นโยบายการรักษาความมั่นคงปลอดภัย
ของ ระบบเทคโนโลยีสารสนเทศ
โรงพยาบาลฟากท่า พ.ศ. ๒๕๕๘

โดย

ทีมสารสนเทศ (IM)

โรงพยาบาลฟากท่า

สารบัญ

หน้า

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลฟากท่า

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลฟากท่าเป็นไปอย่างมีประสิทธิภาพ มี ความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจาก การใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาล จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดย กำหนดให้มีมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ ให้ครอบคลุมดานการรักษาความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้มีความ มั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ

๑.๒. กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอางอิง ตามมาตรฐาน ISO/IEC ๒๗๐๐๑

๑.๓. นโยบายนี้ต้องเผยแพร่ให้เจาหนาที่ทุกระดับในโรงพยาบาลฟากท่าได้รับทราบและถือปฏิบัติตาม นโยบายนี้อย่างเคร่งครัด

๑.๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ และผู้ดูแลระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕. เพื่อป้องกันมิให้มีผู้กระทำหรือใช้วิธีการใดๆ เขาล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นใน ระบบสารสนเทศโดยมิชอบ

๑.๖. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

๒. องค์ประกอบของนโยบาย

๒.๑. คำนิยาม

๒.๒. โครงสรางทางดานความมั่นคงปลอดภัยสำหรับโรงพยาบาล

๒.๓. การบริหารจัดการทรัพยสินของโรงพยาบาล

๒.๔. ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากร

๒.๕. การสรางความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดลอม

๒.๖. การบริหารจัดการดานการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของโรงพยาบาล

๒.๗. การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแตละส่วนที่ กล่าวข้างตน จะประกอบด้วย วัตถุประสงค รายละเอียดของมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติใน การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

เพื่อที่จะทำใหมีมาตรการในการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศอยูในระดับที่ปลอดภัย นโยบายการเขาใชงานระบบสารสนเทศของโรงพยาบาลนี้จัดเปนมาตรฐานดานความ ปลอดภัยในการใช้งานระบบสารสนเทศซึ่งเจ้าหน้าที่ของโรงพยาบาลฟากท่าจะต้องปฏิบัติตามอย่าง เคร่งครัด

คำนิยาม

คำนิยามที่ใชในนโยบายนี้ ประกอบดวย

- โรงพยาบาล หมายถึง โรงพยาบาลฟากท่า
- การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของโรงพยาบาลฟากท่า
- มาตรการ หมายถึง วิธีการที่ตั้งเปนกฎ ข้อกำหนด ระเบียบ หรือกฎหมายเปนต้น
- วิธีปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ทีต้องนำมาปฏิบัติ เพื่อใหได้มาซึ่ง มาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- แนวทางปฏิบัติ หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้ สามารถบรรลุเป้าหมายได่ง่ายขึ้น
- ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลฟากท่า
- ผูดูแลระบบ หมายถึง เจ้าหนาที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการ ดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเขาถึงโปรแกรมเครือขายคอมพิวเตอร์ เพื่อการจัดการฐานขอมูลของเครือข่ายคอมพิวเตอร์
- เจ้าหนาที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจางประจำ และลูกจ้างชั่วคราว
- สารสนเทศ หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่รูปของตัวเลข ข้อความ หรือภาพ ให้เป็นระบบทีผูใชสามารถเข้าใจได้ง่ายและสามารถ นำไปใช้ประโยชน ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- ระบบคอมพิวเตอร หมายถึง อุปกรณหรือชุดอุปกรณ์ของคอมพิวเตอรที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานใหอุปกรณ์ หรือ ชุดอุปกรณทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของโรงพยาบาลได เชน ระบบแลน (LAN) ระบบอินเตอรเน็ต (Internet)
    - ระบบแลน (LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกสที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าดวยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อ การติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
    - ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกสที่เชื่อมต่อระบบเครือขายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

● ระบบเทคโนโลยีสารสนเทศ หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสรางสารสนเทศที่หน่วยงานสามารถ นำมาใช้ประโยชน์ ในการวางแผน บริหาร การสนับสนุนการใหบริการ การพัฒนาและควบคุมการ ติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมฐานข้อมูล และสารสนเทศ เป็นต้น

● การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ หมายถึง การตรวจสอบการอนุมัติ และการ กำหนดสิทธิในการผ่านเข้าสูระบบเทคโนโลยีสารสนเทศใหแกผู้ใช้

● เครื่องเซิรฟเวอร์ (Server) หมายถึง เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรม คอมพิวเตอร์ ที่ทำหน้าที่ใหบริการอย่างใดอย่างหนึ่งหรือหลายอย่าง แกเครื่องคอมพิวเตอร์หรือ โปรแกรมคอมพิวเตอรที่เปนลูกข่ายในระบบเครือข่าย

● อุปกรณ UPS หมายถึง เครื่องสำรองไฟฟาและปรับแรงดันไฟฟ้าอัตโนมัติในกรณีที่ไฟจากการ ไฟฟ้าเกิดมีปัญหาขึ้นมา เช่นไฟตก ไฟเกิน ไฟดับ หรือไฟกระชาก เป็นต้น โดยที่ UPS จะจ่าย พลังงานออกมาอย่างต่อเนื่องและมีคุณภาพในทุกสถานการณ ตลอดจนเป็นอุปกรณ์ที่ช่วย ปองกันความเสียหายที่สามารถเกิดขึ้นกับอุปกรณ์ไฟฟา และอุปกรณอิเล็กทรอนิคส (โดยเฉพาะ คอมพิวเตอร์และอุปกรณเชื่อมต่อ) รวมถึงมีหนาที่ในการจ่ายพลังงานไฟฟ้าสำรองจากแบตเตอรี่ ให้แก่อุปกรณ์ไฟฟ้าหรือคอมพิวเตอร์เมื่อเกิดปัญหาทางไฟฟ้า

● ซอฟตแวร์ (software) หมายถึง ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานใหคอมพิวเตอร์ทำงาน ซอฟต์แวรจึงหมายถึงลำดับขั้นตอนการทำงานที่เขียนขึ้นดวยคำสั่งของคอมพิวเตอร คำสั่งเหลานี้ เรียงกันเป็นโปรแกรมคอมพิวเตอร์ จากที่ทราบมาแลวว่าคอมพิวเตอร์ทำงานตามคำสั่ง การทำงานพื้นฐานเปนเพียงการกระทำกับข้อมูลที่เป็นตัวเลขฐานสอง ซึ่งใชแทนข่อมูลที่เปนตัวเลข ตัวอักษร รูปภาพ หรือแม่แตเป็นเสียงพูดก็ได่ โปรแกรมคอมพิวเตอร์ที่ใช้สั่งงานคอมพิวเตอรจึงเป็นซอฟตแวร์ เพราะเป็นลำดับขั้นตอนการ ทำงานของคอมพิวเตอร คอมพิวเตอร์เครื่องหนึ่งทำงานแตกต่างกันได้มากมายด้วยซอฟตแวร์ที่ แตกต่างกัน ซอฟต์แวรจึงหมายรวมถึงโปรแกรมคอมพิวเตอร์ทุกประเภทที่ทำให้คอมพิวเตอร์ทำงานได้

● ไวรัสคอมพิวเตอร หมายถึง โปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเขาไปติดอยู่ ในระบบคอมพิวเตอร์ได้และถามีโอกาสก็สามารถแทรกเขาไประบาดในระบบคอมพิวเตอร์อื่น ๆ ซึ่งอาจเกิดจากการนำเอาดิสกที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบ เครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได่เช่นกัน การที่คอมพิวเตอร์ใดติดไวรัส หมายถึงไวรัสได้เข้าไปฝงตัวอยู่ในหน่วยความจำคอมพิวเตอร์ เรียบร้อยแล้ว เนื่องจากไวรัสก็เป็นแค่โปรแกรม ๆ หนึ่งการที่ไวรัสจะเข้าไปอยู่ ในหน่วยความจำ ไดนั้นจะต้องมีการถูกเรียกให้ทำงานได้ นั้นยังขึ้นอยูกับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว

- เวชระเบียน หมายถึง แบบบันทึกข้อมูลประวัติส่วนตัว การเจ็บป่วย และการตรวจรักษาทั้งที่ เป็นเอกสารและข้อมูลอิเล็กทรอนิกสของผู้ป่วยแตละรายที่มาขอรับบริการตรวจรักษา ณ โรงพยาบาลฟากท่า

- ทรัพยสิน หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการ สื่อสาร ของหนวยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

สวนที่ ๑ โครงสร้างทางดานความมั่นคงปลอดภัยสำหรับโรงพยาบาล

(Organization of information security)

๑. วัตถุประสงค เพื่อกำหนดเปนมาตรการควบคุมและปองกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข่องกับระบบ เทคโนโลยีสารสนเทศ ซึ่งเปนทรัพยสินที่มีคา และอาจจำเปนตองรักษาความลับ โดยมาตรการนี้จะมีผลบังคับ ใชกับผูใช ซึ่งมีสวนเกี่ยวข่องกับการใชงานระบบเทคโนโลยีสารสนเทศของหนวยงาน

๒. มาตรการและแนวทางปฏิบัติ

โครงสรางทางดานความมั่นคงปลอดภัยภายในองคกร

๑. ผู้บริหารต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด่านความ มั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคลอง การมอบหมายงานที่เหมาะสมตอบุคลากร และการเล็งเห็นถึงความสำคัญของหนาที่และความรับผิดชอบใน การสรางความมั่นคงปลอดภัยให้กับสารสนเทศ

๒. คณะกรรมการบริหารโรงพยาบาลตองกำหนดใหมีตัวแทนเจาหนาที่จากหนวยงานตางๆ ภายในโรงพยาบาลเพื่อประสานงานหรือรวมมือกันในการสรางความมั่นคงปลอดภัยให้กับสารสนเทศของ องคกร

๓. คณะกรรมการสารสนเทศตองกำหนดหนาที่ความรับผิดชอบของเจาหนาที่ในการ ดำเนินงานทางดานความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลไวอยางชัดเจน

๔. คณะกรรมการสารสนเทศตองกำหนดใหมีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวของกับความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยผูตรวจสอบอิสระตาม รอบระยะเวลาที่กำหนดไว หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากตอโรงพยาบาล

สวนที่ ๒ การบริหารจัดการทรัพยสินของโรงพยาบาล
(Asset management)

๑. วัตถุประสงค์

เพื่อเปนมาตรการในการปองกันทรัพยสินของโรงพยาบาลจากความเสียหายที่อาจเกิดขึ้นไดจากมนุษย หรือภัยพิบัติตางๆ

๒. มาตรการและแนวทางปฏิบัติ

หน้าที่ความรับผิดชอบตอทรัพยสินของโรงพยาบาล

๑. หัวหนางานพัสดุและผูดูแลระบบ ต้องจัดทำและปรับปรุงแกไขบัญชีทรัพยสินที่มี ความสำคัญตอโรงพยาบาลใหถูกต่องอยูเสมอ

๒. หัวหนางานพัสดุและผูดูแลระบบ ตองจัดใหมีการระบุผูเปนเจาของทรัพยสินสารสนเทศ ตามที่กำหนดไวในบัญชีทรัพยสิน

๓. หัวหนางานพัสดุและผูดูแลระบบ จะต่องจัดทำกฎ ระเบียบ หรือหลักเกณฑอยางเปนลายลักษณอักษรสำหรับการใชงานอุปกรณสารสนเทศอยางเหมาะสม เพื่อปองกันความเสียหาย
ตอทรัพยสิน เหลานั้น

สวนที่ ๓ ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากร
(Human resources security)

๑. วัตถุประสงค

เพื่อเปนมาตรการใหเจาหนาที่ไดทราบถึงหนาที่ความรับผิดชอบและบทบาทเมื่อมีการลาออกหรือยายหนวยงาน

๒. มาตรการและแนวทางปฏิบัติ

๒.๑. กลุมงานการจัดการต่องกำหนดหนาที่ความรับผิดชอบสำหรับผูที่ลาออกหรือยายหนวยงาน และ กำหนดให ปฏิบัติตามหนาที่ดังกลาว

๒.๒. ผูดูแลระบบตองทำการถอดถอนสิทธิในการเขาถึงสารสนเทศและทรัพยสินสารสนเทศของผูที่ ลาออกหรือ ยายหนวยงาน

๓. วิธีปฏิบัติ

วิธีปฏิบัติเรื่อง การจัดการการลาออกหรือยายหนวยงานของเจาหนาที่

สวนที่ ๔ การสรางความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดลอม
(Physical and environmental security)

๑. วัตถุประสงค

เพื่อเปนมาตรการในการปองกันการเขาถึงทางกายภาพโดยไมไดรับอนุญาต การกอใหเกิดความ เสียหาย การถูกขโมย หรือการถูกเปดเผยโดยไมไดรับอนุญาตของทรัพยสินของโรงพยาบาล

๒. มาตรการและแนวทางปฏิบัติ

๒.๑. บริเวณที่ตองมีการรักษาความมั่นคงปลอดภัย

๒.๑.๑. คณะกรรมการสารสนเทศต่องจัดใหมีการควบคุมการเขา-ออกในบริเวณหรือพื้นที่ที่ ตองการรักษาความปลอดภัย และอนุญาตใหผานเขา-ออกไดเฉพาะผูที่ไดรับอนุญาตแลวเทานั้น

๒.๑.๒. คณะกรรมการสารสนเทศต่องจัดใหมีการปองกันตอภัยคุกคามตางๆ ไดแก ไฟไหม น้ำทวม ปลวก หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษยและธรรมชาติ

๒.๒. ความมั่นคงปลอดภัยของอุปกรณรวมถึงแฟมเวชระเบียน

๒.๒.๑. เจาหนาที่ต่องจัดวางและปองกันอุปกรณภายในหนวยงานเพื่อลดความเสี่ยงจากภัย คุกคามทางดานสิ่งแวดลอมและอันตรายตางๆ รวมทั้งความเสี่ยงในการเขาถึงอุปกรณโดยไมไดรับอนุญาต

๒.๒.๒. ตองกำหนดใหมีการเดินสายไฟฟา สายสื่อสาร และสายเคเบิลอื่นๆ ไดรับการปองกัน การเข้าถึงโดยไมไดรับอนุญาต การทำใหเกิดอุปสรรคตอสายสัญญาณ หรือการทำใหสายสัญญาณเหลานั้น เสียหาย

๓. วิธีปฏิบัติ

วิธีปฏิบัติเรื่อง การใช้งานหองเครื่อง Server

สวนที่ ๕

การบริหารจัดการดานการสื่อสารและการดำเนินงานของเครือขายสารสนเทศ ของโรงพยาบาล

๑. วัตถุประสงค

เพื่อกำหนดเปนมาตรการดำเนินงานที่เกี่ยวข่องกับอุปกรณประมวลผลสารสนเทศและซอฟตแวรให่ เปนไปอยางถูกต่องสมบูรณ ปลอดภัยจากการถูกทำลาย และมีความพร่อมใชของสารสนเทศ

๒. มาตรการและแนวทางปฏิบัติ

๒.๑. การปองกันโปรแกรมที่ไมประสงคดี

๒.๑.๑. ผูดูแลระบบต่องมีมาตรการสำหรับการตรวจจับ การปองกัน และการกูกลับคืน เพื่อ ปองกันทรัพยสินสารสนเทศจากโปรแกรมที่ไมประสงคดี

๒.๑.๒. ผูดูแลระบบต่องมีมาตรการเพื่อควบคุมการใชงานโปรแกรมชนิดเคลื่อนที่ และต่อง ปองกันไมให่โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใชงานได่

๒.๒. การสำรองข่อมูล คณะกรรมการสารสนเทศต่องจัดใหมีการสำรองและทดสอบขอมูลที่สำรองเก็บไวอยางสม่ำเสมอ

๒.๓. การบริหารจัดการทางด่านความมั่นคงปลอดภัยสำหรับเครือขายของโรงพยาบาล คณะกรรมการสารสนเทศตองกำหนดการบริหารจัดการสำหรับบริการเครือขายและ สารสนเทศของโรงพยาบาล

๓. วิธีปฏิบัติ

๑. วิธีปฏิบัติเรื่อง การบริหารจัดการดานความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒. วิธีปฏิบัติเรื่อง การจัดการไวรัสคอมพิวเตอร

๓. วิธีปฏิบัติเรื่อง การสำรองขอมูล

๔. วิธีปฏิบัติเรื่อง การสำรองขอมูลเวชระเบียนที่จัดเก็บในรูปแบบ Electronic Files

๕. วิธีปฏิบัติเรื่อง การใชงานคอมพิวเตอรและเครือขาย

สวนที่ ๖
การควบคุมการเขาถึงระบบเทคโนโลยีสารสนเทศ (Access control)

๑. วัตถุประสงค

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไมไดรับอนุญาต เขาถึงระบบเทคโนโลยีสารสนเทศและปองกัน การบุกรุกผานระบบเครือขายจากผูบุกรุกที่จะสรางความเสียหายแกขอมูล

๒. มาตรการและแนวทางปฏิบัติ

๒.๑. การบริหารจัดการการเขาถึงของผูใช

๒.๑.๑. ผูดูแลระบบตองจัดใหมีการควบคุมและจำกัดสิทธิการใชงานระบบตามความจำเปน ในการใชงาน

๒.๑.๒. ผูดูแลระบบตองจัดใหมีกระบวนการบริหารจัดการรหัสผานสำหรับผูใชงานอยางเปน ทางการเพื่อควบคุมการจัดสรรรหัสผานใหแกผูใชงานอยางมีความมั่นคงปลอดภัย

๒.๒. หนาที่ความรับผิดชอบของผูใช

เจาหนาที่ตองมีวิธีเพื่อปองกันไมใหผูไมมีสิทธิสามารถเขาถึงอุปกรณสารสนเทศที่ไมมี เจาหนาที่ดูแล

๒.๓. การควบคุมการเขาถึงระบบปฏิบัติการ

๒.๓.๑. ผูดูแลระบบตองจัดใหผูใชมีขอมูลสำหรับระบุตัวตนในการเขาใชงานระบบที่ไม ซ้ำซอนกัน และจะตองจัดใหมีกระบวนการพิสูจนตัวตนกอนเขาใชงานระบบตามขอมูลระบุตัวตนที่ไดรับ

๒.๓.๒. ผูดูแลระบบตองจัดทำหรือจัดใหมีระบบบริหารจัดการรหัสผานที่มีการควบคุมการ กำหนดรหัสผานที่มีคุณภาพ

๒.๓.๓. ผูดูแลระบบตองกำหนดใหระบบตัดการใชงานผูใชเมื่อผูใชไมไดใชงานระบบมาเปน ระยะเวลาหนึ่งตามที่กำหนดไว

๒.๓.๔. ผูดูแลระบบตองจำกัดระยะเวลาในการเชื่อมตอระบบสารสนเทศที่มีความสำคัญสูง

๒.๔. การควบคุมการเขาถึงแอปพลิเคชันและสารสนเทศ

ผูดูแลระบบตองจำกัดการเขาถึงสารสนเทศและฟงกชันตางๆ ของแอปพลิเคชันตามนโยบาย ควบคุมการเขาถึงสารสนเทศที่ไดกำหนดไว การเขาถึงจะตองแยกตามประเภทของผูใชงาน

๓. วิธีปฏิบัติ

๓.๑.๑. วิธีปฏิบัติเรื่อง การจัดเก็บข่อมูลตาม พ.ร.บ.วาดวยการกระทำผิดเกี่ยวกับคอมพิวเตอร ป ๒๕๕๐

๓.๑.๒. วิธีปฏิบัติเรื่อง การตั้งรหัสผาน กำหนดและปองกันรหัสผาน

๓.๑.๓. วิธีปฏิบัติเรื่อง การรักษาความปลอดภัย/ ปองกันการสูญหายของแฟมเวชระเบียนที่จัดเก็บใน รูปแบบ Electronic File และปองกันการโจรกรรมข่อมูล

(ลงชื่อ) พรสวรรค์ มีชิน

(แพทย์หญิงพรสวรรค์ มีชิน)
ผู้อำนวยการโรงพยาบาลฟากท่า
วันที่ ๒๒ พฤษภาคม ๒๕๕๕

เอกสารอางอิง คณะอนุกรรมการดานความมั่นคง ภายใต ศูนยเทคโนโลยีอิเล็กทรอนิกสและคอมพิวเตอรแหงชาติ, ๒๕๕๐.
มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอรชัน ๒.๕) ประจำปี ๒๕๕๐.
หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ.