ประกาศโรงพยาบาลวังโป่ง

เรื่อง ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล

ระดับผู้ใช้งานสารสนเทศ

เพื่อการดำเนินงานระบบสารสนเทศของโรงพยาบาลวังโป่งมีความปลอดภัยด้านมาตรฐานเทคโนโลยีสารสนเทศ

1. เจ้าหน้าที่ทุกคนมีหน้าที่ต้องป้องกันดูแลรักษาไว้ซึ่งความลับความถูกต้องและความพร้อมใช้ของข้อมูลตลอดจนเอกสารเวชระเบียนของผู้ป่วย
2. ห้ามเผยแพร่ทำสำเนาถ่ายภาพเปลี่ยนแปลงลบทิ้งหรือทำลายข้อมูลผู้ป่วยในเวชระเบียนและในระบบคอมพิวเตอร์ทุกกรณีนอกจากได้รับมอบหมายให้ดำเนินการจากผู้อำนวยการ
3. การส่งข้อมูลผู้ป่วยให้กับบุคลากรภายในสถานพยาบาลเดียวกันให้ดำเนินการตามระเบียบการส่งข้อมูลลับโดยเคร่งครัดเช่น ไม่ให้ผู้ป่วยเป็นผู้ถือเวชระเบียนจากจุดบริการหนึ่งไปยังจุด อื่น ๆ
4. ตั้งรหัสผ่านในการเข้าใช้งานระบบคอมพิวเตอร์ของตนเองให้คาดเดาได้ยากตรงตามระเบียบของสถานพยาบาลปกปิดรหัสผ่านเป็นความลับส่วนตัวอย่างเคร่งครัดไม่อนุญาตให้ผู้อื่นนำรหัสผ่านของตนเองไปใช้เปลี่ยนรหัสผ่านเมื่อถึงกำหนดเวลาที่บังคับ
5. ห้ามใช้คอมพิวเตอร์ของสถานพยาบาลเปิดไฟล์จากภายนอกทุกกรณีสำหรับการเปิดไฟล์งานจากหน่วยงานภายในให้ตรวจสอบหาไวรัสภายในไฟล์ทุกครั้งก่อนเปิดไฟล์
6. ห้ามนำเครื่องคอมพิวเตอร์อุปกรณ์อื่นๆ รวมถึงอุปกรณ์จัดเก็บข้อมูลเช่น CD-ROM ,USB-Drive, Harddisk อุปกรณ์เครือข่ายเช่น HUB ,Switch ,Wi-Fi ,Router ฯลฯ มาเชื่อมต่อกับคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลที่ใช้ฐานข้อมูลผู้ป่วยยกเว้นได้รับอนุญาตจากดูแลระบบ
7. ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลที่เชื่อมต่อกับระบบฐานข้อมูลผู้ป่วยในการติดต่อกับอินเตอร์เน็ตทุกกรณียกเว้นเครื่องคอมพิวเตอร์ที่มีภารกิจเฉพาะที่ต้องเชื่อมต่ออินเตอร์เน็ตพร้อมกับการเชื่อมต่อระบบฐานข้อมูลผู้ป่วยซึ่งได้รับอนุญาตจากผู้อำนวยการ
8. ผู้ใช้งานห้ามทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดโดยที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบ
9. ห้ามผู้ใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิง เช่น ดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ
10. ผู้ใช้งานห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ
11. ผู้ใช้งานห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟสบุ๊ค (Facebook), ไลน์ (Line), เว็บไซต์ (Website) หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยหรือญาติซึ่งยินยอมเผยแพร่ได้เป็นครั้งคราวและในกรณี consult case ผู้ป่วยทางไลน์ ต้องปกปิดชื่อผู้ป่วยทุกราย
12. ผู้ใช้งานต้องรับผิดชอบป้องกันความเสียหาย ที่อาจจะเกิดขึ้นกับเครื่องคอมพิวเตอร์, ปริ้นเตอร์, ปลั๊กไฟ หรืออุปกรณ์อิเลคทรอนิกส์ เช่น ไม่วางอาหารหรือน้ำดื่มบนเครื่องคอมพิวเตอร์, ไม่ใช้งานปลั๊กไฟที่ชำรุด เป็นต้น

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศใช้ ณ วันที่ ๘ มกราคม พ.ศ. ๒๕๖๔

(นายสุรศักดิ์ จันทร์เกตุ)

นายแพทย์ชำนาญการ รักษาการในตำแหน่ง

ผู้อำนวยการโรงพยาบาลวังโป่ง

	วิธีปฏิบัติ เรื่อง การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโรงพยาบาลบัวเชด	หน่วยงาน: เทคโนโลยีสารสนเทศ
	ผู้อนุมัติ ผู้อำนวยการโรงพยาบาลวังโป่ง	รหัสเอกสาร:WP-CM-01 แก้ไขครั้งที่ 2 วันที่ 4 พ.ค.64

การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโรงพยาบาลวังโป่ง

1. จัดให้มีการทำ และปรับปรุงนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
2. แสดงเจตนารมณ์ หรือสื่อสารให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบาย ด้านความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรโดยเคร่งครัด อย่างสม่ำเสมอ
3. จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง โดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้
    - การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และวิเคราะห์ผลการตรวจสอบ
    - แผนการดำเนินการเชิงป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว
    - การปรับปรุงนโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับปีถัดไป
    - การประเมินความเสี่ยงและแผนลดความเสี่ยง จัดให้มีทรัพยากรด้านบุคลากรงบประมาณการบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการจัดการดังกล่าว
4. จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เจ้าหน้าที่ขององค์กร มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ 1 ครั้ง
5. จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อลดความเสี่ยง หรือปัญหาที่พบ
6. จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ โดยผู้ตรวจสอบภายในด้านสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ
7. จัดให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดได้ระมัดระวัง และดูแลทรัพย์สินขององค์กร ที่ตนเองใช้งานเพื่อป้องกันการสูญหาย อย่างน้อยปีละ 1 ครั้ง
8. กำหนดนโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างชัดเจนว่า บริการใดที่อนุญาตให้ใช้งาน และบริการใดไม่อนุญาตให้ใช้งาน เช่น การใช้งาน Socail ดูหนังฟังเพลงผ่านทางอินเตอร์เน็ต การอัฟโหลด/ดาวน์โหลด การติดตั้งโปรแกรม เป็นต้น รวมทั้งปรับปรุงนโยบายตามความจำเป็น นโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์ ขณะนี้ประกอบด้วย
9. ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้
    - วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์
    - การพนัน
    - ลามก อนาจาร
    - อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม

	ระเบียบปฏิบัติ เรื่อง การลงทะเบียนและควบคุมการเข้าถึงระบบข้อมูลผู้รับบริการ	หน่วยงาน: เทคโนโลยีสารสนเทศ
	ผู้อนุมัติ ผู้อำนวยการโรงพยาบาลวังโป่ง	รหัสเอกสาร:WP-CM-02 แก้ไขครั้งที่ 2 วันที่ 4 ม.ค.64

โรงพยาบาลวังโป่งใช้โปรแกรม HOSxP ในการจัดเก็บข้อมูลเวชระเบียนและการเข้ารับบริการของผู้ป่วยไว้ใน คอมพิวเตอร์ โดยมีระเบียบปฏิบัติดังนี้

1. กำหนดให้เจ้าหน้าที่และผู้ที่เกี่ยวข้อง ที่ทำหน้าที่บันทึกข้อมูลต่างๆ ลงในระบบคอมพิวเตอร์มีรหัสผ่าน Username/Accouunt และ password เพื่อการเข้าถึงระบบโปรแกรม HOSxP ของงานในแต่ละประเภท โดยรหัสที่กำหนดให้จะเข้าถึง(Access_menu) และใช้งานได้ เฉพาะงานในหน้าที่ของตนเองเท่านั้นไม่สามารถใช้งานในด้านอื่นที่ไม่เกี่ยว ข้องได้
2. เจ้าหน้าที่ของโรงพยาบาลทุกคนได้รับ การอบรม ในเรื่องการรักษาข้อมูลผู้ป่วย จรรยาบรรณในการไม่เปิดเผยข้อมูล ซึ่งจะต้องปฏิบัติตามระเบียบการขอประวัติการรักษาเวชระเบียนผู้ป่วย
3. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งานระบบโปรแกรม HOSxP ต้อง Log out ออกจากโปรแกรมทุกครั้งหากไม่ได้ปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ และงานคอมพิวเตอร์ได้ตั้งเวลาให้โปรแกรม Logout อัตโนมัติกรณีที่ไม่มีใช้งานเป็นเวลานานเกิน 10 นาที
4. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งานระบบโปรแกรม HOSxP ต้องเปลี่ยนรหัสผ่านใหม่ทุก 6เดือน และตั้งค่าโปรแกรมให้มีการแจ้งเตือนและล็อกค่า Password เดิมอัตโนมัติหากไม่มีการเปลี่ยนรหัสผ่านใหม่ภายในระยะเวลาที่กำหนด
5. กำหนดให้โปรแกรม HOSxP สามารถตรวจสอบเหตุผิดพลาด ของงานและสืบสวนย้อนกลับได้ว่ามีการเข้าถึง การบันทึกหรือแก้ไข ข้อมูลของผู้ป่วยที่อยู่ในคอมพิวเตอร์ โดยรหัสผู้ใช้ของใคร มีการดำเนินการเมื่อไหร่
6. กำหนดให้โปรแกรม HOSxP สามารถป้องกันการเข้าถึง ข้อมูลและการนำข้อมูลในคอมพิวเตอร์ไปใช้งานโดยไม่ได้รับอนุญาต เช่น จำกัดสิทธิการเข้าถึง เปิดเผย การ print รายงานข้อมูลประวัติผู้ป่วย, กำหนดเครื่องที่ใช้พิมพ์ใบเสร็จ เป็นต้น
7. กำหนดให้มีการติดตั้งโปรแกรมเพื่อป้องกัน และปกป้องข้อมูลจากไวรัส มัลแวร์ โทรจัน หนอนคอมพิวเตอร์ และตรวจสอบให้มีการ Update อัตโนมัติ
8. สำรวจสายไฟ สายแลนด์ ในหน่วยงานไม่ให้ชำรุดสามารถใช้งานได้อย่างปลอดภัย เพื่อป้องกันอัคคีภัย
9. มีการจำลองเหตุการณ์ ร่วมซ้อมแผนภาวะฉุกเฉินของโรงพยาบาล และเตรียมความพร้อมเมื่อเกิดเหตุการณ์ฉุกเฉิน และมีเหตุจำเป็นต้องขนย้ายเครื่องคอมพิวเตอร์แม่ข่าย Server
10. จัดให้มีอุปกรณ์ดับเพลิง และมีการตรวจสอบให้ใช้งานได้อย่างมีประสิทธิภาพเพื่อป้องกันหรือบรรเทาความเสียหายทางกายภาพที่อาจเกิดขึ้นของเวชระเบียน
11. ห้องจัดเก็บคอมพิวเตอร์แม่ข่าย Server ปรับปรุงมาตรฐานเทคโนโลยีสารสนเทศ ของโรงพยาบาล โดยจัดเก็บคอมพิวเตอร์แม่ข่าย Server ไว้ในตู้ Rack สำหรับขนย้าย ภายในห้องคอมพิวเตอร์แม่ข่าย ติดตั้งเครื่องปรับอากาศ 2 ตัว เพื่อสลับการทำงานทุก 6 ชั่วโมง และล็อคห้องคอมพิวเตอร์แม่ข่าย Server เพื่อป้องกันบุคคลภายนอกหรือผู้ไม่เกี่ยวข้องเข้าไปโดยไม่ได้รับอนุญาต

12. กำหนดสิทธิรหัสผู้ใช้ username และ password สำหรับการใช้งาน server และการเข้าถึง database ข้อมูลเวชระเบียนผู้ป่วย

ลงทะเบียนผู้ใช้ใหม่

1. กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้ งานใหม่ตาม "แบบฟอร์มขอใช้บริการอินเตอร์เน็ต hosxp อื่นๆ รพ.วังโป่ง" และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ ให้สิทธิความจำเป็นในการใช้งานเท่านั้น กำหนดตามระดับของผู้ใช้งาน
2. ทบทวนบัญชีผู้ใช้งานและสิทธิของ ผู้ใช้งาน สำหรับเจ้าหน้าที่ของโรงพยาบาลบัวเชดอย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
3. ทบทวนบัญชีผู้ใช้งานและสิทธิของ ผู้ใช้งาน สำหรับหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง

ยกเลิกผู้ใช้

กรณีเจ้าหน้าที่ที่ลาออกโยกย้าย หลังได้รับการแจ้งโยกย้าย / ลาออกจากฝ่ายบริหารงานทั่วไป

1. ยกเลิกสิทธิการเข้าใช้งานออกจากทุกระบบของโรงพยาบาล ได้แก่ HOSxP อินเตอร์เนต
2. ตรวจสอบระบบความถูกต้องของข้อมูลผู้ใช้งานในระบบต่างๆ ทุก 1 สัปดาห์

	ระเบียบปฏิบัติ เรื่อง การใช้งานคอมพิวเตอร์ ระบบเครือข่ายและอินเทอร์เน็ต	หน่วยงาน: เทคโนโลยีสารสนเทศ
	ผู้อนุมัติ  ผู้อำนวยการโรงพยาบาลวังโป่ง	รหัสเอกสาร:WP-CM-03 แก้ไขครั้งที่ 2 วันที่ 4 ม.ค.64

วิธีปฏิบัติ

1. เครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลเป็นสมบัติของทางราชการ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต
2. ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไข ในการรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่โรงพยาบาลกำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของส่วนราชการ มิได้
3. โรงพยาบาลให้รหัสผ่านเครือข่ายสัญญาณไร้สาย(WiFi) และบัญชีผู้ใช้งาน (User/Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้
4. รหัสไวไฟ Wifi Password หรือบัญชีผู้ใช้งาน (User/Account) ที่ทางโรงพยาบาลให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User/ Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
5. ห้ามผู้ใช้งานปฏิบัติการใด ๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของโรงพยาบาล
6. ห้ามผู้ใช้งานทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และ เครือข่ายเช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อ แสวงหากำไร
7. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user/account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ เครือข่ายของหน่วยงานในโรงพยาบาล หรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหาย เสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพที่ไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว โรงพยาบาลไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว
8. โรงพยาบาลจะไม่ควบคุมเนื้อหาของข้อมูล ข่าวสารที่เก็บ และรับส่งผ่านเข้าออกเครื่องคอมพิวเตอร์ เครือข่ายของหน่วยงาน และจะไม่รับประกันในคุณภาพของการเก็บ การรับส่งข้อมูลข่าวสาร และการไม่สามารถใช้งานได้ของระบบบางส่วนหรือทั้งหมด และจะไม่รับผิดชอบในความเสียหายของการใช้งานอันเนื่องมาจากวงจรสื่อสารชำรุด แม่เหล็กชำรุด ความล่าช้า แฟ้มข้อมูลหรือจดหมายส่งไปไม่ถึงปลายทาง หรือส่งผิดสถานที่ และความผิดพลาดในข้อมูลหรือความเสียหายอันเกิดจากการล่วงละเมิดโดยผู้ใช้งาน อื่นๆ
9. ผู้ใช้งานสัญญาว่าจะปฏิบัติตาม เงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่โรงพยาบาล กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสมซึ่งจะมีผลบังคับใช้โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

10. โรงพยาบาลทรงไว้ซึ่งสิทธิ ที่จะปฏิเสธการ เชื่อมต่อ และ/หรือการใช้งานระบบเครือข่าย และทรงไว้ซึ่งสิทธิที่จะยกเลิก หรือระงับการเชื่อมต่อระบบเครือข่าย และ/หรือการใช้งานใดๆ ของผู้ใช้งานที่ล่วงละเมิด หรือพยายามจะล่วงละเมิดกฎระเบียบนี้ของส่วนราชการ
11. ให้ผู้ใช้งาน หรือเจ้าหน้าที่ ซึ่งต้องการนำอุปกรณ์มาเชื่อมต่อ กับระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาล ต้องขออนุญาตศูนย์คอมพิวเตอร์โรงพยาบาล และต้องปฏิบัติตามกฎระเบียบข้อกำหนดโดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่าง ๆ เป็นไปตามมาตรฐานสากล และไม่เกิดผลกระทบกับระบบเครือข่ายคอมพิวเตอร์ส่วนรวมของโรงพยาบาล
12. การขออนุญาตเข้าใช้งานเครือข่ายย่อย หมายเลขไอพี (IP Subnet) และชื่อโดเมน (Domain Name) ของหน่วยงานใดๆหน่วยงานนั้นจะต้องติดต่อขออนุญาตมายังศูนย์คอมพิวเตอร์ เพื่อพิจารณาดำเนินการ
13. โรงพยาบาล ไม่อนุญาตให้บุคคลใดกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่ออุปกรณ์ส่วนกลางโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่อุปกรณ์ส่วนกลางและระบบเครือข่ายของโรงพยาบาลได้
14. บทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามกฎระเบียบดังกล่าว ก่อให้เกิดความเสียหายต่อบุคคลอื่น หรือต่อสมบัติของทางราชการ จะต้องรับโทษตามบทลงโทษต่อไปนี้

- โทษขั้นต้น
- โทษขั้นกลาง
- โทษขั้นสูง
- โทษขั้นร้ายแรงหากการละเมิดฝ่าฝืนก่อให้เกิดความเสียหาย ต่อผู้อื่น หรือต่อทรัพย์สินทั้งของทางราชการอย่างร้ายแรง จะต้องรับโทษตามระเบียบส่วนราชการ หรือรับโทษ ตามกฎหมายโดยลำดับต่อไป

	วิธีปฏิบัติ เรื่อง การใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย Room Server	หน่วยงาน: เทคโนโลยีสารสนเทศ
	ผู้อนุมัติ ผู้อำนวยการโรงพยาบาลวังโป่ง	รหัสเอกสาร:WP-CM-04 แก้ไขครั้งที่ 2 วันที่ 27 ม.ค.64

วิธีปฏิบัติ

1. ห้ามนำบุคคลภายนอกหรือผู้ไม่เกี่ยวข้องเข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย Room Server โดยไม่มีกิจที่จำเป็น
2. ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่องคอมพิวเตอร์แม่ข่าย Room Server
3. ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องคอมพิวเตอร์แม่ข่าย Room Server ให้ปิดล็อกอยู่เสมอ
4. ตรวจสอบสภาพการทำงานของห้องคอมพิวเตอร์แม่ข่าย server อุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ ได้แก่
    - ระบบกระแสไฟฟ้า
    - ระบบการควบคุมความชื้น
    - ระบบการระบายอากาศ
    - ระบบการปรับอุณหภูมิ
    - ระบบกระแสไฟฟ้าสำรอง (เครื่องปั่นไฟ)
    - ระบบเครื่องสำรองไฟ UPS

    ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ อย่างน้อยวันละ 1 ครั้ง ยกเว้นการตรวจสอบระบบกระแสไฟฟ้าสำรองเครื่องปั่นไฟ ให้ตรวจสอบเดือนละ 1 ครั้ง

5. จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่ มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย
6. ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมตามความจำเป็น เช่น ในกรณีที่เป็นมุมอับรวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่องและให้สามารถเก็บภาพได้ในมุมกว้าง และไม่มีสิ่งกีดขวาง โดยบันทึกภาพล่าสุดไว้อย่างน้อย 7 วัน
7. ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยเดือนละ 1 ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่
8. ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อย ของห้องเครื่องคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษหรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่อง
9. ตรวจสอบและจัดเก็บสายไฟฟ้า สายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย
10. จัดทำหรือต่อสัญญา Sofeware หรือการบำรุงรักษาระบบงาน สำคัญไฟร์วอลล์ เราท์เตอร์ อุปกรณ์ UPS สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องเครื่องคอมพิวเตอร์แม่ข่าย ให้ครบถ้วน

11. จัดให้ระบบงานสำคัญ เครื่องคอมพิวเตอร์แม่ข่าย เซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์สำรองไฟ UPS และระบบกระแสไฟฟ้าสำรองเครื่องปั่นไฟ (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน

	วิธีปฏิบัติ เรื่อง การสำรองข้อมูลเวชระเบียนที่จัดเก็บในรูปแบบ Electronic files	หน่วยงาน: เทคโนโลยีสารสนเทศ
	ผู้อนุมัติ ผู้อำนวยการโรงพยาบาลวังโป่ง	รหัสเอกสาร:WP-CM-05 แก้ไขครั้งที่ 2 วันที่ 4 ม.ค.64

วิธีปฏิบัติ

การสำรองข้อมูล Backup ข้อมูลที่จัดเก็บในรูปแบบ Electronic files โรงพยาบาลบัวเชด ให้ปฏิบัติดังนี้

1. จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย Server หลัก จัดทำเป็น RAID-1 โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกันจำนวน 3 ลูก
2. จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย Server รอง ตัวที่ 1 จัดทำเป็น RAIDS-1 โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกันจำนวน 2 ลูก โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักแบบ real time
3. จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย Server รอง ตัวที่ 2 จัดทำเป็น RAIDS-1 โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกันจำนวน 2 ลูก โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักแบบ real time
4. จัดเก็บข้อมูลสำรองเก็บไว้ในเครื่องคอมพิวเตอร์แม่ข่าย Server DHDC ที่เป็นเครื่อง Server DHDC โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักทุกวันศุกร์
5. ทำการ backup ไว้ในเครื่องลูกห้องคอมพิวเตอร์ ทุกวันก่อนเลิกงาน หรือก่อนกลับบ้าน หลัง 16.00 น.เป็นต้นไป
6. ทำ Auto Backup ไว้ในเครื่องห้องลูกข่ายห้องคอมพิวเตอร์ ให้ Backup ทุกวัน เวลา 02.00 น.
7. ทำการ Copy ข้อมูล Back up เก็บไว้ใน Hard disk ของเครื่องลูกข่ายเก็บไว้แยกจุด 2 จุด คือห้องบริหาร และห้องบัตร และใน Hard disk External ของศูนย์คอมพิวเตอร์

ตารางการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย Server

ลำดับ	โปรแกรม ระบบงาน	ข้อมูลที่สำรอง	ความถี่	ผู้รับผิดชอบ	สถานที่เก็บ
1	HOSxP	databases : hos	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal
2	Thai Refer	databases : referdb	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal
3	Paperless	databases : antdb_scan	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal
4	Hosoffice	databases : hosoffice	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal
5	E-claim	databases : ec_claim62	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal
6	ISOnline	databases : isdb	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal
7	Productivity	databases : appdb	ทุกวัน	ปราโมทย์	คอม Backup , hasdisk Extenal

	วิธีปฏิบัติ เรื่อง การปฏิบัติกรณีเกิดอัคคีภัย	หน่วยงาน: เทคโนโลยีสารสนเทศ
	ผู้อนุมัติ ผู้อำนวยการโรงพยาบาลวังโป่ง	รหัสเอกสาร:WP-CM-06 แก้ไขครั้งที่ 3 วันที่ 4 ม.ค.64

เจ้าหน้าที่ไอที

ดำเนินการขนย้ายอุปกรณ์ตามลำดับความสำคัญตามแผนอัคคีภัย ดังนี้

1. ขนย้ายอุปกรณ์ในห้องคอมพิวเตอร์แม่ข่าย Room Server ดังนี้
    - ตู้ Rack Server
2. ขนย้ายอุปกรณ์ในห้องคอมพิวเตอร์ดังนี้
    - Computer PC ที่ติดสติกเกอร์สีแดงหมายเลข 1
    - Switch HUB
    - Computer Notebook
    - เครื่องสำรองไฟฟ้า
    - อุปกรณ์ต่อพ่วงอื่นๆ
3. เมื่อสามารถควบคุมอัคคีภัยได้แล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย ,ระบบไฟฟ้า และติดตั้งอุปกรณ์ให้พร้อมใช้งาน
4. ตรวจสอบความพร้อมใช้ของเครื่องลูกข่าย หากยังไม่พร้อมใช้งานให้ดำเนินการตามระเบียบปฏิบัติ กรณีไฟฟ้าดับ หรือ กรณีเครื่อง Server /Database มีปัญหา

เจ้าหน้าที่อื่นๆ

หากเจ้าหน้าที่ศูนย์คอมพิวเตอร์ไม่อยู่ เจ้าหน้าที่อื่นสามารถดำเนินการได้ดังนี้

- ให้เปิดประตู้ห้องคอมพิวเตอร์แม่ข่าย Room Server หรือพังประตูเพื่อเข้าไปในห้องคอมพิวเตอร์แม่ข่าย Room Server
- ทำการถอด หรือ ตัดสาย LAN โดยใช้คีมตัดสาย LAN ออกให้หมด
- ทำการถอดสายไฟที่อยู่ภายนอกตู้ Server ออกให้หมด
- ทำการเคลื่อนย้ายอุปกรณ์ตามแผนป้องกันอัคคีภัย

<u>ระเบียบวิธีปฏิบัติ เรื่อง ความมั่นคงปลอดภัยของระบบสารสนเทศ</u>

เรื่อง การเข้าถึงระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
๒. เพื่อป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก
๓. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์
๔. เพื่อให้ผู้ปฏิบัติได้รับรู้เข้าใจ และ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วิธีปฏิบัติ

๑. ผู้ดูแลระบบ ได้กำหนดสิทธิเบื้องต้นในการเข้าใช้งานตามมติ บอร์ดพัฒนาระบบสารสนเทศ
๒. เมื่อผู้ใช้งานต้องการเพิ่มสิทธิ์ ให้ติดต่อ ที่ผู้ดูแลระบบ เพื่อทำบันทึกเป็นลายลักษณ์อักษรเพื่อ ขอเพิ่มสิทธิ
๓. ทบทวนเรื่องสิทธิ ปีละ ๑ ครั้ง
๔. ผู้ที่ได้รับสิทธิ์สูงสุด ต้องได้รับความเห็นชอบจากผู้อำนวยการโรงพยาบาล
๕. กรณีผู้ทำงานใหม่ ให้ติดต่อผู้ดูแลระบบเพื่อเข้าใช้งานในระบบต่างๆ
๖. ต้องมีการลงบันทึกการเข้าใช้งาน (login)และต้องมีการพิสูจน์ยืนยันตัวตนด้วยรหัสผ่านก่อนการใช้งาน สำหรับผู้ที่จะเข้าใช้งานต่อไปนี้
   ๖.๑. ระบบ hosxp
   ๖.๒. ระบบ internet
   ๖.๓. ระบบ PAC
   ๖.๔. โปรแกรม RM
   ๖.๕. โปรแกรม SLA
   ๖.๖. ระบบ Smart Queue
๗. ผู้ใช้งานต้องทำการลงบันทึกออกทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
๘. เมื่อผู้ใช้งานระบบอินเตอร์เน็ต ต้องออกจากบราวเซอร์เพื่อป้องกันการใช้โดยบุคคลอื่นด้วยเสมอ
๙. เมื่อมีการตรวจสอบว่า การบันทึกหรือการแก้ไขข้อมูล หรือการเข้าดูข้อมูล นั้นเกิดจาก user,password ใด บุคคลที่มีรายชื่อตามบัญชีรายชื่อผู้นั้น จะเป็นผู้รับผิดชอบ ในการบันทึก แก้ไข เข้าดูข้อมูลในครั้งนั้น
๑๐. จัดระบบสำหรับการเข้าทำงานจากภายนอกโรงพยาบาล ผ่าน VPN

๑๑.การบริหารจัดการรหัสผ่าน

๑๑.๑ กรณีสำหรับระบบ hosxp ที่แรกเริ่มเดิมที เป็นรหัส ๑๒๓๔ ให้ผู้ใช้งานทำคนได้เปลี่ยนรหัส เป็น รหัสอย่างน้อย ๖ ตัว และ ไม่ให้เป็นตัวเลข หรือ ตัวอักษร เรียงกัน หรือ จากคำศัพท์ในพจนานุกรม

๑๑.๒ ผู้ใช้งานควรเปลี่ยนรหัสทุก ๓ เดือน

สำหรับกรณีผู้ใช้งานรายใหม่ ทาง ผู้ดูแลระบบจะได้กำหนดรหัสผ่านที่ไม่ใช่รหัสต้องห้ามไว้

๑๑.๓ ผู้ดูแลระบบทำการยกเลิกการใช้ user password เมื่อผู้ใช้งานได้ลาออก หรือ ย้ายออกจากโรงพยาบาล

๑๑.๔ ผู้ใช้งานต้องไม่ให้ใครล่วงรู้รหัสผ่านของตน

๑๑.๕ ไม่จด หรือ บันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑๑.๖ เมื่อมีความจำเป็นที่จะต้องบอกรหัสให้ผู้อื่น ให้ทำการเปลี่ยนรหัสทันที

๑๒. กำหนดไม่ให้มีการเก็บข้อมูลที่เป็นความลับ รวมทั้งรหัสผ่าน ให้เข้าถึงได้ง่ายทางกายภาพที่โต๊ะทำงานหรือบนหน้าจอ (clear desk, clear screen policy)

๑๓. ผู้ดูแลระบบ ทำการบันทึก การเข้าถึงข้อมูลของ user และ ติดตามเป็นประจำทุกเดือน และ รายงานประธานบอร์ดสารสนเทศทราบทุกเดือน

๑๔. กรณีส่งเครื่องคอมพิวเตอร์ซ่อมภายนอกโรงพยาบาล ให้ดำเนินการสำรองข้อมูลและลบข้อมูลที่เก็บไว้ออกก่อน

๑๕. ความผิดพลาดและปัญหาที่อาจจะเกิดขึ้นจากการไม่ปฏิบัติตามประกาศนี้ หรือจากการนำรหัสผู้ใช้งานและรหัสผ่านไปให้บุคคลอื่นใช้งาน ผู้ที่มีชื่อเป็นเจ้าของรหัสผู้ใช้งานและรหัสผ่านนั้นๆจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๑๖. **สำหรับกรณีบุคคลภายนอก**

๑๖.๑ ให้ติดต่อผู้ดูแลระบบ เพื่อทำบันทึก เพื่อขออนุญาต พร้อมเหตุผล ก่อนเข้าใช้ระบบ โดยระบุความเสี่ยงที่อาจจะเกิดขึ้นพร้อมกำหนดแนวทางป้องกันและแก้ไขความเสี่ยงนั้นก่อนเสนอให้รับการอนุญาตโดยประธานบอร์ดพัฒนาระบบสารสนเทศ นำเสนอผู้อำนวยการโรงพยาบาลวังโป่งเพื่อทำการอนุมัติอีกครั้ง

๑๖.๑.๑กรณีบำรุงรักษาระบบ ต้องมีหนังสือจากองค์กร มาที่ผู้อำนวยการ และ admin จะเป็นผู้กรอกรหัสผ่านให้โดยไม่บอก กับบุคคลภายนอก และ อยู่ดูแล ควบคุม กำกับ กับบุคคลภายนอกตลอดเวลา

๑๖.๑.๒ กรณีขอเข้าดูประวัติผู้ป่วยผ่านระบบ ให้ทำเหมือนขอดูประวัติผู้ป่วยผ่านระบบเวชระเบียน

๑๖.๒ ควบคุม network port number อย่างรัดกุม

๑๖.๓ ผ่านระบบการพิสูจน์ตัวตนด้วยเช่นกัน

๑๗. กรณีผู้ใช้งาน ได้ลาออก หรือ เปลี่ยนตำแหน่ง หน้าที่ความรับผิดชอบ ให้งานบริหารฝ่ายบุคลากร ทำการแจ้งผู้ดูแลระบบ เพื่อทำการปรับปรุงสิทธิการเข้าใช้ หรือ ยกเลิกการใช้งาน

๑๘. จัดทำ log เก็บการใช้งานอินเตอร์เน็ท และ มีระบบพิสูจน์ตัวตนในการเข้าถึงระบบ log