



โรงพยาบาลบางแก้ว ระเบียบวิธีปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

ระเบียบปฏิบัติ

ระเบียบปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ และเครือข่าย และระเบียบการเชื่อมต่อคอมพิวเตอร์และเครือข่ายเอกสารฉบับนี้ มีจุดประสงค์เพื่อสร้างความเข้าใจเกี่ยวกับระเบียบการใช้ระบบคอมพิวเตอร์และเครือข่าย ของโรงพยาบาลบางแก้ว ภายใต้การดูแลของศูนย์คอมพิวเตอร์ ซึ่งกล่าวถึงสิทธิหน้าที่ ข้อปฏิบัติของผู้ใช้

ระบบ

๑. คำจำกัดความในระเบียบนี้

"โรงพยาบาล" หมายถึง โรงพยาบาลบางแก้ว

"ศูนย์คอมพิวเตอร์" หมายถึง ศูนย์คอมพิวเตอร์ โรงพยาบาลบางแก้ว

"เครื่องคอมพิวเตอร์และเครือข่าย" หมายถึง เครื่องคอมพิวเตอร์ที่เป็นสมบัติของโรงพยาบาล ทั้งที่อยู่ภายใน และภายนอกส่วนกลาง รวมทั้งอุปกรณ์ต่อพ่วงต่าง ๆ อุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในโรงพยาบาล ตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ ที่มีได้จัดให้เป็นสื่อสาธารณะ

"หน่วยงาน" หมายถึง หน่วยงานต่างๆ ของโรงพยาบาลบางแก้ว

"ผู้ใช้งาน" หมายถึง ข้าราชการ ลูกจ้าง ผู้ที่โรงพยาบาลอนุญาตให้ใช้เครื่องคอมพิวเตอร์และเครือข่ายได้

๒. มาตรการควบคุมการเข้า-ออกห้องควบคุมห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายและเครือข่าย

๑. ผู้ติดต่อจากโรงพยาบาลภายนอกทุกคน ต้องทำการขออนุญาตผ่านหน่วยงานผู้รับผิดชอบตามแบบฟอร์มการขออนุญาต และได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการ หรือผู้ดูแลระบบที่ได้รับมอบหมาย
๒. ผู้ติดต่อจากโรงพยาบาลภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องทำการขออนุญาตผ่านหน่วยงานผู้รับผิดชอบและได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓. กฎระเบียบการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไขในการรับทราบกฎระเบียบหรือ นโยบายต่างๆ ที่โรงพยาบาลกำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของส่วนราชการ ไม่ได้
๒. โรงพยาบาลให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนจำหน่าย หรือแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๓. บัญชีผู้ใช้งาน (User Account) ที่โรงพยาบาลให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้นรวมถึงผลเสียหายต่าง ๆ ที่เกิดจาก บัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะ พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
๔. ห้ามผู้ใช้งานปฏิบัติการใดๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการค้าต่อกฎหมาย หรือศีลธรรมอันดีแห่ง สาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความ รับผิดชอบของโรงพยาบาล
๕. ห้ามผู้ใช้งานทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหากำไรผ่านเครื่องคอมพิวเตอร์และ เครือข่ายเช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการ ค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อ แสวงหากำไร
๖. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่นกล่าว คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ใน ส่วนที่มีใช้ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของผู้อื่น หรือ เข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงานในโรงพยาบาล หรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่นการใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ ผู้อื่น เสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว โรงพยาบาลไม่มี ส่วนร่วมรับผิดชอบต่อความเสียหายดังกล่าว
๗. โรงพยาบาลจะไม่ควบคุมเนื้อหาของข้อมูล ข่าวสารที่เก็บ และรับส่งผ่านเข้าออกเครื่องคอมพิวเตอร์ของ หน่วยงาน และจะไม่รับประกันในคุณภาพของการเก็บการรับส่งข้อมูลข่าวสาร และการไม่สามารถใช้งานได้ ของระบบบางส่วนหรือทั้งหมดและจะไม่รับผิดชอบในความเสียหายของการใช้งานอันเนื่องมาจากวงจรสื่อ สาร ขำรุด จานแม่เหล็กขำรุด ความล่าช้า แฟ้มข้อมูลหรือจดหมายลงไปไม่ถึงปลายทาง หรือส่งผิดสถานที่ และ ความผิดพลาดในข้อมูลหรือความเสียหายอันเกิดจากการลวงละเมิดโดยผู้ใช้งาน อื่นๆ
๘. ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่โรงพยาบาลกำหนดไว้และที่จะกำหนด ขึ้น ในอนาคตตามความเหมาะสมซึ่งจะมีผลบังคับใช้โดยไม่ จำเป็นต้องแจ้งให้ทราบล่วงหน้า
๙. โรงพยาบาลทรงไว้ซึ่งสิทธิที่จะปฏิเสธการเชื่อมต่อและ/หรือการใช้งานและทรงไว้ซึ่งสิทธิที่จะยกเลิก หรือ ระงับการเชื่อมต่อ และหรือการใช้งานใดๆ ของผู้ใช้งานที่ลวงละเมิดหรือพยายามจะลวงละเมิด กฎระเบียบนี้ของส่วนราชการ

๔. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑. เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในการงาน ราชการ
๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรม ที่ หน่วยงานได้ซื้อ ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไป ติดตั้งบนเครื่อง คอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
๓. ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วน บุคคลของ หน่วยงาน
๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดย เจ้าหน้าที่ของ โรงพยาบาลเท่านั้น
๕. ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกัน ไวรัส
๖. ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

- ๓/. ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง
๔. ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการ ล็อก หน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาทีเพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์
๕. ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของ หน่วยงาน ยกเว้น จะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน
๑๐. ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ
๑๑. ไม่จดหรือบันทึกที่รหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์
๑๒. ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน

๕. การการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑. เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อ ใช้ในงานราชการ
๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรม ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และ นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
๓. ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัย และมีประสิทธิภาพ
๔. ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มี สภาพเดิม
๕. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่อง คอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
๖. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีด ข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
๗. ไม่วางของทับบนหน้าจอและแป้นพิมพ์
๘. การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทาง เดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
๙. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
๑๐. การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
๑๑. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
๑๒. ผู้ใช้ต้องจัดเก็บรหัสผ่านเป็นความลับ
๑๓. ไม่จดหรือบันทึกที่รหัสผ่านแล้วติดไว้หน้าเครื่องคอมพิวเตอร์
๑๔. ควรเปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน
๑๕. ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาทีให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

๖. การการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความ จำเป็นและต้องท การขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร
๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อ อินเทอร์เน็ต ผ่านเว็บเบราว์เซอร์(Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอัปเดตช่องโหว่ ของระบบปฏิบัติการ
๓. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
๔. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็น การ ส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อ สังคม หรือ ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน
๕. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)
๖. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่างๆต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์
๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน
๘. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่ จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงาน อื่นๆ
๙. ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความ มั่นคงแห่ง ราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการ เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
๑๐. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้า ใช้งาน โดยบุคคลอื่น ๆ
๑๑. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดย บุคคลอื่น ๆ
๑๒. ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่าง เคร่งครัด

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้ รั่วไหล ออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด
๒. ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า โดย ปรียาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และ กำหนดให้ชื่อ SSID (Service Set Identifier)

๓. ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย
๔. ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และ ชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการใช้งานระบบเครือข่ายไร้สาย โดย จะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง
๕. ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบ เครือข่ายภายในหน่วยงาน
๖. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย
๗. ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย
๘. ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่าย ไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการ ตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที
๙. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน
๑๐. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ประกาศ ณ วันที่ ๕ มกราคม พ.ศ.๒๕๖๕

(นายทรงเกียรติ พลเพชร)

นายแพทย์ชำนาญการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลบางแก้ว