ประกาศโรงพยาบาลเชียงยืน
เรื่องนโยบาย ความมั่นคง ปลอดภัยระบบสารสนเทศ

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โรงพยาบาลเชียงยืน เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลเชียงยืน ให้อยู่ระดับและการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็ว หลังจากระบบล่ม และระบบถูกโจมตีสิ้นสุดลงแล้ว และเป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของโรงพยาบาลเชียงยืน นโยบายความมั่นคง ปลอดภัยระบบสารสนเทศ โรงพยาบาลเชียงยืน ประกอบด้วย ๘ หมวด โดยมีรายละเอียดดังต่อไปนี้

หมวด ๑ ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ ๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๔ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet)และตัวอักษรพิเศษ(Special character)

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว

ข้อ ๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของโรงพยาบาลเชียงยืน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(๑) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูล ซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๓) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๔) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

หมวด ๒ ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๗ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) โรงพยาบาลเชียงยืน ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๘ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๙ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๑๐ ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใดๆ

ข้อ ๑๑ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลทีมี ลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ ๑๒ ผู้ใช้งานมีหน้าทีต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลเชียงยืน ที่มอบไว้ให้ใช้งาน โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่ แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ที่ โรงพยาบาลเชียงยืน มอบหมาย

ข้อ ๑๓ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของโรงพยาบาลเชียงยืน ที่ได้รับมอบหมาย

ข้อ ๑๔ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๑๕ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๑๖ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่โรงพยาบาลเชียงยืน จัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของโรงพยาบาลเชียงยืน เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมทีโรงพยาบาลเชียงยืน ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงพยาบาลเชียงยืน

ข้อ ๑๗ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๖ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายทีเกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑๘ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลเชียงยืน หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลเชียงยืน ถือเป็นทรัพย์สินของโรงพยาบาลเชียงยืน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๒๐ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลเชียงยืน หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๒๒ ผู้ใช้งานมีสิทธิ โดยชอบธรรมทีจะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลเชียงยืน จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น

ยกเว้นในกรณีที่โรงพยาบาลเชียงยืน ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลเชียงยืน ซึ่งโรงพยาบาลเชียงยืน อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๒๓ ผู้ใช้งานมีสิทธิ ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ทีจะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึงทำให้ผู้ใช้มีสิทธิ และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นใน ลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ทีจะทำลายระบบจำกัดสิทธิiการใช้ (License)ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีทีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๒๔ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมทีมีความเสียงในระดับเดียวกัน เช่น บิทเทอร์เรนท์(Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๒๕ ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๖ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของโรงพยาบาลเชียงยืน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ทีมีลักษณะขัดต่อศีลธรรม ความมั่น คงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลเชียงยืน

ข้อ ๒๗ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของโรงพยาบาลเชียงยืน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาลเชียงยืน

ข้อ ๒๘ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเชียงยืนเพื่อประโยชน์ทางการค้า

ข้อ ๒๙ ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลเชียงยืน โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๓๐ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลเชียงยืน ต้องหยุดชะงัก

ข้อ ๓๑ ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเชียงยืน เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๓๒ ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๓ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของโรงพยาบาลเชียงยืน โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๓๔ บรรดากฎหมายใดๆ ทีได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของโรงพยาบาล

เชียงยืน ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ (Software Licensing and intellectual property)

ข้อ ๓๕ โรงพยาบาลเชียงยืน ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่โรงพยาบาลเชียงยืน อนุญาตให้ใช้งานหรือที่โรงพยาบาลเชียงยืน มีลิขสิทธิ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และโรงพยาบาลเชียงยืน ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ โรงพยาบาลเชียงยืน ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๓๖ ซอฟต์แวร์ (Software) ที่โรงพยาบาลเชียงยืนได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไป ใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

ข้อ ๓๗ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่โรงพยาบาลเชียงยืน ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกันโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓๘ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ทีได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓๙ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายทีอาจเกิดขึ้น

ข้อ ๔๐ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิงผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๔๑ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๔๒ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นทรัพย์สินของโรงพยาบาลเชียงยืน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๔๓ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของโรงพยาบาลเชียงยืน

หมวด ๘ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

ข้อ ๔๔ ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมัน คงปลอดภัยระบบสารสนเทศ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีทีนำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media

Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ ในการเข้า ใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่าย ไร้สายได้อย่างถูกต้อง

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บัญชาการโรงพยาบาลเชียงยืนทราบทันที

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ข้อ ๑ โรงพยาบาลเชียงยืน มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ ๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการ เท่านั้น

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลเชียงยืน อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจากโรงพยาบาลเชียงยืน ก่อน

ข้อ ๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปเดือน

หรือทุกครั้งทีมีการเปลี่ยนแปลงค่า

ข้อ ๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๒ โรงพยาบาลเชียงยืน มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานทีผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมทีมี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก โรงพยาบาลเชียงยืนก่อน

ข้อ ๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

ข้อ ๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

ข้อ ๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ ๓ จัดเก็บข้อมูลทีสำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาทีสำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลทีสำรองควรจัดเก็บไว้ในสถานทีเก็บข้อมูลสำรองซึงติดตั้งอยู่ทีสถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ ๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ประกาศ ณ วันที่ ๘ มกราคม ๒๕๖๘

(นายภาคภูมิ อินทร์ม่วง)
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)
รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลเชียงยืน