โรงพยาบาลสมเด็จ
SOMDET HOSPITAL

นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศโรงพยาบาลสมเด็จ

งานเทคโนโลยีสารสนเทศ

โรงพยาบาลสมเด็จ พ.ศ. ๒๕๖๗

คำนำ

โรงพยาบาลสมเด็จได้กำหนดนโยบายให้มีการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร เป็นเครื่องมือในการพัฒนาองค์กรให้มีความสามารถในการดำเนินการตามวัตถุประสงค์เพื่อพัฒนาถ่ายทอดองค์ความรู้และเทคโนโลยีในการให้บริการ ที่มีคุณภาพมาตรฐาน มีความมั่นคงปลอดภัยทางระบบสารสนเทศ กลุ่มงานยุทธศาสตร์และสารสนเทศ จึงได้ กำหนดให้มีการจัดทำนโยบายและแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จเพื่อให้ระบบสารสนเทศเป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจจะก่อให้เกิดความเสียหายกับข้อมูล ทรัพย์สินและชื่อเสียงของโรงพยาบาลสมเด็จ

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของโรงพยาบาลสมเด็จ

ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการให้บริการและบำรุงรักษาระบบสารสนเทศภายในโรงพยาบาลสมเด็จ ดังนั้นเพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย ศูนย์เทคโนโลยีสารสนเทศจึงได้จัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศเพื่อกำหนดแนวทางและเป็นแผนที่นำทางในการบริหารจัดการระบบสารสนเทศภายในโรงพยาบาล เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จ ให้อยู่ระดับที่ทันสมัยและได้มาตรฐานอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC๒๗๐๐๑ อีกทั้งต้องการลดผลกระทบจากความเสียหายที่อาจเกิดขึ้นหากมีการโจมตีระบบสารสนเทศของโรงพยาบาลตลอดจนแนวทางปฏิบัติในการกู้คืนระบบอย่างรวดเร็ว

คำนิยาม

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความ ถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (reliability)

หมวดที่ ๑
นโยบายว่าด้วยการพิสูจน์ตัวตนและสิทธิ์ในการเข้าถึงและการใช้งาน
(Authentication , Authorization and Accountability)

ข้อ ๑ ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัส ผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๒ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๓ ผู้ใช้งานควรตั้งรหัสผ่านให้เกิดความปลอดภัยโดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น "abcdef" " aaaaaa" "๑๒๓๔๕๖" "๑๒๓๔๕๖" หรือเป็นรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด

ข้อ ๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน หรือมีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

ข้อ ๕ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของโรงพยาบาลและหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านโดนล็อคหรือเกิดจากความผิดพลาดใดๆก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบของงานเทคโนโลยีสารสนเทศโรงพยาบาลทราบทันที โดย

(๕.๑) คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการควรต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๕.๒) การใช้งานระบบเครือข่ายอินเตอร์เน็ต จะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๕.๓) การใช้งานระบบเครือข่ายอินเตอร์เน็ต ต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๕.๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ทุกเครื่องต้องทำการ logout โปรแกรมทุกครั้งและต้องทำการพิสูจน์ ตัวตนก่อนการใช้งานทุกครั้ง

(๕.๕) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๕.๖) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ(Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ครอบครองอยู่

(๕.๗) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

หมวดที่ ๒
นโยบายว่าด้วยการบริหารจัดการทรัพย์สิน
(Assets Management)

ข้อ ๑ ผู้ใช้งาน ต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ศูนย์เทคโนโลยีสารสนเทศ ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๒ ผู้ใช้งานต้องไม่นำอุปกรณ์ หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๔ ผู้ใช้งานต้องไม่คัดลอก หรือทำสำเนาแฟ้มข้อมูล ที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาตและผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใดๆ

ข้อ ๕ ผู้ใช้งานมีหน้าที่ ต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาล มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเองโดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบจะอยู่แนบท้ายเอกสารข้อบังคับนี้การรับหรือคืนทรัพย์สินจะถูกบันทึกและตรวจสอบทุกครั้ง

ข้อ ๖ กรณีมีการนำครุภัณฑ์ไปใช้ภายนอก ศูนย์เทคโนโลยีสารสนเทศผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของ โรงพยาบาลที่ได้รับมอบหมาย

ข้อ ๗ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สินหาก ความเสียหาย นั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๘ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมคอมพิวเตอร์หรือโน๊ตบุ๊คไม่ว่าในกรณีใดๆเว้นแต่การยืมนั้นได้รับการอนุมัติเป็น ลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๙ ทรัพย์สินและระบบสารสนเทศต่างๆที่โรงพยาบาลสมเด็จจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้ งานของโรงพยาบาลสมเด็จเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆไปใช้ในกิจกรรมที่ โรงพยาบาลสมเด็จไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อโรงพยาบาลสมเด็จ

ข้อ ๑๐ ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยระบุผู้รับผิดชอบในทรัพย์สินอย่าง ชัดเจน

ข้อ ๑๑ ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบ เทคโนโลยีและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

หมวดที่ ๓
นโยบายว่าด้วยการบริหารจัดการข้อมูลองค์กร
(Corporate Management)

ข้อ ๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลสมเด็จ หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๒ ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลสมเด็จถือเป็นทรัพย์สินของโรงพยาบาลสมเด็จ ห้ามไม่ให้ทำการเผยแพร่เปลี่ยนแปลงทำซ้ำหรือทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓ ผู้ใช้งานมีสวนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลสมเด็จหรือข้อมูลของ ผู้รับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิดการเผยแพร่โดยไม่รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมใน การรับผิดชอบต่อความเสียหาย นั้นด้วย

ข้อ ๔ ผู้ใช้งานต้องป้องกัน ดูแลรักษาไว้ซึ่งความลับความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๕ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษาใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลสมเด็จ จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำ การละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ โรงพยาบาลสมเด็จ ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้น เกี่ยวข้องกับโรงพยาบาลสมเด็จ ซึ่ง

โรงพยาบาลสมเด็จอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวดที่ ๔
นโยบายว่าด้วยการบริหารจัดการระบบสารสนเทศ
(IT Infrastructure Management)

ข้อ ๑ ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆแต่ต้องไม่ดำเนินการดังนี้

(๑.๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการ แอบใช้รหัสผ่านการลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแก้รหัสผ่านของบุคคลอื่น

(๑.๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(๑.๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือ ไวรัสคอมพิวเตอร์

(๑.๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๑.๕) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของ ประเทศไทยกรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๒ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกันเว้นแต่จะได้รับอนุญาตจากโรงพยาบาลสมเด็จ

ข้อ ๓ ห้ามเจ้าหน้าที่สำนักงานเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนังฟังเพลง เกม เป็นต้นในระหว่างเวลาปฏิบัติราชการ

ข้อ ๔ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของโรงพยาบาลสมเด็จที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลสมเด็จ

ข้อ ๕ ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภทรวมถึงอุปกรณ์อื่นใดของโรงพยาบาลสมเด็จ เพื่อการรบกวนก่อให้เกิดความเสียหายหรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรมหรือกระทบต่อภารกิจของโรงพยาบาลสมเด็จ

ข้อ ๖ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลสมเด็จ เพื่อประโยชน์ทางการค้า

ข้อ ๗ ห้ามกระทำการใดๆเพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลสมเด็จโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆก็ตาม

ข้อ ๘ ห้ามกระทำการรบกวน ทำลายหรือทำให้ระบบสารสนเทศของโรงพยาบาลสมเด็จต้องหยุดชะงัก

ข้อ ๙ ห้ามใช้ระบบสารสนเทศของโรงพยาบาลสมเด็จ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศ

ข้อ ๑๐ ห้ามกระทำการใดๆอันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆเพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๑๑ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของโรงพยาบาลสมเด็จโดยไม่ได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศ

หมวดที่ ๕
นโยบายว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ
(Law and Compliance)

ข้อ ๑ บรรดากฎหมายใดๆที่ได้ประกาศใช้ในประเทศไทยรวมทั้งประกาศและกฎระเบียบของ โรงพยาบาลสมเด็จถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าวถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ ๖
นโยบายว่าด้วยซอฟต์แวร์และลิขสิทธิ์
(Software Licensing and intellectual property)

ข้อ ๑ โรงพยาบาลสมเด็จได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาดังนั้นซอฟต์แวร์ที่โรงพยาบาลสมเด็จอนุญาตให้ใช้งานหรือที่โรงพยาบาลสมเด็จมีลิขสิทธิ์ผู้ใช้งานสามารถข้อใช้งานได้ตามหน้าที่ความจำเป็น และโรงพยาบาลสมเด็จห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๒ ซอฟต์แวร์ (Software) ที่โรงพยาบาลสมเด็จ ได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวดที่ ๗
ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์
(Preventing Malware)

ข้อ ๑ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่งานเทคโนโลยีสารสนเทศ ได้ประกาศให้ใช้เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาพัฒนาระบบป้องกันโดยต้องได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศ

ข้อ ๒ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่พึงประสงค์ตลอดเวลารวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบโรงพยาบาลสมเด็จทันที

ข้อ ๕ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบของโรงพยาบาลสมเด็จ

ข้อ ๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความเอกสาร หรือสิ่งใดๆที่เป็นทรัพย์สินของโรงพยาบาลสมเด็จหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ (Malware) หรือโปรแกรมอันตรายใดๆที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินโรงพยาบาลสมเด็จ

หมวดที่ ๘
ว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์
(Electronic mail)

ข้อ ๑ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (Email) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (Email) ของตน

ข้อ ๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Email) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๓ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย อิเล็กทรอนิกส์ (Email) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล Email ที่หน่วยงานกำหนดไว้ ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ Email ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๔ ห้ามส่ง Email ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๕ ห้ามส่ง Email ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๖ ห้ามส่ง Email ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๗ ห้ามส่ง Email ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๘ ให้ระบุชื่อของผู้ส่งใน Email ทุกฉบับที่ส่งไป

ข้อ ๙ ให้ทำการสำรองข้อมูล Email ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล Email ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น Email ที่เก่ามากๆ และจำเป็นต้อง ใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ข้อ ๑๐ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ ๑๑ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก หรืออาจแอบอ้างเป็นบุคคลอื่น หรือองค์กร จากจดหมายอิเล็กทรอนิกส์ และสื่อสังคมออนไลน์ (Social Media) ต่างๆ ที่มีเนื้อหาในการขอข้อมูลส่วนบุคคล รหัสผ่าน เป็นต้น

ข้อ ๑๒ ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับส่งจดหมายอิเล็กทรอนิกส์ รวมไปถึงสื่อสังคม ออนไลน์ (Social Media) ต่างๆ ของทางราชการ และไม่ใช้ข้อความที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสีย ชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์ และสื่อสังคมออนไลน์ (Social Media) ต่างๆ

หมวดที่ ๙
นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย
(Wireless Policy)

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

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

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้แสดงชื่อระบบเครือข่ายไร้สายตามที่กำหนดเท่านั้น

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบ เครือข่ายภายในหน่วยงาน

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ เครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือนและในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ (System Administrator) รายงานต่องานเทคโนโลยีสารสนเทศทราบทันที

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆของหน่วยงาน

หมวดที่ ๑๐
นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์
(Firewall Policy)

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการการติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ ๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางศูนย์เทคโนโลยีสารสนเทศ อนุญาตให้ใช้งานซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความความยินยอมจากศูนย์เทคโนโลยีสารสนเทศก่อน

ข้อ ๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาต เฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้นโดยขอนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๑๐ ทำการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตเว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๒ ศูนย์เทคโนโลยีสารสนเทศมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะ ต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากศูนย์เทคโนโลยีสารสนเทศก่อน

ข้อ ๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

หมวดที่ ๑๑
นโยบายความมั่นคงปลอดภัยของอินเตอร์เน็ต
(Internet Security Policy)

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่ เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับ โรงพยาบาล

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงพยาบาล หรือที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่าน ระบบอินเทอร์เน็ต (Internet)

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

ข้อ ๔ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของโรงพยาบาล

ข้อ ๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความ เสื่อมเสียต่อชื่อเสียงของโรงพยาบาลการทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ ๖ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปลดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

หมวดที่ ๑๒
นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
(Access control Policy)

ส่วนที่ ๑ การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล เพื่อดูแลรักษาความ ปลอดภัยโดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการโรงพยาบาล

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อน เข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆและ การผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ(System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลสมเด็จ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การ ใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไรสาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้นโดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์ อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๓.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือ ยกเลิกการใช้งาน

(๓.๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๓.๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๓.๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓.๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๓.๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้ บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และควรกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึง ข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้น ความลับ ดังตอไปนี้

(๔.๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๔.๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ ละชั้นความลับของข้อมูล

(๔.๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๕.๔) การรับส่งข้อมูลสำคัญผ่าน ระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือXML Encryption เป็นตน

ข้อ ๕ ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

ข้อ ๖ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของโรงพยาบาลเช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนเป็นต้น

หมวดที่ ๑๓
นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

ข้อ ๑ งานเทคโนโลยีสารสนเทศ กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลต้องได้รับอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ ๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) จะต้องทำหนังสือขออนุญาตต่อหัวหน้า งานเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

ข้อ ๔ ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือทำการใดๆต่ออุปกรณ์ส่วนกลาง ได้แก่อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมี ประสิทธิภาพดังต่อไปนี้

(๕.๑) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๕.๒) ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๕.๓) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้

(๕.๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานควรเชื่อมต่อผ่าน อุปกรณ์ป้องกันการบุกรุกรวมทั้งควรมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕.๕) ระบบเครือข่ายควรติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาล ในลักษณะที่ผิดปกติ

(๕.๖) การเข้าสู่ระบบเครือข่ายภายในโรงพยาบาลสมเด็จโดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(๕.๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของโรงพยาบาลสมเด็จควรต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(๕.๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายใน และเครือข่ายภายนอกและอุปกรณ์ต่างๆพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๕.๙) การใช้เครื่องมือต่างๆเพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแล ระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๗ ศูนย์เทคโนโลยีสารสนเทศ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

(๗.๑) ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแล ระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ยกเว้นผู้ตรวจสอบระบบสารสนเทศของโรงพยาบาล (IT Auditor) หรือบุคคลที่โรงพยาบาลมอบหมาย

(๗.๒) ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน(Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบบันทึกการพยายามเข้าสู่ระบบบันทึกการใช้งาน Command Line และ Firewall Log เป็นต้นเพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลง

(๗.๓) ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลง บันทึกต่างๆและจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๘ ศูนย์เทคโนโลยีสารสนเทศ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทางดังต่อไปนี้

(๘.๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาลสมเด็จ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานในโรงพยาบาล ที่ได้ทำการฝากให้อยู่ในความดูแลของงานเทคโนโลยีสารสนเทศ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจาก หัวหน้างานเทคโนโลยีสารสนเทศ

(๘.๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๘.๓) วิธีการใดๆที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าศูนย์เทคโนโลยี สารสนเทศ

(๘.๔) การเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงาน อย่างเพียงพอ

(๘.๕) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

หมวดที่ ๑๔
นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล
(Backup Policy)

ข้อ ๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของ หน่วยงานจากจำเป็นมากไปหาน้อย

ข้อ ๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบ สารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ ๓ ควรจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูล สำรองซึ่งติดตั้งอยู่ที่สถานที่อื่นและควรมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ ๔ ควรมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

หมวดที่ ๑๕

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้รับจ้างภายนอก
(Outsource)

ข้อ ๑ ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (outsource) ต้อง กำหนดในคุณลักษณะเฉพาะของงาน (TOR) สัญญาจ้าง ให้ผู้รับจ้างภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยี สารสนเทศในโครงการต้องตระหนักถึงความมั่นคงปลอดภัยของระบบสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ รวมไปถึงการสื่อสารข้อมูลในโครงการที่มีผลต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ จะต้องไปถูกสื่อสารไปยังผู้ที่ไม่มีสิทธิเข้าถึง ควรสื่อสารเท่าที่จำเป็น และต้องรักษาความลับของโรงพยาบาล

ข้อ ๒ ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (outsource) จะต้องเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งาน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงาน

ข้อ ๓ ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (outsource) ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล และระบบงานต่างๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงาน และต้องขออนุญาตผู้ดูแล ระบบเครือข่ายคอมพิวเตอร์ก่อนปฏิบัติงาน

ข้อ ๔ ผู้รับผิดชอบโครงการหรืองานที่มีการจ้างผู้รับจ้างภายนอก (outsource) ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจาก ระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

ข้อ ๕ ผู้รับผิดชอบโครงการหรืองานที่มีการจ้าง ผู้รับจ้างภายนอก (outsource) หากต้องเข้าปฏิบัติงานภายในโรงพยาบาลสมเด็จ ต้องอยู่ในการดูแลของเจ้าหน้าที่งานเทคโนโลยีสารสนเทศตลอดระยะเวลาการปฏิบัติงาน

หมวดที่ ๑๖

การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ

ข้อ ๑ การเปลี่ยนแปลงอุปกรณ์ระบบเครือข่ายและการสื่อสาร ให้ดำเนินการ ดังนี้

- ผู้เกี่ยวข้องต้องดำเนินการแจ้งผู้บังคับบัญชาเป็นลายลักษณ์อักษร
- ผู้เกี่ยวข้องต้องวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงนั้นๆ
- ผู้เกี่ยวข้องต้องรายงานผลการเปลี่ยนแปลงและผลกระทบต่อผู้บังคับบัญชาเมื่อสิ้นสุดการดำเนินการ

ข้อ ๒ ประชุมร่วมกับผู้เกี่ยวข้องเพื่อพิจารณาทรัพยากรที่มีอยู่ในปัจจุบัน หากไม่เพียงพอให้ ดำเนินการจัดทำคำของบประมาณ ตามแบบฟอร์ม รายงานการจัดหาระบบคอมพิวเตอร์ภาครัฐ ที่มีมูลค่า ไม่เกิน ๕ ล้าน

ข้อ ๓ ศูนย์เทคโนโลยีสารสนเทศรวบรวมข้อมูลเสนอคณะกรรมการพิจารณาในรายละเอียดการจัดสรร

ทั้งนี้ให้บุคลากรทุกท่านนำสู่การปฏิบัติอย่างเคร่งครัด ถือเป็นหน้าที่สืบไป

(ลงชื่อ).....

(นายสมานมิตร อัฐนาค)
ผู้อำนวยการโรงพยาบาลสมเด็จ