



นโยบายการรักษาความมั่นคงปลอดภัยของ

ระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลศิริราช

พ.ศ. 2555

โดย

ทีมสารสนเทศ (IM)

โรงพยาบาลศิริราช

สารบัญ

หน้า

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

คำนิยาม

โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับโรงพยาบาล

การบริหารจัดการทรัพย์สินของโรงพยาบาล

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของโรงพยาบาล

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

เอกสารอ้างอิง

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลทุ่งใหญ่

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

- 1.1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้มีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ
- 1.2. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC 27001
- 1.3. นโยบายนี้ต้องเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลทุ่งใหญ่ได้รับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- 1.4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
- 1.5. เพื่อป้องกันมิให้มีผู้กระทำการหรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก่ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ
- 1.6. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

2. องค์ประกอบของนโยบาย

- 2.1. คำนิยาม
- 2.2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับโรงพยาบาล
- 2.3. การบริหารจัดการทรัพย์สินของโรงพยาบาล
- 2.4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
- 2.5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- 2.6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของโรงพยาบาล
- 2.7. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อที่จะทำให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอยู่ในระดับที่ปลอดภัย

นโยบายการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบสารสนเทศซึ่งเจ้าหน้าที่ของโรงพยาบาลทุ่งใหญ่จะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **โรงพยาบาล** หมายถึง โรงพยาบาลทุ่งใหญ่
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งใหญ่
- **มาตรการ** หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น
- **วิธีปฏิบัติ** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลทุ่งใหญ่
- **ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว
- **สารสนเทศ** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่รูปของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้ เช่น ระบบแลน (LAN) ระบบอินเทอร์เน็ต (Internet)
 - **ระบบแลน (LAN)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อกับคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
 - **ระบบอินเทอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถ

นำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูล และสารสนเทศ เป็นต้น

- **การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ** หมายถึง การตรวจสอบการอนุมัติ และการกำหนดสิทธิในการผ่านเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้
- **เครื่องเซิร์ฟเวอร์ (Server)** หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่ายในระบบเครือข่าย
- **อุปกรณ์ UPS** หมายถึง เครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่เกิดไฟจากฟ้า ไฟฟ้าเกิดมีปัญหาขึ้นมา เช่น ไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่ UPS จะจ่ายพลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ์ ตลอดจนเป็นอุปกรณ์ที่ช่วยป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟ้า และอุปกรณ์อิเล็กทรอนิกส์ (โดยเฉพาะคอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า
- **ซอฟต์แวร์ (software)** หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวร์จึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหล่านี้เรียงกันเป็นโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เป็นตัวเลขตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้
โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์จึงเป็นซอฟต์แวร์ เพราะเป็นลำดับขั้นตอนการทำงานของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟต์แวร์ที่แตกต่างกัน ซอฟต์แวร์จึงหมายถึงรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้
- **ไวรัสคอมพิวเตอร์** หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบ คอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้กับเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน
การที่คอมพิวเตอร์ติดไวรัส หมายถึงไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว

- **เวชระเบียน** หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่เป็นเอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลทุ่งใหญ่
- **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

ส่วนที่ 1

โครงสร้างทางด้านการมั่นคงปลอดภัยสำหรับโรงพยาบาล (Organization of information security)

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. มาตรการและแนวทางปฏิบัติ

โครงสร้างทางด้านการมั่นคงปลอดภัยภายในองค์กร

1. ผู้บริหารต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านการมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดค่านิยมที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2. คณะกรรมการบริหารโรงพยาบาลต้องกำหนดให้มีตัวแทนเจ้าหน้าที่จากหน่วยงานต่างๆ ภายในโรงพยาบาลเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร

3. คณะกรรมการสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการดำเนินงานทางด้านการมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลไว้อย่างชัดเจน

4. คณะกรรมการสารสนเทศต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อโรงพยาบาล

ส่วนที่ 2

การบริหารจัดการทรัพย์สินของโรงพยาบาล (Asset management)

1. วัตถุประสงค์

เพื่อเป็นมาตรการในการป้องกันทรัพย์สินของโรงพยาบาลจากความเสียหายที่อาจเกิดขึ้นได้จากมนุษย์หรือภัยพิบัติต่างๆ

2. มาตรการและแนวทางปฏิบัติ

หน้าที่ความรับผิดชอบต่อทรัพย์สินของโรงพยาบาล

1. หัวหน้างานพัสดุและผู้ดูแลระบบ ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อโรงพยาบาลให้ถูกต้องอยู่เสมอ
2. หัวหน้างานพัสดุและผู้ดูแลระบบ ต้องจัดให้มีการระบุผู้เป็นเจ้าของทรัพย์สินสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน
3. หัวหน้างานพัสดุและผู้ดูแลระบบ จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานอุปกรณ์สารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น

ส่วนที่ 3

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

1. วัตถุประสงค์

เพื่อเป็นมาตรการให้เจ้าหน้าที่ได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทเมื่อมีการลาออกหรือย้ายหน่วยงาน

2. มาตรการและแนวทางปฏิบัติ

2.1. กลุ่มงานการจัดการต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่ลาออกหรือย้ายหน่วยงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

2.2. ผู้ดูแลระบบต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่ลาออกหรือย้ายหน่วยงาน

3. วิธีปฏิบัติ

วิธีปฏิบัติเรื่อง การจัดการการลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่

ส่วนที่ 4

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

1. วัตถุประสงค์

เพื่อเป็นมาตรการในการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินของโรงพยาบาล

2. มาตรการและแนวทางปฏิบัติ

2.1. บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1.1. คณะกรรมการสารสนเทศต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

2.1.2. คณะกรรมการสารสนเทศต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม ปลวก หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

2.2. ความมั่นคงปลอดภัยของอุปกรณ์รวมถึงแฟ้มเวชระเบียน

2.2.1. เจ้าหน้าที่ต้องจัดวางและป้องกันอุปกรณ์ภายในหน่วยงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2.2.2. ต้องกำหนดให้มีการเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

3. วิธีปฏิบัติ

วิธีปฏิบัติเรื่อง การใช้งานห้องเครื่อง Server

ส่วนที่ 5

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ ของโรงพยาบาล

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศและซอฟต์แวร์ให้ เป็นไปอย่างถูกต้องสมบูรณ์ ปลอดภัยจากการถูกทำลาย และมีความพร้อมใช้ของสารสนเทศ

2. มาตรการและแนวทางปฏิบัติ

2.1. การป้องกันโปรแกรมที่ไม่ประสงค์ดี

2.1.1. ผู้ดูแลระบบต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกักกลับคืน เพื่อ ป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี

2.1.2. ผู้ดูแลระบบต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ และต้อง ป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

2.2. การสำรองข้อมูล

คณะกรรมการสารสนเทศต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่าง สม่าเสมอ

2.3. การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายของโรงพยาบาล

คณะกรรมการสารสนเทศต้องกำหนดการบริหารจัดการสำหรับบริการเครือข่ายและ สารสนเทศของโรงพยาบาล

3. วิธีปฏิบัติ

1. วิธีปฏิบัติเรื่อง การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
2. วิธีปฏิบัติเรื่อง การจัดการไวรัสคอมพิวเตอร์
3. วิธีปฏิบัติเรื่อง การสำรองข้อมูล
4. วิธีปฏิบัติเรื่อง การสำรองข้อมูลเวชระเบียนที่จัดเก็บในรูปแบบ Electronic Files
5. วิธีปฏิบัติเรื่อง การใช้งานคอมพิวเตอร์และเครือข่าย

ส่วนที่ 6

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกที่จะสร้างความเสียหายแก่ข้อมูล

2. มาตรการและแนวทางปฏิบัติ

2.1. การบริหารจัดการการเข้าถึงของผู้ใช้

2.1.1. ผู้ดูแลระบบต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

2.1.2. ผู้ดูแลระบบต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

2.2. หน้าที่ความรับผิดชอบของผู้ใช้

เจ้าหน้าที่ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สารสนเทศที่ไม่มีเจ้าหน้าที่ดูแล

2.3. การควบคุมการเข้าถึงระบบปฏิบัติการ

2.3.1. ผู้ดูแลระบบต้องจัดให้ผู้ที่มีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และจะต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

2.3.2. ผู้ดูแลระบบต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

2.3.3. ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

2.3.4. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

2.4. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ

ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

3. วิธีปฏิบัติ

- 3.1.1. วิธีปฏิบัติเรื่อง การจัดเก็บข้อมูลตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐
- 3.1.2. วิธีปฏิบัติเรื่อง การตั้งรหัสผ่าน กำหนดและป้องกันรหัสผ่าน
- 3.1.3. วิธีปฏิบัติเรื่อง การรักษาความปลอดภัย/ ป้องกันการสูญหายของแฟ้มเวชระเบียนที่จัดเก็บในรูปแบบ Electronic File และป้องกันการโจรกรรมข้อมูล

(ลงชื่อ)



(นายแพทย์ศรัณยู ไกรนรา)
ผู้อำนวยการโรงพยาบาลทุ่งใหญ่
วันที่ 22 พฤษภาคม 2555

เอกสารอ้างอิง

คณะกรรมการด้านความมั่นคง ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2550.

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5)

ประจำปี 2550. หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ.