มาตรฐานด้านเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเก้าเลี้ยว เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาล ทีมนำระบบสารสนเทศ จึงได้กำหนดแนวทางในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยอ้างอิงจากแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วย 8 หมวด ได้แก่

หมวด 1 การพิสูจน์ตัวตน (Accountability , Identification and Authentication)

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

2. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

3. ผู้ใช้งานต้องตั้งรหัสของตนเป็นข้อมูลเฉพาะเพื่อให้เกิดความปลอดภัย

4. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

5. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้งานระบบสารสนเทศของโรงพยาบาลและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านโดนล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

5.1. การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

5.2. คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

5.3. การใช้งานระบบคอมพิวเตอร์โดยอุปกรณ์อื่น ๆ ในเครือข่าย ได้แก่ แท็บเลท ไอแพด และโทรศัพท์มือถือ เป็นต้น จะต้องทำการพิสูจน์ตัวตนทุกครั้ง

5.4. เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อคหน้าจอทุกครั้ง และต้องทาการพิสูจน์ตัวตนก่อนการใช้งานในภายหลังทุกครั้ง

5.5. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen saver) โดยตั้งเวลาอย่างน้อย 15 นาที

หมวด 2 การบริหารจัดการทรัพย์สิน (Assets Management)

1. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของโรงพยาบาล ถือเป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

2. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

3. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

4. ผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

5. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์เกี่ยวกับการใช้งาน ก่อนได้รับอนุญาต

6. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่โรงพยาบาลแม่สรวยมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง

7. กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของโรงพยาบาลตาม ที่ได้รับมอบหมาย

8. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

9. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์หรือโน๊ตบุ๊คไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

10. ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่โรงพยาบาลจัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของโรงพยาบาลเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่โรงพยาบาลไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อโรงพยาบาล

11. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ 10 ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด 3 การบริหารจัดการข้อมูลขององค์กร (Corporate Management)

1. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลหรือเป็นข้อมูลของบุคลากรภายนอก

2. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของโรงพยาบาลถือเป็นทรัพย์สินของโรงพยาบาล ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำหรือ ทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

3. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาล หรือข้อมูลของผู้รับบริการหากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

4. ผู้ใช้งานต้องป้องกัน ดูแลรักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

5. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่

โรงพยาบาลอาจแต่งตั้งให้มีผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด 4 การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

1. ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ แต่ต้องไม่ดำเนินการดังนี้

1.1. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆที่จะทำลายกลไกลรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

1.2. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

1.3. พัฒนาโปรแกรมใดที่จะทาซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

1.4. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้งาน (License) ซอฟต์แวร์

1.5. นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

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

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

4. ห้ามใช้ทรัพยากรระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใด ของโรงพยาบาล ที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาล

5. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลเพื่อประโยชน์ทางการค้า

6. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

7. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลต้องหยุดชะงัก

8. ห้ามใช้ระบบสารสนเทศของโรงพยาบาลเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

9. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

10. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อให้สามารถเข้าถึงระบบสารสนเทศของโรงพยาบาลโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด 5 การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

1. กฎหมายที่ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของโรงพยาบาล ถือว่าเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัดและไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด 6 ซอฟแวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

1. โรงพยาบาลได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟแวร์ที่โรงพยาบาลอนุญาตให้ใช้งานหรือที่โรงพยาบาลมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ ความจำเป็นและโรงพยาบาลห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ โรงพยาบาลถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

2. ซอฟแวร์ (Software) ที่โรงพยาบาลได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

หมวด 7 การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Mal Ware)

1. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่โรงพยาบาลได้ประกาศให้ใช้ หมั่นตรวจสอบและอัพเดทระบบปฏิบัติการ (Operating System) เช่น Windows หรือซอฟต์แวร์ที่ใช้ให้เป็นเวอร์ชั่นปัจจุบัน เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนาระบบป้องกันโดยต้องได้รับอนุญาตจากผู้ดูแลระบบ

2. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

3. ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

4. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา เมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทราบ

5. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทราบ

6. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของโรงพยาบาล หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

7. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของโรงพยาบาล

หมวด 8 การใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Electronic mail)

1. ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศว่าด้วยการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail Policy) ดังนี้

1.1. ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

1.2. ควรเปลี่ยนรหัสผ่าน (Password) ทุก 3 - 6 เดือน

1.3. ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email address) ของผู้อื่นเพื่ออ่านหรือรับ ส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (Email) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (Email) ของตน

1.4. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Email) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง