# นโยบายการรักษาความมั่นคงปลอดภัย

# ระบบเทคโนโลยีสารสนเทศ

# นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช

## 1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและ สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศใน ลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคง ปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ ให้ครอบคลุมด้านการ รักษาความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ดังต่อไปนี้

1.1. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้มีความมั่นคง ปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ

1.2. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อ้างอิงตามมาตรฐาน ISO/IEC 27001

1.3. เผยแพร่นโยบายให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราชได้รับทราบและถือปฏิบัติตาม นโยบาย นี้อย่างเคร่งครัด

1.4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบตระหนักถึง ความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติ ตามอย่างเคร่งครัด

1.5. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆ เขาล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นใน ระบบ สารสนเทศโดยมิชอบ

1.6. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี

**2. องค์ประกอบของนโยบาย**

2.1 คำนิยาม

2.2 การบริหารจัดการทรัพย์สินของโรงพยาบาล

2.3 ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากร

2.4 การสรางความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดลอม

2.5 การบริหารจัดการดานการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของโรงพยาบาล

2.6 การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติใน การรักษาความมั่นคงปลอดภัย ระบบสารสนเทศ เพื่อที่จะทำให้มีมาตรการในการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศอยู่ในระดับที่ปลอดภัย นโยบาย การเข้าใช้งานระบบสารสนเทศของโรงพยาบาลนี้จัดเป็นมาตรฐานด้านความ ปลอดภัยในการใช้งานระบบสารสนเทศซึ่ง เจ้าหน้าที่ของโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช จะต้องปฏิบัติตามอย่าง เคร่งครัด

**คำนิยาม**

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- โรงพยาบาล หมายถึง โรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช
- การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช
- มาตรการ หมายถึง วิธีการที่ตั้งเป็นกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเป็นต้น
- วิธีปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้ กำหนดไว้ตามวัตถุประสงค์
- แนวทางปฏิบัติ หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุ เป้าหมายได้ง่ายขึ้น
- ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช
- ผู้ดูแลระบบ หมายถึง เจ้าหนาที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษา ระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเขาถึงโปรแกรมเครือขายคอมพิวเตอร์เพื่อการจัดการฐานขอมูลของเครือข่าย คอมพิวเตอร์
- เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจางประจำ และลูกจ้างชั่วคราว
- สารสนเทศ หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่รูป ของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถ นำไปใช้ประโยชน ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มี การกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือ ชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูล โดยอัตโนมัติ
- ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่าง ระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได้ เช่น ระบบแลน (LAN) ระบบอินเตอร์เน็ต (Internet)
    - ♣ ระบบแลน (LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ คอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อ การติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
    - ♣ ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบเครือขายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

● ระบบเทคโนโลยีสารสนเทศ หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถ นำมาใช้ประโยชน์ในการวางแผน บริหารการสนับสนุนการให้บริการ การพัฒนาและควบคุมการ ติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูล และสารสนเทศ เป็นต้น

● การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ หมายถึง การตรวจสอบการอนุมัติ และการกำหนดสิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้

● เครื่องเซิรฟเวอร์(Server) หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ที่ทำ หน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แกเครื่องคอมพิวเตอร์หรือ โปรแกรมคอมพิวเตอร์ที่เป็นลูกข่ายในระบบ เครือข่าย

● อุปกรณ์ UPS หมายถึง เครื่องสำรองไฟฟาและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการไฟฟ้าเกิดมีปัญหาขึ้นมา เช่นไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่ UPS จะจ่าย พลังงานออกมาอย่างต่อเนื่องและมี คุณภาพในทุกสถานการณ์ ตลอดจนเป็นอุปกรณ์ที่ช่วย ป้องกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟา และ อุปกรณ์อิเล็กทรอนิคส์ (โดยเฉพาะ คอมพิวเตอร์และอุปกรณ์เชื่อมต่อ) รวมถึงมีหน้าที่ในการจ่ายพลังงานไฟฟ้าสำรองจาก แบตเตอรี่ ให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า

● ซอฟตแวร์(software) หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน ซอฟต์แวรจึง หมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นด้วยคำสั่งของคอมพิวเตอร์ คำสั่งเหลานี้เรียงกันเป็นโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแล้วว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเป็นเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใช้แทนข้อมูลที่เปนตัวเลข ตัวอักษร รูปภาพ หรือแม้แต่เป็นเสียงพูดก็ได้ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอร์ จึงเป็นซอฟตแวร์เพราะเป็นลำดับขั้นตอนการ ทำงานของคอมพิวเตอร์ คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้ มากมายด้วยซอฟตแวร์ที่ แตกต่างกัน ซอฟต์แวรจึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ ทำงานได้

● ไวรัสคอมพิวเตอร์ หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเขาไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเขาไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติด ไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้ เช่นกัน การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำคอมพิวเตอร์เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นโปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ ในหน่วยความจำ ได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้นยังขึ้นอยู่กับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกไวรัสคอมพิวเตอร์ขึ้นมาทำงานแล้ว

● เวชระเบียน หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่ เป็นเอกสารและข้อมูลอิเล็กทรอนิกส์ของผู้ป่วยแต่ละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช

● ทรัพย์สิน หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

ส่วนที่ 1 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับโรงพยาบาล (Organization of information security)

1. วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวของกับระบบ เทคโนโลยีสารสนเทศ ซึ่งเป็นทรัพยสินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ ซึ่งมีสวนเกี่ยวของกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. มาตรการและแนวทางปฏิบัติ โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร

2.1 ผู้บริหารต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความ มั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคลอง การมอบหมายงานที่ เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบใน การสรางความมั่นคงปลอดภัยให กับสารสนเทศ

2.2 คณะกรรมการบริหารโรงพยาบาลต้องกำหนดให้มีตัวแทนเจ้าหน้าที่จากหน่วยงานต่างๆ ภายในโรงพยาบาลเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร

2.3 คณะกรรมการสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการ ดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลไว้อย่างชัดเจน

2.4 คณะกรรมการสารสนเทศต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวของกับความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยผู้ตรวจสอบอิสระตาม รอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อโรงพยาบาล

## การบริหารจัดการทรัพย์สินของโรงพยาบาล (Asset management)

1. วัตถุประสงค์ เพื่อเป็นมาตรการในการป้องกันทรัพย์สินของโรงพยาบาลจากความเสียหายที่อาจเกิดขึ้นได้จากมนุษย์ หรือภัยพิบัติต่างๆ และมีอุปกรณ์พร้อมใช้งาน

2. มาตรการและแนวทางปฏิบัติ หน้าที่ความรับผิดชอบต่อทรัพยสินของโรงพยาบาล

2.1 หัวหน้างานพัสดุและผู้ดูแลระบบ ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพยสินที่มีความสำคัญต่อโรง พยาบาลให้ถูกต้องอยู่เสมอ

2.2 หัวหน้างานพัสดุและผู้ดูแลระบบ ต้องจัดให้มีการระบุผู้เป็นเจ้าของทรัพยสินสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพยสิน

2.3 หัวหน้างานพัสดุและผู้ดูแลระบบ จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานอุปกรณ์สารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น

3. วิธีปฏิบัติ

3.1 จัดทำทะเบียนครุภัณฑ์คอมพิวเตอร์

3.2 มีแผนบริหารจัดการ วัสดุ ครุภัณฑ์คอมพิวเตอร์

3.3 มีแผนบำรุงรักษาครุภัณฑ์คอมพิวเตอร์

## ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

1. วัตถุประสงค์ เพื่อเป็นมาตรการให้เจ้าหน้าที่ได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทเมื่อมีการย้ายเข้า ลาออกหรือย้ายหน่วยงาน

2. มาตรการและแนวทางปฏิบัติ

2.1 กลุ่มงานการจัดการต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่ย้ายเข้า ลาออกหรือย้ายหน่วยงาน และ กำหนดให้ ปฏิบัติตามหน้าที่ดังกล่าว

2.2 ผู้ดูแลระบบต้องทำการเพิ่ม หรือ ถอดถอนสิทธิ์ในการเขาถึงสารสนเทศและทรัพยสินสารสนเทศของผู้ที่ย้ายเข้า ลาออกหรือ ย้ายหน่วยงาน

3. วิธีปฏิบัติ

3.1 การเพิ่มสิทธิ์การเข้าใช้ระบบสารสนเทศ

3.1.1 เพิ่มเมื่อผู้ใช้งานได้เข้ามาทำงานในโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช โดยดำเนินหลังจากได้ดำเนินการด้านธุรการ มีการระบุตำแหน่งการทำงานและฝ่ายในการปฏิบัติงาน โดยผู้ใช้งานมีการร้องขอสิทธิ์ และหัวหน้างานยินยอมการเข้าใช้งานสารสนเทศเป็นลายลักษณ์อักษร

3.1.2 การเพิ่มสิทธิ์การเข้าใช้งานเพิ่มเติมภายหลัง เมื่อมีการปรับเปลี่ยนหน้าที่ความรับผิดชอบโดยความเห็นชอบจากหัวหน้างานของผู้ใช้งาน

3.2 การลด เพิกถอนสิทธิ์การเข้าใช้งานสารสนเทศ

3.2.1 การลดทอนสิทธิ์การเข้าใช้งานระบบสารสนเทศ จะลดทอนตามคำร้องขอของผู้ใช้งานระบบ หรือ หัวหน้างาน หรือ การปรับเปลี่ยนระบบสารสนเทศของโรงพยาบาล

3.2.2 การเพิกถอนสิทธิ์การเข้าใช้งานระบบสารสนเทศ จะกระทำตามการร้องขอของหัวหน้างานด้านบุคลากรโรงพยาบาล เมื่อยืนยันว่าบุคคลดังกล่าวได้ ลาออก หรือย้ายสถานที่ปฏิบัติงาน จากโรงพยาบาลเฉลิมพระเกียรติ จังหวัดนครศรีธรรมราช

## การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดลอม
## (Physical and environmental security)

1. วัตถุประสงค์ เพื่อเป็นมาตรการในการป้องกันการเขาถึงทางกายภาพโดยไม่ได้รับอนุญาตอันก่อให้เกิดความเสียหาย การถูก ขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพยสินของโรงพยาบาล

2. มาตรการและแนวทางปฏิบัติ

2.1. บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1.1. คณะกรรมการสารสนเทศต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการ รักษาความปลอดภัย และอนุญาตให้ผ่านเขา-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

2.1.2. คณะกรรมการสารสนเทศต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม ปลวก หรือภัยพิบัติอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

2.2. ความมั่นคงปลอดภัยของอุปกรณ์รวมถึงแฟ้มเวชระเบียน

2.2.1. เจ้าหน้าที่ต้องจัดวางและป้องกันอุปกรณ์ภายในหน่วยงานเพื่อลดความเสี่ยงจากภัยคุกคาม ทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเขาถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2.2.2. ต้องกำหนดให้การเดินสายไฟฟา สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้น เสียหาย

3. วิธีปฏิบัติ

3.1 วิธีปฏิบัติเรื่อง การใช้งานห้อง Server

**การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือขายสารสนเทศ ของโรงพยาบาล**

1. วัตถุประสงค์ เพื่อกำหนดเป็นมาตรการดำเนินงานที่เกี่ยวของกับอุปกรณ์ประมวลผลสารสนเทศและซอฟต์แวร์ให้เป็นไปอย่างถูกต้องสมบูรณ์ ปลอดภัยจากการถูกทำลายและมีความพร้อมใช้ของสารสนเทศ

2. มาตรการและแนวทางปฏิบัติ

2.1. การป้องกันโปรแกรมที่ไม่ประสงค์ดี

2.1.1. ผู้ดูแลระบบต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืน เพื่อป้อง กันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี

2.1.2. ผู้ดูแลระบบต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่และต้องป้องกันไม่ให้ โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

2.2. การสำรองข้อมูล คณะกรรมการสารสนเทศต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่าง สม่ำเสมอ

2.3. การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายของโรงพยาบาล คณะกรรมการ สารสนเทศต้องกำหนดการบริหารจัดการสำหรับบริการเครือข่ายและสารสนเทศของโรงพยาบาล

3. วิธีปฏิบัติ

3.1 วิธีปฏิบัติเรื่อง การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

3.2 วิธีปฏิบัติเรื่อง การจัดการไวรัสคอมพิวเตอร์

3.3 วิธีปฏิบัติเรื่อง การสำรองข้อมูล

3.4 วิธีปฏิบัติเรื่อง การสำรองข้อมูลเวชระเบียนที่จัดเก็บในรูปแบบ Electronic Files

3.5 วิธีปฏิบัติเรื่อง การใช้งานคอมพิวเตอร์และเครือข่าย

**การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ (Access control)**

1. วัตถุประสงค์ เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาต เขาถึงระบบเทคโนโลยีสารสนเทศและป้องกัน การบุกรุก ผ่านระบบเครือข่ายจากผู้บุกรุกที่จะสร้างความเสียหายแก่ข้อมูล

2. มาตรการและแนวทางปฏิบัติ

2.1. การบริหารจัดการการเข้าถึงของผู้ใช้

2.1.1. ผู้ดูแลระบบต้องจัดให้มีการควบคุมและจำกัดสิทธิ์การใช้งานระบบตามความจำเป็นในการใช้งาน

2.1.2. ผู้ดูแลระบบต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอยางมีความมั่นคงปลอดภัย

2.2. หน้าที่ความรับผิดชอบของผู้ใช้ เจ้าหน้าที่ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเขาถึงอุปกรณ์สารสนเทศที่ไม่มีเจ้าหน้าที่ดูแล

2.3. การควบคุมการเข้าถึงระบบปฏิบัติการ

2.3.1. ผู้ดูแลระบบต้องจัดให้ผู้ใช้มีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และ จะต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

2.3.2. ผู้ดูแลระบบต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผานที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

2.3.3. ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลา หนึ่งตามที่กำหนดไว้

2.3.4. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

2.4. การควบคุมการเข้าถึงแอปพลิเคชั่นและสารสนเทศ ผู้ดูแลระบบต้องจำกัดการเขาถึงสารสนเทศและฟังก์ชั่นต่างๆของแอปพลิเคชั่นตามนโยบายควบคุมการเขาถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

3. วิธีปฏิบัติ

3.1 วิธีปฏิบัติเรื่อง การจัดเก็บข้อมูลตาม พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐

3.2 วิธีปฏิบัติเรื่อง การตั้งรหัสผ่าน กำหนดและป้องกันรหัสผ่าน

3.3 วิธีปฏิบัติเรื่อง การรักษาความปลอดภัย/ป้องกันการสูญหายของแฟ้มเวชระเบียนที่จัดเก็บในรูปแบบ Electronic File และป้องกันการโจรกรรมข้อมูล