ประกาศโรงพยาบาลสัตหีบกม.10
เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลสัตหีบกม.10 พ.ศ.2567

ตามประกาศของกระทรวงสาธารณสุข เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข และประกาศโรงพยาบาลสัตหีบกม.10 เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลสัตหีบ กม.10 ที่กำหนดให้บุคลากรทุกระดับปฏิบัติตามแนวปฏิบัติฯ นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกระทรวงสาธารณสุข เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสมารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ โรงพยาบาลสัตหีบ กม.10 จึงได้ประกาศแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด ดังนี้

1.ประกาศฉบับนี้มีวัตถุประสงค์เพื่อเผยแพร่แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลสัตหีบกม.10 พ.ศ.2567 ให้บุคลากรทุกระดับในหน่วยงาน และผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบเข้าใจและถือปฏิบัติ

2.บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

3.ให้บุคลากรทุกระดับของโรงพยาบาลสัตหีบกม.10 ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลสัตหีบกม.10 พ.ศ. 2567 ตามแนบท้ายประกาศนี้อย่างเคร่งครัด

ประกาศ ณ วันที่ 1 กุมภาพันธ์ 2567

(นายชีวิน ประพันธ์)
ผู้อำนวยการโรงพยาบาลสัตหีบกม.10

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลสัตหีบกม.10 พ.ศ. 2567

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลสัตหีบ กม.10

หมวดที่ 1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรของกลุ่มแผนงานมีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุม การใช้งานสารสนเทศ (Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

แนวปฏิบัติ

1.การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

1.1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

1.2 เจ้าหน้าที่ITมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ

1.3 เจ้าหน้าที่ITมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password)ให้กับผู้ใช้งานสำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

1.4 ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

1.5 เมื่อมีความจำเป็นต้องให้บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาล ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูงหรือหัวหน้าหน่วยงานแล้ว แต่กรณีเพื่อให้ความเห็นชอบ และอนุญาตก่อนให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณีเพื่อให้ ความเห็นชอบ และอนุญาตก่อน และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

2. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

2.1 สิทธิของผู้ใช้งาน (User) ได้ตามสิทธิการเข้าถึงข้อมูล

2.2 สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

3. การจัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วย การรักษา ความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการ เอกสาร อิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนด กระบวนการ และ กรรมวิธีต่อ เอกสาร ที่สำคัญไว้ดังนี้

3.1 จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

3.2 จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้ เกิดความเสียหาย อย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายอย่างร้ายแรงมาก

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความ เสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

3.3 จัดแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูล ยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงิน และบัญชี

-ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุขเป็นข้อมูลที่เกี่ยวข้องกับ การรักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และ ข้อมูล สถานพยาบาล

3.4 จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับ บัญชาในหน่วยงานนั้น

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึง ได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้ โดยสิทธิที่ได้รับมอบหมายตามอำนาจหน้าที่

4. ช่องทางการเข้าถึงสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ 2 ช่องทาง ดังนี้

4.1 ระบบเครือข่ายภายใน (Intranet)

4.2 ระบบเครือข่ายภายนอก (Internet)

หมวดที่ 2 การบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้วและสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

1. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

1.1 เจ้าหน้าที่ITของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ อย่างน้อยประกอบด้วยชื่อ นามสกุล ตำแหน่ง หน่วยงาน และหมายเลขโทรศัพท์

1.2 การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

1.2.1 กรณีบุคลากรโรงพยาบาล

1.2.1.1 จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และ

ระบบสารสนเทศ

1.2.1.2 เจ้าหน้าที่IT ต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

1.2.1.3 เจ้าหน้าที่IT ต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ ความรับผิดชอบ

1.2.2 กรณีบุคคลภายนอก

1.2.2.1ให้บุคคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลในการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด

1.3 การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

1.3.1การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

1.3.1.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

1.3.1.2 กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

1.3.1.3 ส่งมอบรหัสผ่าน (Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกัน ในการส่งรหัสผ่าน (Password)

1.3.1.4 กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน 3 ครั้ง

1.3.1.5 กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

1.3.2 ให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน ทราบโดยตรง

1.3.3 เมื่อผู้ใช้งาน มีการเปลี่ยนข้อมูลให้แจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลผู้ใช้งาน

1.3.4 ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่าน(Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2. การยกเลิกสิทธิการใช้งานของบุคลากร หรือบุคคลภายนอกให้ดำเนินการ ดังนี้ เจ้าหน้าที่ITต้องดำเนินงานการยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุด การจ้าง

3. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ของผู้ใช้งาน ให้ดำเนินการ ดังนี้

3.1 ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้ดำเนินการแจ้งเจ้าหน้าที่IT เพื่อให้เจ้าหน้าที่ IT เปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

3.2. ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้รับผิดชอบงานด้านสารสนเทศเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตาม

หลักเกณฑ์ ดังนี้ กรณีที่ผู้ใช้งาน ลืมรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ วิธีการขอแจ้งเจ้าหน้าที่IT กำหนด เช่น โทรศัพท์ หรือ ออนไลน์

5. เจ้าหน้าที่IT ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย

หมวดที่ 3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลับลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

แนวปฏิบัติ

1. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

1.1 ผู้ใช้งานต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

1.2 ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) ส าหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

1.3 หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็น ในการเข้าถึง หลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

1.4 หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของ บัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว

2. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

หมวดที่ 4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของโรงพยาบาลสัตหีบกม.10 ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเตอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติ

1. การเข้าถึงเครือข่ายของผู้ใช้งาน

1.2 ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของโรงพยาบาลสัตหีบกม.10มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

1.1.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการ

เครือข่ายอินเตอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่งานสารสนเทศโรงพยาบาลสัตหีบกม.10 โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลสัตหีบกม.10 สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้างานสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

1.1.2ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication)

1.1.3 ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

1.1.4 ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลเครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

1.1.5 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

1.1.6 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

1.1.7 ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

1.1.8ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของงานของหน่วยงานเว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

1.1.9 ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเคร่งครัด

1.1.10 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจาก การเครือข่ายอินเตอร์เน็ตด้วยการ Logoutจากการ Authentication เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่นๆ

1.2 การใช้งานเครือข่ายอินเตอร์เน็ตหรือเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

1.2.1 ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) การใช้งานเครือข่ายอินเตอร์เน็ตไร้สาย (WiFi)

1.2.2 ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของโรงพยาบาลไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

1.2.3 ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของโรงพยาบาล และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

1.3 การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

1.3.1 ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของโรงพยาบาล ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

1.3.2 กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณาความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

1.3.3 ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากหน่วยงานและต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

1.3.4 หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

หมวดที่ 5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

1. ผู้ใช้งานต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ

2. ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น ค่าคอนฟิกกูเรชั่น (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น

3. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้

3.1 ผู้ใช้งานต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใด ๆ บนระบบปฏิบัติการ ทั้งนี้ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อเจ้าหน้าที่IT

3.2 การใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ เช่น โปรแกรมดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatterกำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่มีสิทธิใช้งาน

หมวดที่ 6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control) โดยไม่ได้รับอนุญาต

แนวปฏิบัติ

1. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการดังนี้

1.1 ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งานที่เข้าถึงระบบคอมพิวเตอร์ และ ระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)

1.2 การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก

1.3 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ปฏิบัติงานจากภายนอกองค์กร (Mobile

Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการ รบกวนมีผลกระทบและมีความสำคัญสูงต่อโรงพยาบาลสัตหีบกม.10 ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากกลุ่มงานประกันสุขภาพ

2.การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) กำหนด ดังนี้

2.1 ผู้ใช้งานต้องปฏิบัติตามหมวด 6 แนวปฏิบัติ ข้อ 1 การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

2.2 เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งานต้องระมัดระวังไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้ และต้องออกจากระบบ (Log Out) ทันทีเมื่อปฏิบัติเลิกใช้งาน

หมวดที่ 7 การจัดทำระบบสำรองของระบบสารสนเทศ (Disaster Recovery Site)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกลุ่มแผนงาน ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่างๆและสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสมและสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

แนวปฏิบัติ

1. เจ้าหน้าที่ITจะต้องจัดทำสำรองของระบบสารสนเทศโดยมีขั้นตอน ดังนี้

1.1 เจ้าหน้าที่ITต้องจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

1.2 กำหนดรูปการสำรองข้อมูลระบบสารสนเทศ ดังนี้

1.2.1 คัดเลือกระบบสารสนเทศในการสำรองข้อมูล

1.2.2 กำหนดรูปแบบการสำรองข้อมูล เช่น เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) แบบสมบูรณ์ (Full Backup)

1.2.3 กำหนดความถี่ในการสำรองข้อมูลตามความเหมาะสมของระบบสารสนเทศ

1.3 เจ้าหน้าที่ITดำเนินการสำรองของระบบสารสนเทศ ตามข้อที่ 1.2

2. เจ้าหน้าที่ITต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่สำรองไว้ อย่างน้อย 1 ระบบ โดยอย่างน้อยปีละ 1 ครั้ง

3. มีการทบทวนระบบสารสนเทศในการระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

หมวดที่ 8 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

แนวปฏิบัติ

1. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

2.กำหนดแนวทางเพื่อรองรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

2.1 หน่วยงานต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

2.2 ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้หน่วยงาน สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งกลุ่มแผนงานเป็นลายลักษณ์อักษร

2.3 ในกรณีต้องการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
(Read Only)

หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

1. จัดให้มีขั้นตอนหรือกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่สำคัญ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถ และประสบการณ์ โดยมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

1.1 การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

1.2 การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

1.3 จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ และรายงานเหตุการณ์ ผู้ที่เกี่ยวข้องให้ทราบและดำเนินการต่อไป

1.4 การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติ

1.5 วิเคราะห์ รวบรวมและรายงานเหตุการณ์ต่อผู้บังคับบัญชาทราบ ทั้งนี้ เพื่อระบุถึงสาเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

2. ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคล หรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยให้ดำเนินการดังนี้

2.1 แจ้งเจ้าหน้าที่IT โดยช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เช่น Social Network, E- mail เป็นต้น ทั้งนี้ เนื้อหาขั้นต่ำ ต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น

2.2 รายงานผู้บังคับบัญชาเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น

- การบุกรุกด้านกายภาพ

- การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- การเปลี่ยนแปลง การเข้าถึงโดยไม่ได้รับอนุญาต
- การทำงานผิดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ หรือการปฏิบัติงาน

จัดให้มีบุคคลหรือหน่วยงานงาน (point of contact) เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นต่อผู้บังคับบัญชา โดยให้รายงานดังต่อไปนี้

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและ สาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ชื่อผู้ติดต่อ/ประสานงานของบริษัทเพื่อให้ข้อมูล	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและ สาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ดำเนินการแก้ไขปัญหาและระยะเวลาในการแก้ไข 5. ความคืบหน้าในการแก้ไขปัญหา	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและ สาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น โดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้น 4. ดำเนินการแก้ไขปัญหา 5. ผลการแก้ ไขปัญหา และระยะเวลาในการแก้ไข 6. แนวทางป้องกันในอนาคตและการเก็บรวบรวมหลักฐาน เพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่ รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว	รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่ รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว	รายงานเป็นลายลักษณ์อักษรโดยมีเนื้อหาจากข้อมูลข้างต้น

หมวดที่ 10 การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource)

เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ ศูนย์ข้อมูลและสารสนเทศ และพื้นที่ปฏิบัติงานทั่วไป ซึ่งเป็นทรัพย์สินที่มีค่าของโรงพยาบาลสัตหีบกม.10 มีความปลอดภัยต่อการถูกบุกรุกโจมตีและลดความเสี่ยงต่อลักลอบเปิดเผยข้อมูลสารสนเทศ จึงกำหนดแนวปฏิบัติการควบคุมการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource) ดังนี้

1. ก่อนปฏิบัติงาน

1.1 ผู้รับจ้าง (Outsource) ต้องขออนุญาตหัวหน้าส่วนราชการนั้น ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก ตามหมวดที่ 2

1.2 หัวหน้าส่วนราชการหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร

2. ระหว่างปฏิบัติงาน

2.1 ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

2.2 เจ้าหน้าที่ITหรือผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนราชการต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้างโดยเฉพาะการติดตั้ง ซ่อมแซม หรือการเปลี่ยนอุปกรณ์ประมวลผลข้อมูล ภายในห้องศูนย์ข้อมูล (Data Center) ต้องกำกับดูแลโดยเคร่งครัด

2.3 ผู้รับจ้างต้องปฏิบัติตามหน้าที่ที่ได้รับมอบหมายเท่านั้นและต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ได้รับมอบหมายที่กำกับดูแลการปฏิบัติงานทันที

3. หลังปฏิบัติงาน

3.1 ให้ผู้รับจ้างแจ้งความประสงค์ต่อเจ้าหน้าที่เพื่อยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

3.2 เจ้าหน้าที่IT จะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ และลบข้อมูลสารสนเทศของผู้รับจ้างเป็นการถาวรทันทีเมื่อสิ้นสุดการจ้างงานหรือข้อตกลงร่วมกัน

4. การรักษาความลับ

ผู้รับจ้างต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

เจ้าหน้าที่ผู้ได้รับมอบหมายให้สำรองข้อมูลของระบบสารสนเทศ ของโรงพยาบาลสัตหีบกม.10 ได้แก่

1. นายภูมิพัฒน์ แก้วแหวน นักวิชาการคอมพิวเตอร์ปฏิบัติการ

2.นางสาวอัจฉรา ศรีเพริศ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หมวดที่ 11 การบริหารจัดการสินทรัพย์(Assets Management)

1. ผู้ใช้งานต้องไม่เข้าไปในศูนย์ข้อมูล (Data Center) หมายถึง สถานที่ที่ใช้สำหรับติดตั้ง เครื่องคอมพิวเตอร์ แม่ข่าย และ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวง ห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

2. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

3. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจ ส่วนบุคคล

4. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับ อนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

5. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัด อุปกรณ์

ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญและข้อมูล อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธินั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึก ข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็น มาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็น มาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

6. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง

7. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติ เป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

8. ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใด ๆ ที่เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ พกพา หรือระบบคอมพิวเตอร์และระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าหน้าที่IT

9. ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรือ เพื่อป้องกันการรั่วไหลของข้อมูล

10. กรณีปฏิบัติงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับ มอบหมาย

11.ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่า ทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

12. ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และ ระบบสารสนเทศ ต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อโรงพยาบาลสัตหีบ กม.10

13. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ 10. ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้อง

รับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวดที่ 12 การปฏิบัติงานจากภายนอกสำนักงาน(Teleworking)

1. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยี สารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

2. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และ อุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

3. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

4. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ หน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของ หน่วยงาน

5. ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการ ต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

6. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุง สิทธิการเข้าถึงระบบสารสนเทศและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

หมวดที่ 13 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

1.แนวทางปฏิบัติการใช้งานทั่วไป

1.1 เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ ใน งานราชการ

1.2ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ ส่วนบุคคลของหน่วยงาน

1.3การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดย เจ้าหน้าที่IT หรือบุคคล/บริษัทภายนอกที่ได้รับอนุญาต เท่านั้น

1.4 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรม ป้องกันไวรัส

1.5 ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

1.6 ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง

1.7ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวบุคคลที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน โดยไม่มีการติดตั้งโปรแกรมป้องกันไวรัส อย่างเหมาะสมและต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานอย่างเคร่งครัด ยกเว้นจะได้รับการตรวจสอบจากเจ้าหน้าที่IT ของหน่วยงานก่อนการใช้งาน

2. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

2.1ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

2.2ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลด มาจาก

อินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

2.3 ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผล ทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

2.4 อุปกรณ์สื่อบันทึกข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายตามวิธีการที่กำหนดไว้ใน หมวดที่11

3.การสำรองข้อมูลและการกู้คืน

3.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

3.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้ อย่างสม่ำเสมอ

3.3 ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูล สำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อ การดำเนินการของหน่วยงาน

หมวดที่14 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

1. แนวทางปฏิบัติการใช้งานทั่วไป

1.1 เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ

1.2 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่าง ปลอดภัยและมีประสิทธิภาพ

1.3 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ ให้มีสภาพเดิม

1.4 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

1.5 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีด ข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

1.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

1.7 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปใน แนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

1.8 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อน จัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่

1.9การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้ แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.ความปลอดภัยทางด้านกายภาพ

2.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ ใช้งาน ไม่

วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น /ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3. การสำรองข้อมูลและการกู้คืน

3.1ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและ สื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

3.2ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

3.3แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

3.4 ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับ การทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการ ดำเนินการของหน่วยงาน

หมวดที่15 แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้นเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์(Firewall) ของโรงพยาบาลสัตหีบกม.10 มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

1.1 งานสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลสัตหีบกม.10

1.2 การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

1.3 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

1.4 ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

1.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

1.7ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

1.8 การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลสัตหีบกม.10ให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากหัวหน้างานสารสนเทศ ก่อน

1.9 การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้นโดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้างานสารสนเทศ โดยต้องระบุข้อมูลดังนี้

1.9.1 หมายเลข Port ที่ต้องการขอให้เปิด

1.9.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

1.9.3 วัตถุประสงค์หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

1.9.4 วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

1.10 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

1.11 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

1.12 โรงพยาบาลสัตหีบกม.10 มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลสัตหีบกม.10 หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

1.13 ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบ ของโรงพยาบาลสัตหีบกม.10 หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางงานสารสนเทศจะยกเลิกการให้บริการทันที

1.14 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากโรงพยาบาลสัตหีบกม.10ก่อน