

ประกาศ โรงพยาบาลร็องกวาง

เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศโรงพยาบาลร็องกวาง เป็นการจัดทำขึ้นเพื่อกำหนด แนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลร็องกวาง ให้อยู่ระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็ว หลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของโรงพยาบาลร็องกวาง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ โรงพยาบาลร็องกวาง ประกอบด้วย ๘ หมวด โดยมีรายละเอียดดังต่อไปนี้

หมวด ๑ ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

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

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน (Username) ไม่ว่าจะ การกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อย กว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่าน

ข้อ ๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพยากรหรือระบบสารสนเทศของโรงพยาบาลร็องกวาง และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล๊อคก็ดี หรือเกิด จากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(๑) คอมพิวเตอร์โน้ตบุ๊ก (Notebook) ต้องทำการพิสูจน์ตัวตนในระดับไบออส(BIOS) ก่อนการใช้งาน

(๒) คอมพิวเตอร์ทุกประเภท ล່อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๔) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึก ข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๕) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล๊อค หน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๖) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

หมวด ๒ ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ ๗ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) โรงพยาบาลร็องกวางที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๘ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๙ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจ ส่วนบุคคล

ข้อ ๑๐ ผู้ใช้งานต้องไม่ใช้ หรือลบแท้มข้อมูลของผู้อื่น ไม่ว่าจะกรณีใดๆ

ข้อ ๑๑ ผู้ใช้งานต้องไม่ตัดลอกหรือทำสำเนาแท้มข้อมูลที่มีลิขสิทธิ์กับการใช้งาน ก่อนได้รับอนุญาต

ข้อ ๑๒ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลร็องกวางมอบไว้ให้ใช้งานเสมือน หนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่ แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ที่ โรงพยาบาลร็องกวางมอบหมาย

ข้อ ๑๓ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลรับผิดชอบทรัพย์สินของโรงพยาบาลร็องกวางที่ได้รับมอบหมาย

ข้อ ๑๔ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่า ทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๑๕ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ก ไม่ว่าจะในกรณีใดๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๑๖ ทรัพย์สินและระบบสารสนเทศต่างๆ ที่โรงพยาบาลร็องกวาง จัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของโรงพยาบาลร็องกวางเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบ สารสนเทศต่างๆ ไปใช้ในกิจกรรมที่โรงพยาบาลร็องกวางไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อ โรงพยาบาลร็องกวาง

ข้อ ๑๗ ความเสียหายใดๆ ที่เกิดจากการละเมิดตาม

ข้อ ๑๘ ให้ถือเป็นความผิดส่วนบุคคลโดย ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑๘ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของ โรงพยาบาลร็องกวาง หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลร็องกวาง ถือเป็นทรัพย์สินของ โรงพยาบาลร็องกวาง ห้ามมิให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำหรือทำลาย โดยไม่ได้รับอนุญาตจาก ผู้บังคับบัญชา

ข้อ ๒๐ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลร็องกวาง หรือ ข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งาน ต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๒๒ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตาม เห็นสมควร โรงพยาบาลรื่องกวาง จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคล หนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลรื่องกวาง ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับข้อบังคับโรงพยาบาลรื่องกวาง ซึ่งโรงพยาบาลรื่องกวางอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๒๓ ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการ ดังนี้

- (๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมถึงการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูล บุคคลอื่นหรือ แะรหัสผ่านของบุคคลอื่น
- (๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้อื่น
- (๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรม อื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์
- (๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์
- (๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือ ขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๒๔ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง ในระดับเดียวกัน เช่น บิททอร์เรนท์(Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจาก ผู้บังคับบัญชา

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

ข้อ ๒๖ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของโรงพยาบาลรื่องกวางที่ จัดเตรียมไว้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคง ของประเทศ กฎหมาย หรือ กระทบต่อภารกิจของโรงพยาบาลรื่องกวาง

ข้อ ๒๗ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของโรงพยาบาลรื่องกวาง เพื่อ การรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมาย และศีลธรรม หรือ กระทบต่อภารกิจของโรงพยาบาลรื่องกวาง

ข้อ ๒๘ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลรื่องวางเพื่อประโยชน์ทางการค้า ข้อ ๒๙ ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรืออื่นใดใน เครือข่ายระบบสารสนเทศของโรงพยาบาลรื่องวาง โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ ๓๐ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลรื่องวาง ต้อง หยุดชะงัก

ข้อ ๓๑ ห้ามใช้ระบบสารสนเทศของโรงพยาบาลรื่องวาง เพื่อการควบคุมคอมพิวเตอร์หรือระบบ สารสนเทศ ภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๓๒ ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้อิสส่วนตัวบุคคลของผู้อื่น ไม่ว่าจะป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๓ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของ โรงพยาบาลรื่องวาง โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๓๔ บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมถึงกฎระเบียบ ของโรงพยาบาลรื่องวาง ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งาน จะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

ข้อ ๓๕ โรงพยาบาลรื่องวาง ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่ โรงพยาบาลรื่องวาง อนุญาตให้ใช้งานหรือที่โรงพยาบาลรื่องวาง มีลิขสิทธิ์ ผู้ใช้งานสามารถใช้งานได้ตาม หน้าที่ความจำเป็น และ โรงพยาบาลรื่องวางห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มี ลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ โรงพยาบาลรื่องวางถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๓๖ ซอฟต์แวร์ (Software) ที่โรงพยาบาลรื่องวางได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อ การทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไป ใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

ข้อ ๓๗ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ โรงพยาบาลรื่องวาง ได้ประกาศให้ใช้วันแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓๘ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการ ตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓๙ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔๐ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมถึงเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๔๑ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๔๒ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบตั้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดที่เป็น ทรัพย์สินของโรงพยาบาลรื่องกวาง หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๔๓ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิด ความเสียหาย มาสู่ทรัพย์สินของโรงพยาบาลรื่องกวาง

หมวด ๘ ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

ข้อ ๔๔ ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบ สารสนเทศ 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) ที่ ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้า ใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่าย ไร้สายได้อย่างถูกต้อง

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบ เครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

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

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบ เครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งาน ระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บัญชาการโรงพยาบาลรื่องกวาง ทราบทันที

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอก ที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูล ภายในต่างๆ ของหน่วยงาน

นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ข้อ ๑ โรงพยาบาลรื่องขวาง มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ ทั้งหมด

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 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิด พอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลรื่องขวาง อนุญาตให้ใช้งาน ซึ่งหากมีความ จำเป็นที่ใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากโรงพยาบาลรื่องขวาง ก่อน

ข้อ ๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้อง ลูกข่ายให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง

ข้อ ๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มี การเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๒ โรงพยาบาลรื่องขวาง มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มี พฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรือ อุปกรณ์เครือข่าย ภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่องคอมพิวเตอร์แม่ข่ายและ อุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจาก โรงพยาบาลรื่องขวางก่อน

ข้อ ๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

นโยบายความมั่นคงปลอดภัยของอีเมล(E-mail Policy)

ข้อ ๑ ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่ โรงพยาบาลรื่องขวาง

ข้อ ๒ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๓ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ข้อ ๔ ควรเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือน

ข้อ ๕ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

ข้อ ๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๗ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย อิเล็กทรอนิกส์

นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ต(Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการ ส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่น่าก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่าง เป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับ ของหน่วยงาน

ข้อ ๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของ หน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการ ใช้งานโดยบุคคลอื่นๆ

นโยบายความมั่นคงปลอดภัยของโปรแกรมการเข้าถึงระบบ (Access control Policy)

หมวด ๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ โรงพยาบาลรื่องกวาง กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงาน เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบ สารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการสำนักงานโรงพยาบาลรื่องกวาง

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้ เหมาะสมกับการใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงาน ก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้ งานระบบ สารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไข เปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ทั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและ ไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวด ๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลรื่อง กวาง ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตาม ความจำเป็นรวมทั้งขั้นตอน ปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยน ตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบ เครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงาน ในหน้าที่และต้องได้รับความเห็นชอบจาก ผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน ของบุคลากร ดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบ ลาออก หรือพ้น จากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควร หลีกเลี่ยงการ ใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบ คอมพิวเตอร์ในรูปแบบที่ ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้น จะต้องได้รับความ เห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึง ได้ถึงระดับใดได้บ้าง และต้อง กำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้น ความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่าน ระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- (๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่าน ระบบงาน
- (๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการ ตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
- (๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว (๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น
- (๕) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับ ความสำคัญของข้อมูล
- (๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่อง คอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูล ที่เก็บอยู่ในสื่อบันทึกก่อน

นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

(Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

ข้อ ๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความ ปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาล แพร่ ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับ บทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลรื่องวางและเครือข่าย ข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง 'ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการ ตรวจสอบจากระบบ IDS/IPS

ข้อ ๔ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และ เปิดให้บริการ

ข้อ ๕ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการ ตรวจสอบ

ข้อ ๖ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

ข้อ ๗ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณ ข้อมูลเข้าใช้งาน เครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๘ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของ ระบบสารสนเทศ ตามปกติ

ข้อ ๙ เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๑๐ พหุติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การ โจมตีระบบ พหุติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ตั้งที่ประสบความสำเร็จและไม่ประสบ ความสำเร็จ จะต้องมีการรายงานให้ ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๑๑ พหุติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการ รายงานให้ ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

ข้อ ๑๒ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน ข้อ ๑๓ มีรูปแบบการ ตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของ เหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ร้ายที่ตรวจพบ ป้องกัน เหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๑๓ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และ ดำเนินการตามแผน

ข้อ ๑๔ โรงพยาบาลรื่องกาง มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มี พหุติกรรมเสี่ยงต่อ การบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๑๕ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลรื่องกาง การ พยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพหุติกรรมเสี่ยงต่อการทำงานของระบบ สารสนเทศ จะถูกระงับการใช้ เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาล รื่องกาง จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

ข้อ ๑ โรงพยาบาลรื่องกาง กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย(Server)

ข้อ ๒ ผู้ให้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และ ระบบเครือข่ายของ หน่วยงาน ต้องได้รับอนุญาตจากผู้บัญชาการโรงพยาบาลรื่องกาง และต้องปฏิบัติตาม นโยบายนี้โดยเคร่งครัด

ข้อ ๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงาน รับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บัญชาการโรงพยาบาลรื่องกาง และจะต้องไม่ติดตั้ง โปรแกรมใดๆ ที่ส่งผล กระทบต่อการกระทำของระบบและผู้ให้บริการอื่นๆ

ข้อ ๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเต้น ทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย หลัก โดยไม่ได้รับอนุญาตจาก ผู้ดูแลระบบ (System Administrator)

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหาร จัดการระบบ เครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะ ระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องมีวิธีการจำกัดเส้นทางในการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน (๓) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไป ยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมถึงต้องมีความสามารถในการตรวจจับ โปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ หน่วยงานในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้อง มีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ของผู้ใช้บริการ

(๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็น ปัจจุบันอยู่เสมอ

(๙) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจาก ผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๗ โรงพยาบาลรöntgen กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

(๑) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษา ความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้อง กำหนดขึ้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

(๒) ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึก การพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการ ใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๓) ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึง บันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๘ โรงพยาบาลร็องกวาง กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่อง คอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

- (๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและ เครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจาก ผู้บัญชาการโรงพยาบาลร็องกวาง
- (๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
- (๓) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจากผู้ บัญชาการโรงพยาบาลร็องกวาง
- (๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความ จำเป็นในการ ดำเนินงานกับหน่วยงานอย่างเพียงพอ
- (๕) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

ข้อ ๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรอง ข้อมูลระบบ สารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

ข้อ ๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบ ซอฟต์แวร์ และข้อมูล ในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ ๓ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบ ซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่าง ชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ใน สถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการ ทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ ๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ ภายใน ระยะเวลาที่เหมาะสม



(นายรุ่งกิจ ปินใจ)
นายแพทย์ชำนาญการ
รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาล