้านสารสนเทศที่สำคัญ และหามาตรการป้องกัน (Incident Management)
- ❖ ออกแบบระบบเทคโนโลยีสารสนเทศให้สอดคล้องต่อการใช้งาน การดูแลผู้ป่วย
- ❖ ส่งเสริมบุคลากรโรงพยาบาลให้มีทัศนคติในการใช้เทคโนโลยีสารสนเทศ ปฏิบัติ ดำเนินการพัฒนาการวัดวิเคราะห์ ปรับทิศทาง ทบทวน และปรับปรุงผลงาน โดยใช้ข้อมูลและสารสนเทศในทุกระดับ และ ทุกส่วนขององค์กร
- ❖ ติดตามและประเมินผลการปฏิบัติงานตามยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศขององค์กร และแผนงาน / โครงการด้านสารสนเทศ

๒. คณะทำงานพัฒนาคุณภาพและวิเคราะห์ข้อมูล

๒.๑	นายธนัฐกรณ์ โภคินกรณ์พงศ์	พยาบาลวิชาชีพชำนาญการพิเศษ	ประธาน
๒.๒	นางสาววรางคณา แท่นตั้งเจริญชัย	ทันตแพทย์ชำนาญการพิเศษ	กรรมการ
๒.๓	นางสาวอาริยา เลิศวิไล	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๒.๔	จรรยพร แซ่เฒ่า	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๒.๕	นายสันติ แววสกุล	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๒.๖	นางสาวศุภรักษ์ วังสุข	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๒.๗	นางสาวสิธรัตน์ จันทร์ฐานิกา	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๒.๘	นางสาวพัสตราภรณ์ เยี่ยงกุลเชาว์	เภสัชกรปฏิบัติการ	กรรมการ
๒.๙	นายอรรถพงษ์ จันทร์เศรษฐ์	นักเทคนิคการแพทย์ปฏิบัติการ	กรรมการ
๒.๑๐	นางสาวอัมราพร ลิ้มบริบูรณ์	เจ้าพนักงานการเงินและบัญชีปฏิบัติงาน	กรรมการ
๒.๑๑	นางสาวดารณี ชาวโพธิ์สระ	เจ้าพนักงานเวชสถิติ	กรรมการ
๒.๑๒	นางสาวชนาพร เพ็งจันทร์	นักจัดการงานทั่วไปปฏิบัติการ	กรรมการ
๒.๑๓	นางสาวณัฐกฤตา แดงเถาว์จินดา	นักจัดการงานทั่วไป	เลขานุการ

บทบาทหน้าที่

- ❖ กำหนดทิศทาง ออกแบบการจัดเก็บข้อมูล การบันทึกข้อมูลให้สอดคล้องกับการใช้ประโยชน์ทั้งในด้านบริหาร บริการ วิชาการ
- ❖ การพัฒนาคุณภาพ รวมถึงมาตรฐานข้อกำหนดต่าง ๆ เช่น ๔๓ แฟ้ม ให้มีความถูกต้อง น่าเชื่อถือ และพร้อมใช้
- ❖ วิเคราะห์ข้อมูลองค์กร เพื่อหาโอกาสพัฒนา

๓. คณะทำงานเทคโนโลยีสารสนเทศ

๓.๑	นายสุรฤทธิ์ เจริญศรี	นายแพทย์ชำนาญการ	ประธาน
๓.๒	นางสาวบุญเรือง สว่างอารมณ์	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๓.๓	นายสุริยา บุญเลิศฟ้า	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ และเลขานุการ
๓.๔	นายอนุพงศ์ ทองบ้านกวย	นักวิชาการคอมพิวเตอร์	ผู้ช่วยเลขานุการ

บทบาทหน้าที่

- ❖ วิเคราะห์ความต้องการด้านเทคโนโลยีสารสนเทศ
- ❖ จัดทำแผน Gap Analysis ด้านเทคโนโลยีสารสนเทศ
- ❖ กำหนดและคัดเลือกเทคโนโลยีสารสนเทศที่เหมาะสมกับองค์กร

๔. คณะทำงานพัฒนาคุณภาพเวชระเบียน

๔.๑	นางสาวบุญเรือง สว่างอารมณ์	พยาบาลวิชาชีพชำนาญการ	ประธาน
๔.๒	นางสาวดารณี ชาวโพธิ์สระ	เจ้าพนักงานเวชสถิติ	กรรมการ
๔.๓	นายสุริยา บุญเลิศฟ้า	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ และเลขานุการ
๔.๔	นายอนุพงศ์ ทองบ้านกวย	นักวิชาการคอมพิวเตอร์	ผู้ช่วยเลขานุการ

บทบาทหน้าที่

- ❖ กำหนดนโยบาย มาตรการ ระเบียบปฏิบัติให้เกิดแนวทางปฏิบัติเกี่ยวกับการบันทึก การแก้ไข การจัดเก็บ และการเข้าถึงเวชระเบียนที่เหมาะสม
- ❖ ตรวจประเมินคุณภาพการบันทึกเวชระเบียนผู้ป่วยของหน่วยบริการ
- ❖ ติดตามและประเมินผลกระบวนการทบทวนเวชระเบียน
- ❖ เสนอผลการตรวจสอบคุณภาพของเวชระเบียน ทั้งด้านการใช้ทรัพยากรของโรงพยาบาลในการดูแลผู้ป่วย กระบวนการดูแลผู้ป่วย และผลของการรักษา
- ❖ พัฒนากระบวนการทบทวนคุณภาพเวชระเบียนอย่างต่อเนื่อง
- ❖ ดำเนินการ ประสานงานหน่วยงานและทีมนำต่างๆ เพื่อให้เกิดกิจกรรมการทบทวนคุณภาพและความสมบูรณ์ของเวชระเบียน

สั่ง ณ วันที่ ๑๑ มกราคม พ.ศ. ๒๕๖๗

.....

(นายสุรฤทธิ์ เจริญศรี)

ผู้อำนวยการโรงพยาบาลบ้านคา

นโยบายความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

นโยบายความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านคา

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

๑. **การรักษาความมั่นคงปลอดภัยทางกายภาพ และ สิ่งแวดล้อมของศูนย์ข้อมูล (Data Center)** เช่น ความมั่นคงปลอดภัยทางกายภาพ กำหนดให้มีผู้รับผิดชอบในการเข้าถึงเอกสาร อุปกรณ์คอมพิวเตอร์ / สถานที่เก็บเอกสาร / ข้อมูลสารสนเทศ

๒. **การควบคุมการเข้าออกศูนย์ข้อมูล** เช่น ห้ามมิให้ผู้ไม่มีหน้าที่เกี่ยวข้องเข้าออกโดยพลการ เว้นแต่จะได้รับอนุญาตจากผู้รับผิดชอบ รวมถึงจัดการควบคุมการเข้าใช้งานจากระยะไกลต้องเป็นผู้ที่ได้รับอนุญาต และ มีกิจอันควรในการใช้งาน

๓. **การบริการระบบเครือข่ายคอมพิวเตอร์อย่างต่อเนื่อง** เช่น ความมั่นคงปลอดภัยของระบบเครือข่าย มาตรการทางเทคนิค ในการจำกัดการเข้าถึงระบบเครือข่าย การใช้อุปกรณ์ Firewall เพื่อป้องกันภัยคุกคามในระบบเครือข่ายการเข้ารหัสข้อมูลสำคัญ ติดตั้ง / ตั้งค่าอุปกรณ์ ให้ได้มาตรฐาน เฝ้าระวังและบำรุงรักษาอย่างต่อเนื่อง

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 และข้อมูลบุคคลของบุคลากร

๖. **การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพา (Use of Personal Computer)** เช่น ไม่อนุญาตให้ผู้ใช้ทำการ ติดตั้ง/ถอดถอน/เปลี่ยนแปลงการตั้งค่าในเครื่องคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจาก ผู้มีอำนาจ ผู้ใช้ต้องไม่บันทึกข้อมูลไว้ที่ Drive C หรือ Desktop และ ไม่ควรนำอาหาร หรือเครื่องดื่มมารับประทาน หรือ วางใกล้บริเวณเครื่องคอมพิวเตอร์

๗. **การใช้งานอินเทอร์เน็ต (Use of the Internet)** เช่น ผู้ใช้สามารถใช้งาน Internet เฉพาะ Website ที่เกี่ยวข้องกับภารกิจโรงพยาบาลบ้านคาเท่านั้น และ ไม่กระทำการใด ๆ ที่เป็นการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘. **การจัดทำระบบสำรองข้อมูล** เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถ ให้บริการได้อย่างต่อเนื่องและ มีเสถียรภาพ เช่น ทุกหน่วยงานต้องมีแผนเตรียมความพร้อมในกรณีฉุกเฉิน และ การนำสารสนเทศกลับคืนสู่ระบบเมื่อเข้าสู่ภาวะปกติ 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 บำรุงรักษาระบบคอมพิวเตอร์ และ เครือข่ายของโรงพยาบาลบ้านคา

๔. **หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ** หมายถึง ผู้มีอำนาจ ในด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลบ้านคาซึ่งบทบาทหน้าที่ และ ความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบสารสนเทศ

๕. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของโรงพยาบาลบ้านคา

๖. **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้พอเห็นโดยตามวัตถุประสงค์หรือเป้าหมาย

๗. **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๘. **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๙. **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของโรงพยาบาลบ้านคา

๑๐. **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารระดับสูงของโรงพยาบาลบ้านคา

๑๑. **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ และ เครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลเครือข่ายคอมพิวเตอร์

๑๒. **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุขลูกจ้างประจำ ลูกจ้างชั่วคราว และ พนักงานเจ้าหน้าที่บริการ

๑๓. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลบ้านคา อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๔. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือ สิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และ ให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๑๕. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และ สามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และ อื่น ๆ

๑๖. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้า ด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และ แนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๗. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และ สารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของโรงพยาบาลบ้านคา ได้ เช่น ระบบ LAN, ระบบ Internet เป็นต้น

๑๘. **ระบบ LAN และ ระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑๙. **ระบบ Internet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๒๐. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และ ระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่ง มีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูล และสารสนเทศ เป็นต้น

๒๑. **พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ ที่หน่วยงานอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น

๒๑.๑ **ห้องปฏิบัติงาน พื้นที่ทำงานทั่วไป (General Working area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล 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 โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๓. **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และ ทรัพย์สินด้านเทคโนโลยีสารสนเทศ และ การสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น

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

๒๕. **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และ ระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ ข้อมูล และ ระบบสารสนเทศ

๒๖. **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือ ปฏิบัติงานไม่ตรงตาม คำสั่งที่กำหนดไว้

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

<u>นโยบาย</u>

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 อุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม 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

ระเบียบปฏิบัติการ
รักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศ
สำหรับบุคลากร
โรงพยาบาลบ้านคา

ประกาศโรงพยาบาลบ้านคา

เรื่อง ระเบียบปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศ
สำหรับบุคลากรในโรงพยาบาลบ้านคา

.....

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านคา มีเสถียรภาพ ปลอดภัย สามารถใช้งานในระบบบริการและสนับสนุนบริการสุขภาพของโรงพยาบาลบ้านคาได้ต่อเนื่องตลอดเวลา รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลบ้านคา จึงเห็นสมควรกำหนดระเบียบปฏิบัติดังต่อไปนี้

๑. ผู้ใช้งานมีหน้าที่จัดเก็บและรักษาชื่อบัญชีผู้ใช้งาน รวมทั้งห้ามเผยแพร่ แจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่านของตนเอง
๒. ไม่อนุญาติให้ผู้อื่นเข้าใช้งานชื่อบัญชีผู้ใช้งาน และ รหัสผ่านในกรณีที่ใช้งานเครื่องคอมพิวเตอร์ของหน่วยงงานร่วมกัน ให้ทำการลงชื่อออก ทันทีหลังการใช้งาน
๓. ห้ามนำข้อมูลผู้ป่วยออกนอกโรงพยาบาล อาทิ เช่น ข้อมูลการรักษา ข้อมูลผลตรวจทางห้องปฏิบัติการ โดยไม่ได้รับอนุญาตจากผู้อำนวยการ หรือผู้ที่ได้รับมอบอำนาจแทน
๔. ห้ามติดตั้ง แก้ไข เปลี่ยนแปลง เคลื่อนย้าย คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ตลอดจนโปรแกรม
๕. ห้ามนำเข้าหรือส่งออกข้อมูลผ่านอุปกรณสำรองข้อมูลภายนอก เช่น Flash drive, External Hard disk กับเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านคา
๖. ห้ามเปิดหรือใช้งานเครื่องคอมพิวเตอร์เพื่อการบันเทิง ทำธุรกิจหรือหาผลประโยชน์ส่วนตัว เช่น Facebook TikTok การดูหนัง การเล่นเกมส์ เป็นต้น
๗. ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line และเว็บไซต์ต่างๆ หรือโปรแกรมอื่นที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อการรักษาผู้ป่วยเท่านั้น โดยปฏิบัติตามแนวทางปฏิบัติกรณีมีการส่งต่อข้อมูลผู้ป่วยโดยสื่อสังคมออนไลน์
๘. หัวหน้าฝ่าย/งาน ควบคุมกำกับช่องทางการสื่อสารออนไลน์ขององค์กร และ หน่วยงาน
๙. ไม่อนุญาตให้ใช้บัญชีส่วนตัวในการส่งต่อข้อมูลโดยไม่จำเป็น
๑๐. การส่งต่อข้อมูลทั้งภาพและข้อความที่เป็นการระบุตัวบุคคล ต้องดำเนินการลบภายใน ๒๔ ชั่วโมง หลังประบวนการรักษาเสร็จสิ้น
๑๑. ผู้มีสิทธิในการส่งข้อมูล คือแพทย์ผู้รักษาและผู้ที่ได้รับมอบหมายเป็นกรณีไป
๑๒. การสื่อสารใดๆ ที่เกิดขึ้น ไม่อนุญาตให้มีการบันทึกในรูปแบบต่างๆ หรือถ่ายภาพ ยกเว้นในกรณีเพื่อการรักษา

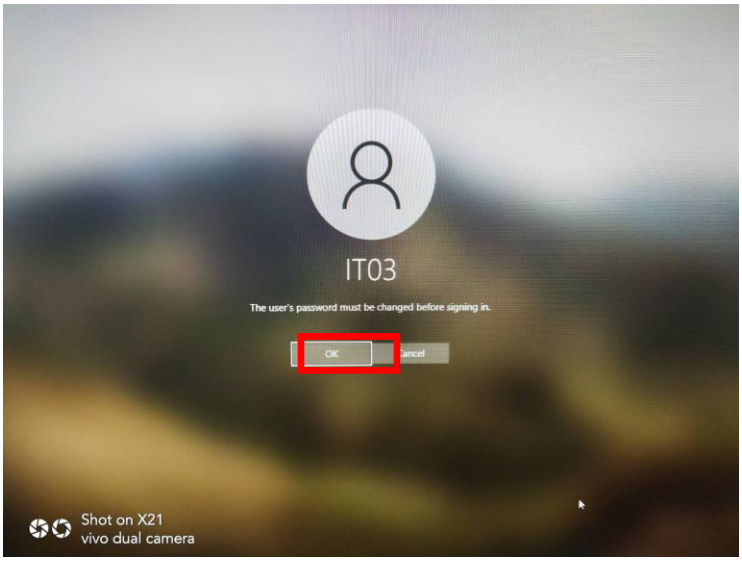
.....
(นายสุรฤทธิ์ เจริญศรี)
นายแพทย์ชำนาญการ
รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลบ้านคา

ขั้นตอนการเปลี่ยนรหัสผ่านตอนระบบแจ้งเตือนมีทั้งหมด ๓ ขั้นตอน ดังนี้

ขั้นตอนที่ ๑ ระบบจะทำการแจ้งเตือนให้ USER ทำการเปลี่ยนรหัสผ่าน

ให้ USER ทำการ คลิ๊ก 

เพื่อทำการเปลี่ยนรหัสผ่าน



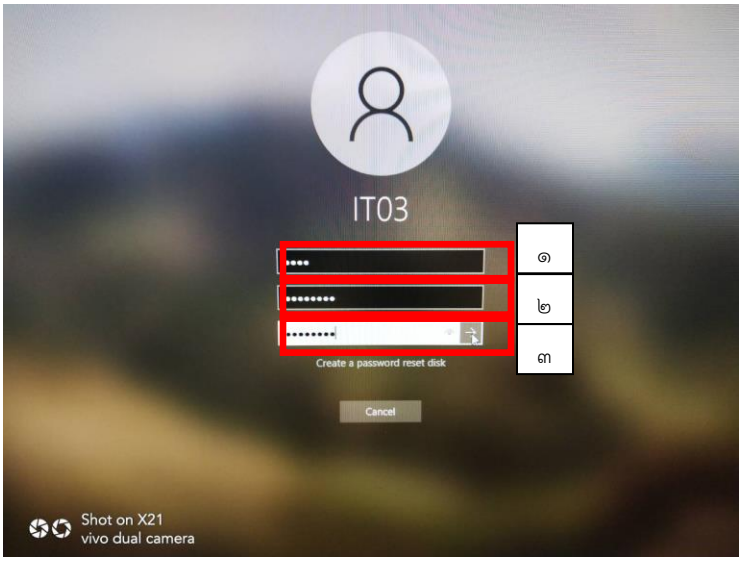
ขั้นตอนที่ ๒ บนหน้าจอ จะปรากฏ ให้ USER เริ่มดำเนินการเปลี่ยนรหัสผ่าน

ให้ USER ทำการ กรอกรหัสผ่านเดิม ใน ช่องที่ ๑

กรอกรหัสผ่านใหม่ ใน ช่องที่ ๒

Confirm รหัสผ่านใหม่ ใน ช่องที่ ๓

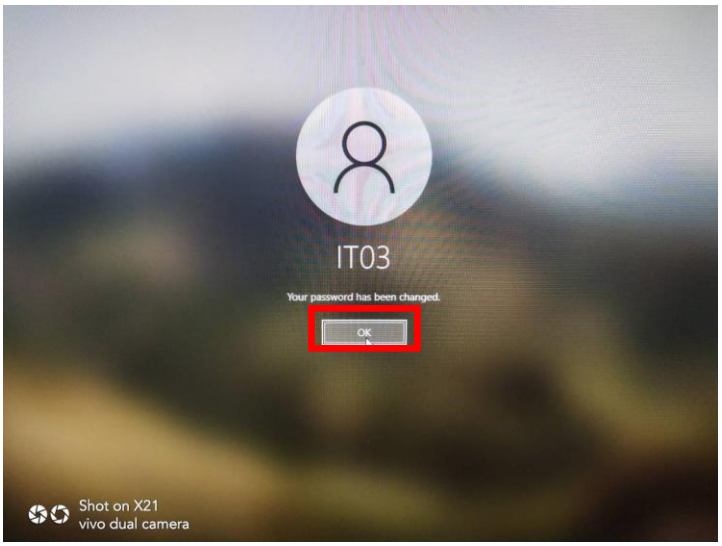
จากนั้นทำการ คลิ๊ก  เพื่อทำการยืนยันรหัสผ่านใหม่



ขั้นตอนที่ ๓ บนหน้าจอ จะปรากฏ ว่าการเปลี่ยนรหัสผ่านใหม่ดำเนินการเรียบร้อยแล้ว

ให้ USER ทำการ คลิ๊ก 

จากนั้นจะเข้าสู่หน้า WINDOWS ใช้งานได้ตามปกติ



โปสเตอร์
แผ่นพับประชาสัมพันธ์
ระเบียบปฏิบัติ

ระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศ **“มาตรการ 6 ป.”**

“ ปกปิด ”

ต้องเก็บ Username และ Password
เป็นความลับ ไม่เปิดเผยต่อผู้อื่น
เป็นสิทธิ์ใช้งานเฉพาะบุคคล

“ ปกป้อง ”

ต้อง Login ก่อน และ Logout
หลังเลิกใช้งานทุกครั้ง
อย่าทิ้งหน้าจอไว้ให้ใครมาสวมรอย

“ ป้องกัน ”

ต้องติดตั้ง Antivirus ทุกเครื่อง
และล็อคหน้าจอเมื่อพักการใช้งานหรือ
ปิดหน้าจอเพื่อป้องกันข้อมูลอันสำคัญ

โรงพยาบาลบ้านคา

(.....)
นายสุรฤทธิ์ เจริญศรี
ตำแหน่ง นายแพทย์ชำนาญการ
ผู้อำนวยการโรงพยาบาลบ้านคา

“ เปิดเผย ”

ต้องได้รับการอนุมัติ
เป็นลายลักษณ์อักษรก่อนการเผยแพร่
ข้อมูลในเว็บไซต์โรงพยาบาล

“ ปลดปล๊ัก ”

ห้ามนำอุปกรณ์ใด ๆ มาเชื่อมต่อ
กับระบบเน็ตเวิร์คของโรงพยาบาล
โดยไม่ได้รับอนุญาติ

“ ปลอดภัย ”

ห้ามนำอาหารหรือเครื่องดื่มมาวาง
บริเวณคอมพิวเตอร์ เพื่อความปลอดภัย
และ ยืดอายุการใช้งาน

ผลการประเมินความรับรู้ ความเข้าใจ และ การปฏิบัติ ตามระเบียบของเจ้าหน้าที่

แบบประเมินการรับรู้ระเบียบการรักษา
ความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลบ้านคา

เรื่อง ระเบียบปฏิบัติการรักษาความปลอดภัยด้านสารสนเทศ	การรับรู้		การปฏิบัติ	
	รับรู้	ไม่รับรู้	ละเมิด	ไม่ละเมิด
1.ผู้ใช้งานมีหน้าที่จัดเก็บและรักษาชื่อบัญชีผู้ใช้งาน รวมทั้งห้ามเผยแพร่แจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่านของตนเอง				
2.ไม่อนุญาติให้ผู้อื่นเข้าใช้งานชื่อบัญชีผู้ใช้งาน และรหัสผ่านในกรณีที่ใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน ให้ทำการลงชื่อออก ทันทีหลังการใช้งาน				
3.ห้ามนำข้อมูลผู้ป่วยออกนอกโรงพยาบาล อาทิเช่น ข้อมูลการรักษา ข้อมูลผลตรวจทางห้องปฏิบัติการ โดยไม่ได้รับอนุญาตจากผู้อำนวยการ หรือผู้ที่ได้รับมอบอำนาจแทน				
4.ห้ามติดตั้ง แก้ไข เปลี่ยนแปลง เคลื่อนย้าย คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ตลอดจนโปรแกรม				
5.ห้ามนำเข้าหรือส่งออกข้อมูลผ่านอุปกรณสำรองข้อมูลภายนอก เช่น Flash drive, External Hard disk กับเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านคา				
6.ห้ามเปิดหรือใช้งานเครื่องคอมพิวเตอร์เพื่อการบันเทิง ทำธุรกิจหรือหาผลประโยชน์ส่วนตัว เช่น Facebook TikTok การดูหนัง การเล่นเกมส์ เป็นต้น				
7.ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line และเว็บไซด์ต่างๆ หรือโปรแกรมอื่นที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อการรักษาผู้ป่วยเท่านั้น โดยปฏิบัติตามแนวทางปฏิบัติกรณีมีการส่งต่อข้อมูลผู้ป่วยโดยสื่อสังคมออนไลน์				
8.หัวหน้าฝ่าย/งาน ควบคุมกำกับช่องทางการสื่อสารออนไลน์ขององค์กรและหน่วยงาน				
9.ไม่อนุญาตให้ใช้บัญชีส่วนตัวในการส่งต่อข้อมูลโดยไม่จำเป็น				
10.การส่งต่อข้อมูลทั้งภาพและข้อความที่เป็นการระบุตัวบุคคล ต้องดำเนินการลบภายใน 24 ชั่วโมงหลังประบวนการรักษาเสร็จสิ้น				
11.ผู้มีสิทธิในการส่งข้อมูล คือแพทย์ผู้รักษาและผู้ที่ได้รับมอบหมายเป็นกรณีไป				
12.การสื่อสารใดๆ ที่เกิดขึ้น ไม่อนุญาตให้มีการบันทึกในรูปแบบต่างๆ หรือถ่ายภาพ ยกเว้นในกรณีเพื่อการรักษา				

คำถามการรับรู้

ข้อคำถามการรู้	ข้อคำถามการปฏิบัติ
1.ผู้ใช้งานมีหน้าที่จัดเก็บและรักษาชื่อบัญชีผู้ใช้งาน รวมทั้งห้ามเผยแพร่แจกจ่ายให้ผู้อื่นล่วงรู้รหัสผ่านของตนเอง	ท่านเก็บรักษา user/password และมิให้ผู้อื่นล่วงรู้ใช่หรือไม่ (ทุกระบบที่มีการยืนยันการเข้าใช้งาน เช่น HOSxP/Web Service) ทำ ทำบางครั้ง ไม่ทำเลย
2.ไม่อนุญาติให้ผู้อื่นเข้าใช้งานชื่อบัญชีผู้ใช้งาน และรหัสผ่านในกรณีที่ใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน ให้ทำการลงชื่อออก ทันทีหลังการใช้งาน	ท่านปิดโปรแกรมทุกครั้ง ทันทีหลังเลิกใช้งาน ใช่ / ไม่ใช่
3.ห้ามนำข้อมูลผู้ป่วยออกนอกโรงพยาบาล อาทิเช่น ข้อมูลการรักษา ข้อมูลผลตรวจทางห้องปฏิบัติการ โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ที่ได้รับมอบอำนาจแทน	ท่านนำข้อมูลการรักษาออกนอกโรงพยาบาล อาทิเช่น ข้อมูลการรักษา ข้อมูลผลตรวจทางห้องปฏิบัติการ โดยไม่ได้รับอนุญาตจากผู้อำนวยการ หรือผู้ที่ได้รับมอบอำนาจแทน ไม่ / ไม่ใช่
4.ห้ามติดตั้ง แก้ไข เปลี่ยนแปลง เคลื่อนย้าย คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ตลอดจนโปรแกรม	ท่านแจ้งศูนย์คอมก่อนการ ติดตั้ง แก้ไข เปลี่ยนแปลง เคลื่อนย้าย คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ตลอดจนโปรแกรม ใช่ / ไม่ใช่
5.ห้ามนำเข้าหรือส่งออกข้อมูลผ่านอุปกรณสำรองข้อมูลภายนอก เช่น Flash drive, External Hard disk กับเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านคา	ท่านนำเข้าหรือส่งออกข้อมูลผ่านอุปกรณสำรองข้อมูลภายนอก เช่น Flash drive, External Hard disk กับเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านคา ใช่ / ไม่ใช่
6.ห้ามเปิดหรือใช้งานเครื่องคอมพิวเตอร์เพื่อการบันเทิง ทำธุรกิจหรือหาผลประโยชน์ส่วนตัว เช่น Facebook TikTok การดูหนัง การเล่นเกมส์ เป็นต้น	ท่านเปิดหรือใช้งานเครื่องคอมพิวเตอร์เพื่อการบันเทิง ทำธุรกิจหรือหาผลประโยชน์ส่วนตัว เช่น Facebook TikTok การดูหนัง การเล่นเกมส์ เป็นต้น ใช่ / ไม่ใช่
7.ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line และเว็บไซต์ต่างๆ หรือโปรแกรมอื่นที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อการรักษาผู้ป่วยเท่านั้น โดยปฏิบัติตามแนวทางปฏิบัติกรณีมีการส่งต่อข้อมูลผู้ป่วยโดยสื่อสังคมออนไลน์	ท่านเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line และเว็บไซต์ต่างๆ หรือโปรแกรมอื่นที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อการรักษาผู้ป่วยเท่านั้น โดยปฏิบัติตามแนวทางปฏิบัติกรณีมีการส่งต่อข้อมูลผู้ป่วยโดยสื่อสังคมออนไลน์ ใช่/ไม่ใช่

ข้อคำถามการรู้	ข้อคำถามการปฏิบัติ
8.หัวหน้าฝ่าย/งาน ควบคุมกำกับช่องทางการสื่อสารออนไลน์ขององค์กรและหน่วยงาน	หัวหน้าฝ่าย/งาน ของท่านควบคุมกำกับช่องทางการสื่อสารออนไลน์ขององค์กรและหน่วยงาน ท่านติดต่อสื่อสารผ่านช่องทางที่องค์การกำหนด ใช่/ไม่ใช่
9.ไม่อนุญาตให้ใช้บัญชีส่วนตัวในการส่งต่อข้อมูลโดยไม่จำเป็น	ท่านใช้บัญชีส่วนตัวในการส่งต่อข้อมูลโดยไม่จำเป็น ใช่/ไม่ใช่ กลุ่มไม่ทำ
10.การส่งต่อข้อมูลทั้งภาพและข้อความที่เป็นการระบุตัวบุคคล ต้องดำเนินการลบภายใน 24 ชั่วโมงหลังประบวนการรักษาเสร็จสิ้น	ท่านลบข้อมูลการส่งต่อข้อมูลทั้งภาพและข้อความที่เป็นการระบุตัวบุคคลภายใน 24 ชั่วโมงหลังประบวนการรักษาเสร็จสิ้น ใช่/ไม่ใช่
11.ผู้มีสิทธิในการส่งข้อมูล คือแพทย์ผู้รักษาและผู้ที่ได้รับมอบหมายเป็นกรณีไป	ท่านส่งต่อข้อมูลโดยไม่มีสิทธิการส่งต่อข้อมูลหรือไม่ ใช่/ไม่ใช่
12.การสื่อสารใดๆ ที่เกิดขึ้น ไม่อนุญาตให้มีการบันทึกในรูปแบบต่างๆ หรือถ่ายภาพ ยกเว้นในกรณีเพื่อการรักษา	ท่านมีการบันทึกข้อมูลการสื่อสารในรูปแบบต่างๆ หรือถ่ายภาพ ที่มิใช่เพื่อการรักษาหรือไม่ ใช่/ไม่ใช่

สรุปผลการประเมินการรับรู้ และ การละเมิด ระเบียบในการรักษาความปลอดภัย ด้านเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านคา ปี พ.ศ. ๒๕๖๗

ลำดับ	ระเบียบปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ / แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๑	ผู้ใช้งานมีหน้าที่จัดเก็บและรักษาชื่อบัญชีผู้ใช้งาน รวมทั้งห้ามเผยแพร่ แจกจ่ายให้ผู้อื่นล่วงรู้ รหัสผ่านของตนเอง	๑๑๗	๑๐๐%	๐	๐	๔	๓.๔๒	๑๑๓	๙๖.๕๘	เก็บรักษา user/password และมิให้ผู้อื่นล่วงรู้
๒	ไม่อนุญาตให้ผู้อื่นเข้าใช้งาน ชื่อบัญชีผู้ใช้งาน และรหัสผ่านในกรณีที่ใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน ให้ทำการลงชื่อออก ทันทีหลังการใช้งาน	๑๑๗	๑๐๐%	๐	๐	๑๑	๙.๔๐	๑๐๖	๙๐.๖๐	แจ้งผู้ละเมิดให้ตระหนัก รับรู้ว่า กรณีเกิดปัญหากับระบบ HOSxP หรือเครื่องคอมพิวเตอร์ จะต้องเป็นผู้รับผิดชอบทั้งหมดที่เกิดขึ้น

ลำดับ	ระเบียบปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ / แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๓	ห้ามนำข้อมูลผู้ป่วยออกนอกโรงพยาบาล อาทิเช่น ข้อมูลการรักษา ข้อมูลผลตรวจทางห้องปฏิบัติการ โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ที่ได้รับมอบอำนาจแทน	๑๑๗	๑๐๐	๐	๐	๕	๔.๒๗	๑๑๒	๙๕.๗๓	นำข้อมูลการรักษาออกนอกโรงพยาบาล อาทิเช่น ข้อมูลการรักษา ข้อมูลผลตรวจทางห้องปฏิบัติการ ต้องได้รับอนุญาตจากผู้อำนวยการ หรือผู้ที่ได้รับมอบอำนาจแทน
๔	ห้ามติดตั้ง แก้ไข เปลี่ยนแปลง เคลื่อนย้าย คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ตลอดจนโปรแกรม	๑๑๗	๑๐๐	๐	๐	๐	๐	๑๑๗	๑๐๐	แจ้งศูนย์คอมก่อนการ ติดตั้ง แก้ไข เปลี่ยนแปลง เคลื่อนย้าย คอมพิวเตอร์ อุปกรณ์ต่อพ่วง ตลอดจนโปรแกรม
๕	ห้ามนำเข้าหรือส่งออกข้อมูลผ่านอุปกรณสำรองข้อมูลภายนอก เช่น Flash drive, External Hard disk กับเครื่องคอมพิวเตอร์ของโรงพยาบาลบ้านคา	๑๑๗	๑๐๐	๐	๐	๐	๐	๑๑๗	๑๐๐	ปิดช่องทางนำ เข้า / ออก ข้อมูลได้แก่ USB
๖	ห้ามเปิดหรือใช้งานเครื่องคอมพิวเตอร์เพื่อการบันเทิง ทำธุรกิจหรือหาผลประโยชน์ส่วนตัว เช่น Facebook TikTok การดูหนัง การเล่นเกมส์ เป็นต้น	๑๑๗	๑๐๐	๐	๐	๒๓	๑๙.๖๖	๙๔	๘๐.๓๔	บล็อก Facebook TikTok เว็บหนัง, การ์ตูน,เกมส์

ลำดับ	ระเบียบปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ / แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๗	ห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line และเว็บไซต์ต่างๆ หรือโปรแกรมอื่นที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อการรักษาผู้ป่วยเท่านั้น โดยปฏิบัติตามแนวทางปฏิบัติกรณีมีการส่งต่อข้อมูลผู้ป่วยโดยสื่อสังคมออนไลน์	๑๑๗	๑๐๐	๐	๐	๓	๒.๕๖	๑๑๔	๙๗.๔๔	เผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์(Social Media) เช่น Facebook, Line และเว็บไซต์ต่างๆ หรือโปรแกรมอื่นที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อการรักษาผู้ป่วยเท่านั้น โดยปฏิบัติตามแนวทางปฏิบัติกรณีมีการส่งต่อข้อมูลผู้ป่วยโดยสื่อสังคมออนไลน์
๘	หัวหน้าฝ่าย/งาน ควบคุมกำกับช่องทางการสื่อสารออนไลน์ขององค์กรและหน่วยงาน	๑๑๗	๑๐๐	๐	๐	๐	๐	๑๑๗	๑๐๐	หัวหน้าฝ่าย/งานควบคุมกำกับช่องทางการสื่อสารออนไลน์ของหน่วยงาน ผู้ใช้ติดต่อสื่อสารผ่านช่องทางที่องค์การกำหนด
๙	ไม่อนุญาตให้ใช้บัญชีส่วนตัวในการส่งต่อข้อมูลโดยไม่จำเป็น	๑๑๗	๑๐๐	๐	๐	๑๐	๘.๕๕	๑๐๗	๙๑.๔๕	ไม่ใช้บัญชีส่วนตัวในการส่งต่อข้อมูลโดยไม่จำเป็น
๑๐	การส่งต่อข้อมูลทั้งภาพและข้อความที่เป็นการระบุตัวบุคคล ต้องดำเนินการลบภายใน ๒๔ ชั่วโมงหลังกระบวนการรักษาเสร็จสิ้น	๑๑๗	๑๐๐	๐	๐	๑	๐.๘๕	๑๑๖	๙๙.๑๕	ลบข้อมูลการส่งต่อข้อมูลทั้งภาพและข้อความที่เป็นการระบุตัวบุคคลภายใน ๒๔ ชั่วโมงหลังกระบวนการรักษาเสร็จสิ้น

ลำดับ	ระเบียบปฏิบัติ	รับรู้		ไม่รับรู้		ละเมิด		ไม่ละเมิด		มาตรการ / แนวทางแก้ไข
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	จำนวน	ร้อยละ	
๑๑	ผู้มีสิทธิในการส่งข้อมูล คือ แพทย์ผู้รักษาและผู้ที่ได้รับมอบหมายเป็นกรณีไป	๑๑๗	๑๐๐	๐	๐	๒๓	๑๙.๖๖	๙๔	๘๐.๓๔	การส่งต่อข้อมูลจะต้องมีสิทธิการส่งต่อข้อมูลเท่านั้น
๑๒	การสื่อสารใดๆ ที่เกิดขึ้น ไม่อนุญาตให้มีการบันทึกในรูปแบบต่างๆ หรือถ่ายภาพ ยกเว้นในกรณีเพื่อการรักษา	๑๑๗	๑๐๐	๐	๐	๐	๐	๑๑๗	๑๐๐	การบันทึกข้อมูลการสื่อสารในรูปแบบต่างๆ หรือถ่ายภาพ ที่มิใช่เพื่อการรักษา

แนวทางการปรับปรุง
ห้อง SERVER

แนวทางการปรับปรุงห้อง SERVER

ทรัพยสิน	สถานการณ์ปัจจุบัน	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ชวงเวลาดำเนินการ
SERVER แม่ข่าย อัพเกรด จัดทำระบบ RAID ๑๐ เพื่อให้มีประสิทธิภาพมากขึ้น	- HDD เสีย ระบบจะไม่สามารถ RUN ต่อได้ - ไม่สามารถใช้งาน HOSxP ได้	เพิ่มประสิทธิภาพ SERVER จัดทำระบบ Raid ๑๐ - HDD ๖ ลูก (๙๖๐ GB) เป็นเงิน ๙๓,๐๐๐ บาท - RAM ๓๒ GB (๑๖*๑๖) เป็นเงิน ๑๑,๐๐๐ บาท - Kvm switch ๔ Port เป็นเงิน ๒,๐๐๐ บาท	นายสุริยา บุญเลิศฟ้า	๑๐๖,๐๐๐	ดำเนินการเรียบร้อย
ห้อง DATA CENTER	- ไฟไหม้ - ถูกขโมย	ระบบรักษาความปลอดภัย DATA CENTER จัดทำระบบป้องกันอุณหภูมิห้อง (อัคคีภัย) - ถังดับเพลิงอัตโนมัติ ๒ ถัง - ตัวดักจับควัน - ตัววัดอุณหภูมิ เป็นเงิน ๗๒,๑๕๐ บาท	นายสุริยา บุญเลิศฟ้า	๗๒,๑๕๐	ดำเนินการเรียบร้อย

แนวทางการปรับปรุงห้อง SERVER

ทรัพยสิน	สถานการณ์ปัจจุบัน	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ชวงเวลาดำเนินการ
UPS SERVER	- ไฟฟ้าลัดวงจร	บำรุงรักษา UPS SERVER - ๓ kVA แบตเตอรี่ ๑๐ ก้อน เป็นเงิน ๙,๕๐๐ บาท - สะพานไฟอย่างดี ๑ อัน เป็นเงิน ๓,๐๐๐ บาท	นายสุริยา บุญเลิศฟ้า	๑๒,๕๐๐	ดำเนินการเรียบร้อย
		เพิ่ม UPS SERVER ๓ kVM เดิมมี UPS ขนาด ๓kVM ๑ ตัว กรณี UPS ไม่ทำงานหรือเสียจะไม่มี UPS ให้สำหรับ SERVER เป็นเงิน ๓๒,๐๐๐ บาท	นายสุริยา บุญเลิศฟ้า	๗๒,๐๐๐	ดำเนินการเรียบร้อย

รอดำเนินการปรับปรุงห้อง SERVER
DATA CENTER DR SITE

ทรัพยสิน	สถานการณ์ปัจจุบัน	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ชวงเวลาดำเนินการ
ห้อง SERVER DATA CENTER DR Site	ยังไม่มี DATA CENTER DR Site	สร้างห้อง DATA CENTER DR Site แยกตึก จาก SERVER MASTER	นายสุริยา บุญเลิศฟ้า นายอนุพงศ์ ทองบ้านกวย	ราคาประมาณการ ๓๐๐,๐๐๐	ตุลาคม ๒๕๖๘ ถึง กันยายน ๒๕๖๙
SERVER Slave	อายุการใช้งาน >๕ ปี CPU ๑๐ Core RAM ๓๒ STORAGE ๑ TB	จัดซื้อ เพิ่มในโครงการพัฒนาระบบสารสนเทศ	นายสุริยา บุญเลิศฟ้า นายอนุพงศ์ ทองบ้านกวย	ราคากลาง ICT ๓๕๐,๐๐๐ บาท	ตุลาคม ๒๕๖๘ ถึง กันยายน ๒๕๖๙
UPS SERVER ๓ KVA	ยังไม่มี	จัดซื้อ เพิ่มในโครงการพัฒนาระบบสารสนเทศ UPS ๓ KVA	นายสุริยา บุญเลิศฟ้า นายอนุพงศ์ ทองบ้านกวย	ราคากลาง ICT ๓๒,๐๐๐ บาท ๒ เครื่อง ปีงบ ๒๕๖๘ = ๖๔,๐๐๐ บาท	ตุลาคม ๒๕๖๘ ถึง กันยายน ๒๕๖๙
Switch Layer ๒	ยังไม่มี	จัดซื้อ เพิ่มในโครงการพัฒนาระบบสารสนเทศ Switch Layer ๒	นายสุริยา บุญเลิศฟ้า นายอนุพงศ์ ทองบ้านกวย	ราคากลาง ICT ๑๓,๐๐๐ บาท ๑ เครื่อง	ตุลาคม ๒๕๖๘ ถึง กันยายน ๒๕๖๙