

มาตรฐานด้านเทคโนโลยีสารสนเทศโรงพยาบาลเชียงใหม่กลาง

QM ๒.๒.๑๕.นโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเชียงใหม่กลาง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาล ที่มนาระบบสารสนเทศ จึงได้กำหนดแนวทางในการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยอ้างอิงจากแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย ๘ หมวด ได้แก่

หมวด ๑ ว่าด้วยเรื่องการพิสูจน์ตัวตน(Accountability , Identification and Authentication)

๑. ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username)ของตนเองห้ามใช้ร่วมกับผู้อื่นรวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) ของตนเอง

๒. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

๓. ผู้ใช้งานต้องตั้งรหัสของตนเป็นข้อมูลเฉพาะเพื่อให้เกิดความปลอดภัย

๔. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๕. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้งานระบบสารสนเทศของโรงพยาบาลเชียงใหม่กลาง และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนลือคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

๕.๑. การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๕.๒. คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๕.๓. การใช้งานระบบคอมพิวเตอร์โดยอุปกรณ์อื่น ๆ ในเครือข่าย ได้แก่ แท็บเล็ต ไอแพด และโทรศัพท์มือถือ เป็นต้น จะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๕.๔. เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานในภายหลังทุกครั้ง

๕.๕. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

หมวด ๒ ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

๑. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลเชียงใหม่กลาง ถือเป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๒. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๓. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

๔. ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

๕. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์เกี่ยวกับการใช้งาน ก่อนได้รับอนุญาต

๖. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลเชียงใหม่ ออไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

๗. กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบต่อทรัพย์สินของโรงพยาบาลเชียงใหม่ ตามที่ได้รับมอบหมาย

๘. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๙. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์หรือเน็ตบุ๊กไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

๑๐. ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่โรงพยาบาลเชียงใหม่ จัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของโรงพยาบาลเชียงใหม่ เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่โรงพยาบาลไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อโรงพยาบาล

๑๑. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๑๐ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งาน ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลขององค์กร (Corporate Management)

๑. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลเชียงใหม่ หรือเป็นข้อมูลของบุคลากรภายนอก

๒. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลเชียงใหม่ ถือเป็นทรัพย์สินของโรงพยาบาลเชียงใหม่ ห้ามมิให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำหรือ ทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลเชียงใหม่ หรือข้อมูลของผู้รับบริการหากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๔. ผู้ใช้งานต้องป้องกัน ดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

๕. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลเชียงใหม่ จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลเชียงใหม่ อาจแต่งตั้งให้มีผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

๑. ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ แต่ต้องไม่ดำเนินการดังนี้

๑.๑. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกการรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกระหัสผ่านของบุคคลอื่น

๑.๒. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้อื่น

๑.๓. พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๑.๔. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้งาน (License) ซอฟต์แวร์

๑.๕. นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๒. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent) , อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง และเล่นเกมส์ เป็นต้น ระหว่างปฏิบัติงาน

๔. ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใด ของโรงพยาบาลเชียงใหม่กลาง ที่จัดเตรียมไว้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการกิจของโรงพยาบาลเชียงใหม่กลาง

๕. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเชียงใหม่กลาง เพื่อประโยชน์ทางการค้า

๖. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลเชียงใหม่กลาง โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๗. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลเชียงใหม่กลาง ต้องหยุดชะงัก

๘. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเชียงใหม่กลาง เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๙. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๑๐. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อให้สามารถเข้าถึงระบบสารสนเทศของโรงพยาบาลเชียงใหม่กลาง โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

๑. บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของโรงพยาบาลเชียงใหม่ ถือว่าเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำความผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบ ต่อความผิดที่เกิดขึ้นเอง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

๑. โรงพยาบาลเชียงใหม่ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่โรงพยาบาลอนุญาตให้ใช้งานหรือที่โรงพยาบาลมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ ความจำเป็นและ โรงพยาบาลเชียงใหม่ ห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ โรงพยาบาลเชียงใหม่ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๒. ซอฟต์แวร์ (Software) ที่โรงพยาบาลเชียงใหม่ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

๑. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่โรงพยาบาลเชียงใหม่ได้ประกาศให้ใช้ หมั่นตรวจสอบและอัปเดตระบบปฏิบัติการ (Operating System) เช่น Windows หรือซอฟต์แวร์ที่ใช้ให้เป็นเวอร์ชันปัจจุบัน เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

๒. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๓. ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๔. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา เมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทราบ

๕. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทราบ

๖. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของโรงพยาบาลเชียงใหม่ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๗. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของโรงพยาบาลเชียงใหม่

หมวด ๘ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

๑. ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy) ดังนี้

๑.๑. ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๑.๒. ควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

๑.๓. ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) ของผู้อื่นเพื่ออ่านหรือรับ ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (Email)

เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (Email) ของตน

๑.๔. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Email) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ทั้งนี้ ให้ถือปฏิบัติตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑ กรกฎาคม ๒๕๖๗

(นายอภิชาติ สถาวรวิวัฒน์)

นายแพทย์ชำนาญการพิเศษ ปฏิบัติหน้าที่

ผู้อำนวยการโรงพยาบาลเชียงใหม่