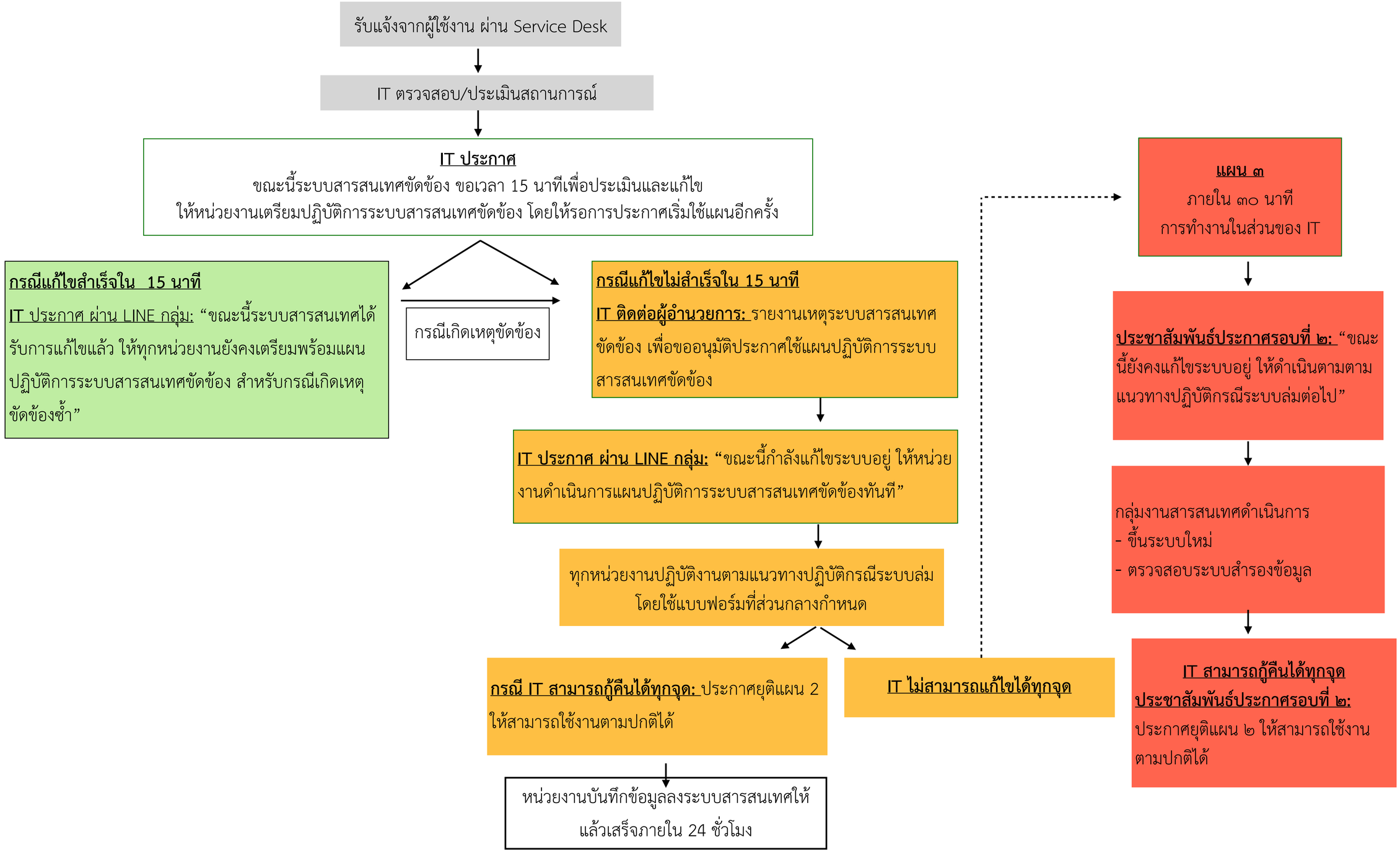
บทที่ 3

การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

Security Management in Hospital Information System

แผนปฏิบัติการระบบสารสนเทศขัดข้อง (BCP)


รับแจ้งจากผู้ใช้งาน ผ่าน Service Desk
IT ตรวจสอบ/ประเมินสถานการณ์
IT ประกาศ
ขณะนี้ระบบสารสนเทศขัดข้อง ขอเวลา 15 นาทีเพื่อประเมินและแก้ไข
ให้หน่วยงานเตรียมปฏิบัติการระบบสารสนเทศขัดข้อง โดยให้รอการประกาศเริ่มใช้แผนอีกครั้ง
กรณีแก้ไขสำเร็จใน 15 นาที
IT ประกาศ ผ่าน LINE กลุ่ม: “ขณะนี้ระบบสารสนเทศได้รับการแก้ไขแล้ว ให้ทุกหน่วยงานยังคงเตรียมพร้อมแผนปฏิบัติการระบบสารสนเทศขัดข้อง สำหรับกรณีเกิดเหตุขัดข้องซ้ำ”
กรณีเกิดเหตุขัดข้อง
กรณีแก้ไขไม่สำเร็จใน 15 นาที
IT ติดต่อผู้อำนวยการ: รายงานเหตุระบบสารสนเทศขัดข้อง เพื่อขออนุมัติประกาศใช้แผนปฏิบัติการระบบสารสนเทศขัดข้อง
IT ประกาศ ผ่าน LINE กลุ่ม: “ขณะนี้กำลังแก้ไขระบบอยู่ ให้หน่วยงานดำเนินการแผนปฏิบัติการระบบสารสนเทศขัดข้องทันที”
ทุกหน่วยงานปฏิบัติงานตามแนวทางปฏิบัติกรณีระบบล่ม
โดยใช้แบบฟอร์มที่ส่วนกลางกำหนด
กรณี IT สามารถกู้คืนได้ทุกจุด: ประกาศยุติแผน 2 ให้สามารถใช้งานตามปกติได้
หน่วยงานบันทึกข้อมูลลงระบบสารสนเทศให้แล้วเสร็จภายใน 24 ชั่วโมง
IT ไม่สามารถแก้ไขได้ทุกจุด
แผน ๓
ภายใน ๓๐ นาที
การทำงานในส่วนของ IT
ประชาสัมพันธ์ประกาศรอบที่ ๒: “ขณะนี้ยังคงแก้ไขระบบอยู่ ให้ดำเนินตามตามแนวทางปฏิบัติกรณีระบบล่มต่อไป”
กลุ่มงานสารสนเทศดำเนินการ
- ขึ้นระบบใหม่
- ตรวจสอบระบบสำรองข้อมูล
IT สามารถกู้คืนได้ทุกจุด
ประชาสัมพันธ์ประกาศรอบที่ ๒:
ประกาศยุติแผน ๒ ให้สามารถใช้งานตามปกติได้

ระบบสำรองข้อมูลผู้ป่วย ขณะเกิดเหตุการณ์ระบบสารสนเทศขัดข้อง

OPD

นโยบายและระเบียบปฏิบัติ
ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

- กรณีระบบกลับมาสู่ปกติแล้ว ผู้ป่วยที่ได้รับการรักษาด้วยระบบ manual ไปแล้ว ให้คงการใช้การรักษาด้วยระบบ manual ต่อไปจนจบขั้นตอน
- กรณีเกิดเกตุขัดข้องระหว่างการรักษาโดยที่ได้ใช้ระบบแบบปกติรักษาไปแล้วบางส่วน
  จุดผู้ป่วยรอตรวจ/รอซักประวัติ —> ส่งให้ห้องบัตรบันทึกใหม่แบบ Manual ส่งไป OPD
  จุดรอยา —> ห้องจดรายการยาที่แพทย์สั่งไปแล้วที่ห้องตรวจ 1
- ทุกหน่วยงานมีแบบบันทึกจดชื่อและ HN ผป.ทุกคนที่เข้ารับบริการหน่วยตนเอง สำหรับตรวจสอบความครบถ้วนในการลงข้อมูลย้อนหลัง หลังระบบกลับมาเป็นปกติแล้ว

นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

- โรงพยาบาลจะยึดถือและปฏิบัติตามข้อกำหนดในกฎหมายเทคโนโลยีสารสนเทศของประเทศ ขั้นตอนของการบริหารจัดการระบบสารสนเทศของโรงพยาบาล
- โรงพยาบาลจะวางแผนและดำเนินการพัฒนาศักยภาพระบบสารสนเทศอย่างต่อเนื่องเพื่อให้ระบบมีประสิทธิภาพและทันสมัยตามเทคโนโลยีที่ก้าวหน้าอย่างเหมาะสม
- โรงพยาบาลจะกำกับ และควบคุมการใช้งานระบบสารสนเทศของบุคลากรในโรงพยาบาลให้เป็นไปอย่างเหมาะสม และจำกัดสิทธิ์เข้าถึงข้อมูลเท่าที่จำเป็น เพื่อลดโอกาสการนำข้อมูลของโรงพยาบาลไปใช้ในทางที่เสียหาย
- โรงพยาบาลจะบริหารจัดการระบบรักษาความปลอดภัยของระบบสารสนเทศ เพื่อลดความเสี่ยงจากการถูกโจมตีจากสิ่งคุมคามภายนอก รวมทั้งการจัดเก็บรักษาข้อมูลสำคัญไว้อย่างมีประสิทธิภาพ
- โรงพยาบาลจะยึดถือหลักการในการปกปิดข้อมูลของผู้ป่วยตามคำประกาศสิทธิของผู้ป่วยมาเป็นหลักสำคัญในการจัดการระบบสารสนเทศ
- โรงพยาบาลจะเผยแพร่ข้อมูลที่มีความสำคัญและเป็นประโยชน์ต่อบุคลากร ผู้รับบริการของโรงพยาบาล หรือองค์กรอื่นๆที่ร้องขอ โดยอาศัยช่องทางที่เหมาะสมกับข้อมูล

อาจารย์สุ่ม ให้จนท.ท่อง ให้ฟัง

หน่วยงาน Download แบบฟอร์มจาก Intranet และพิมพ์สำรองเอกสารเก็บไว้

ระเบียบปฏิบัติ
ความมั่นคงปลอดภัยด้านไซเบอร์

DO's

ต้อง ลงทะเบียนบัญชีผู้ใช้ระบบ
Internet HOSxP และ HosMerge ทุกคน

3 months

ต้อง ตั้งรหัสผ่านของตนเองและเปลี่ยนใหม่
ทุกๆ 3 เดือน

aAaaa111

ต้อง กำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร
โดยประกอบด้วยตัวเลข
พยัญชนะตัวพิมพ์เล็กและตัวพิมพ์ใหญ่

ต้อง ออกระบบทุกครั้งหลังใช้งาน
Internet HOSxP และ HosMerge เสร็จ

ต้อง ยื่นคำขอแจ้งขออนุญาตผู้ดูแลระบบ
ก่อนนำคอมพิวเตอร์ อุปกรณ์ต่อพ่วง
มาเชื่อมต่อระบบของโรงพยาบาล

DON'Ts

ห้าม เปิดเผย username และ password ของตนเอง

ห้าม เข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ
โดยไม่ได้รับอนุญาตจากผู้รับผิดชอบโดยตรง

ห้าม ส่งต่อหรือเปิดเผยข้อมูลผู้ป่วย ต่อสาธารณะและ
Social media ต่างๆ ก่อนได้รับคำยินยอมจากผู้ป่วย
หรือญาติเป็นลายลักษณ์อักษร

ห้าม ใช้ระบบ internet ของรพ.เข้าสู่เว็บไซต์ที่ไม่เหมาะสม
เช่น เว็บลามกอนาจาร การพนัน เป็นต้น

ห้าม Download โปรแกรมจาก internet หรือ update
โปรแกรมต่างๆนอกจากผู้ดูแลระบบอนุญาต

ห้าม เคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆต่อ
อุปกรณ์ของรพ.โดยไม่ได้รับอนุญาต

ห้าม นำอาหารหรือเครื่องดื่ม วางใกล้อุปกรณ์คอมพิวเตอร์
หรืออุปกรณ์เครือข่ายคอมพิวเตอร์

โรงพยาบาลสมเด็จพระยุพราชยะหา

ระเบียบปฏิบัติ
ความมั่นคงปลอดภัยด้านไซเบอร์

DO's

ต้อง ลงทะเบียนบัญชีผู้ใช้ระบบ Internet HOSxP และ HosMerge ทุกคน

3 months

ต้อง ตั้งรหัสผ่านของตนเองและเปลี่ยนใหม่ **ทุกๆ 3 เดือน**

aAaaa111

ต้อง กำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร โดยประกอบด้วยตัวเลข พยัญชนะตัวพิมพ์เล็กและตัวพิมพ์ใหญ่

ต้อง ออกระบบทุกครั้งหลังใช้งาน Internet HOSxP และ HosMerge เสร็จ

ต้อง ยื่นคำขอแจ้งขออนุญาตผู้ดูแลระบบ ก่อนนำคอมพิวเตอร์ อุปกรณ์ต่อพ่วง มาเชื่อมต่อระบบของโรงพยาบาล

DON'Ts

ห้าม เปิดเผย username และ password ของตนเอง

ห้าม เข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ได้รับอนุญาตจากผู้รับผิดชอบโดยตรง

ห้าม ส่งต่อหรือเปิดเผยข้อมูลผู้ป่วย ต่อสาธารณะและ Social media ต่างๆ ก่อนได้รับคำยินยอมจากผู้ป่วย หรือญาติเป็นลายลักษณ์อักษร

ห้าม ใช้ระบบ internet ของรพ.เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บลามกอนาจาร การพนัน เป็นต้น

ห้าม Download โปรแกรมจาก internet หรือ update โปรแกรมต่างๆนอกจากผู้ดูแลระบบอนุญาต

ห้าม เคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆต่ออุปกรณ์ของรพ.โดยไม่ได้รับอนุญาต

ห้าม นำอาหารหรือเครื่องดื่ม วางใกล้อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่ายคอมพิวเตอร์

โทษการไม่ปฏิบัติตามระเบียบปฏิบัติ ผู้ฝ่าฝืนต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้น เช่น

- เป็นผู้รับผิดชอบ หากเกิด Med error กรณีไม่ได้ลงชื่อออก หรือให้บัญชีของตนเองให้ผู้อื่นใช้
- ชดใช้ค่าเสียหาย กรณีอุปกรณ์ไฟฟ้าชำรุดจาก น้ำ อาหารหกใส่

โรงพยาบาลสมเด็จพระยุพราชยะหา

ระเบียบปฏิบัติ
ความมั่นคงปลอดภัยด้านไซเบอร์

DO's

ต้อง ลงทะเบียนบัญชีผู้ใช้ระบบ Internet HOSxP และ HosMerge ทุกคน

3 months

ต้อง ตั้งรหัสผ่านของตนเองและเปลี่ยนใหม่ **ทุกๆ 3 เดือน**

aAaaa111

ต้อง กำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร โดยประกอบด้วยตัวเลข พยัญชนะตัวพิมพ์เล็กและตัวพิมพ์ใหญ่

DON'Ts

ห้าม เปิดเผย username และ password ของตนเอง

ห้าม เข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ โดยไม่ได้รับอนุญาตจากผู้รับผิดชอบโดยตรง

ห้าม ส่งต่อหรือเปิดเผยข้อมูลผู้ป่วย ต่อสาธารณะและ Social media ต่างๆ ก่อนได้รับคำยินยอมจากผู้ป่วย หรือญาติเป็นลายลักษณ์อักษร

ห้าม ใช้ระบบ internet ของรพ.เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บลามกอนาจาร การพนัน เป็นต้น

สุ่มคนให้ log in อาจารย์จับสังเกต:

- มีบัญชีของตนเองมั้ย
- จำนวนตัวอักษรของรหัสที่พิมพ์ เท่าจำนวนที่ระเบียบกำหนดไหม

ระเบียบปฏิบัติ
ความมั่นคงปลอดภัยด้านไซเบอร์

DO's

ต้อง ลงทะเบียนบัญชีผู้ใช้ระบบ
Internet HOSxP และ HosMerge ทุกคน

3 months

ต้อง ตั้งรหัสผ่านของตนเองและเปลี่ยนใหม่
ทุกๆ 3 เดือน

aAaaa111

ต้อง กำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร
โดยประกอบด้วยตัวเลข
พยัญชนะตัวพิมพ์เล็กและตัวพิมพ์ใหญ่

DON'Ts

ห้าม เปิดเผย username และ password ของตนเอง

- ห้ามมีรหัสแปะตามโต๊ะคอม หรือที่ใดๆ
- ห้ามมีรหัสเซฟไว้ในคอม

ห้าม เข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ
โดยไม่ได้รับอนุญาตจากผู้รับผิดชอบโดยตรง

ห้าม ส่งต่อหรือเปิดเผยข้อมูลผู้ป่วย ต่อสาธารณะและ
Social media ต่างๆ ก่อนได้รับคำยินยอมจากผู้ป่วย
หรือญาติเป็นลายลักษณ์อักษร

- รวมถึงห้ามส่งต่อข้อมูลผู้ผ่านกลุ่มไลน์ต่างๆ เช่น กลุ่มไลน์มีจนท.หลายรพ.
  = เป็นการส่งข้อมูลผู้ป่วยให้ผู้ไม่เกี่ยวข้อง

ห้าม ใช้ระบบ internet ของรพ.เข้าสู่เว็บไซต์ที่ไม่เหมาะสม
เช่น เว็บลามกอนาจาร การพนัน เป็นต้น

ต้อง ลงทะเบียนบัญชีผู้ใช้ระบบ
Internet HOSxP และ HosMerge ทุกคน

3 months

ต้อง ตั้งรหัสผ่านของตนเองและเปลี่ยนใหม่
ทุกๆ 3 เดือน

aAaaa111

ต้อง กำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร
โดยประกอบด้วยตัวเลข
พยัญชนะตัวพิมพ์เล็กและตัวพิมพ์ใหญ่

ต้อง ออกระบบทุกครั้งหลังใช้งาน
Internet HOSxP และ HosMerge เสร็จ

ต้อง ยื่นคำขอแจ้งขออนุญาตผู้ดูแลระบบ
ก่อนนำคอมพิวเตอร์ อุปกรณ์ต่อพ่วง
มาเชื่อมต่อระบบของโรงพยาบาล

ห้าม เข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบ
โดยไม่ได้รับอนุญาตจากผู้รับผิดชอบโดยตรง

ห้าม ส่งต่อหรือเปิดเผยข้อมูลผู้ป่วย ต่อสาธารณะและ
Social media ต่างๆ ก่อนได้รับคำยินยอมจากผู้ป่วย
หรือญาติเป็นลายลักษณ์อักษร

ห้าม ใช้ระบบ internet ของรพ.เข้าสู่เว็บไซต์ที่ไม่เหมาะสม
เช่น เว็บลามกอนาจาร การพนัน เป็นต้น

ห้าม Download โปรแกรมจาก internet หรือ update
โปรแกรมต่างๆนอกจากผู้ดูแลระบบอนุญาต

ห้าม เคลื่อนย้าย ติดตั้งเพิ่มเติม หรือกระทำการใดๆต่อ
อุปกรณ์ของรพ.โดยไม่ได้รับอนุญาต

ห้าม นำอาหารหรือเครื่องดื่ม วางใกล้อุปกรณ์คอมพิวเตอร์
หรืออุปกรณ์เครือข่ายคอมพิวเตอร์

- อาจเดินสำรวจหน่วยงาน จนท.ที่ปฏิบัติงาน
อยู่ ใช้ชื่อบัญชีผู้ใช้เป็นชื่อตนเองไหม

- สำรวจพื้นที่โต๊ะรอบๆอย่าให้มีเครื่องดื่ม อาหาร
วางไกล้อุปกรณ์ไฟฟ้า คอมพิวเตอร์