นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

INFORMATION TECHNOLOGY SECURITY POLICY

โรงพยาบาลบ้านตาขุน อำเภอบ้านตาขุน จังหวัดสุราษฎร์ธานี

ตุลาคม 2564

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับองค์กรที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของหน่วยงานที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ เป็นต้น แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่างๆ ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัย ด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลบ้านตาขุน จึงจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และเพื่อดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

คณะกรรมการบริหารความเสี่ยงทางด้านสานสนเทศ
โรงพยาบาลบ้านตาขุน
ตุลาคม 2564

สารบัญ

นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1. บทนำ

โรงพยาบาลบ้านตาขุนได้ตระหนักถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายและแนวปฏิบัติในการรักษามั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ขึ้น เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีการควบคุมภายในที่ดี มีความมั่นคงปลอดภัย ถูกต้อง เชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง และ สามารถป้องกันรักษาสารสนเทศที่เป็นความลับของโรงพยาบาล ทั้งที่เป็นข้อมูลของโรงพยาบาล ข้อมูลผู้ป่วย และข้อมูลบุคคลากร ซึ่งนโยบายและแนวปฏิบัตินี้ จะเป็นกรอบแนวทางปฏิบัติของเจ้าหน้าที่ทุกคนในองค์กร ให้มีความเข้าใจ งานแต่ละระดับและร่วมมือ ในการใช้และเก็บรักษาข้อมูล, ระบบ และเครื่องใช้เทคโนโลยีสารสนเทศฯ อย่างมี ประสิทธิภาพให้ถูกต้องตามกฎหมาย อีกทั้งปกป้องให้มีความปลอดภัย

2. วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของโรงพยาบาลทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล และวัตถุประสงค์ที่กำหนดไว้

2.2 เพื่อกำหนดแนวปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

2.3 เพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของโรงพยาบาล ถูกบุกรุก เปลี่ยนแปลง ถูกขโมย ทำลาย หรือการกระทำอื่นๆ ที่อาจสร้างความเสียหายต่อโรงพยาบาล

2.4 เพื่อป้องกันพนักงานและบุคคลที่เกี่ยวข้อง ไม่ให้กระทำความผิดตามพะราชบัญญัติว่าด้วยการ กระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560

2.5 เพื่อเผยแพร่ให้ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลท ซึ่งโรงพยาบาลหรือหน่วยงานในโรงพยาบาลอนุญาตให้มีสิทธิ์ในการเข้าถึงข้อมูล หรือระบบสารสนเทศ ได้รับทราบและถือปฏิบัติอย่างเคร่งครัด

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านตาขุนเป็นไป ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2550 และ พ.ศ.2560 ได้กำหนดนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกอบด้วยนโยบาย หลัก 3 ด้าน และแนวทางปฏิบัติ ภายในกรอบนโยบายหลัก ดังต่อไปนี้

1. นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ
2. นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน
3. นโยบายการตรวจสอบและประเมินความเสี่ยง

1. ด้านการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ เป็นนโยบายในการกำหนดการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และ ทางกายภาพ รวมทั้งการอนุญาต เช่นว่านั้น สำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมิชอบเอาไว้ด้วยก็ได้

2. ด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน เป็นนโยบายในการธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้ง คุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability) รวมถึงกรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่ แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย

3. ด้านการตรวจสอบและประเมินความเสี่ยง เป็นนโยบายในการตรวจสอบและประเมินความเสี่ยง เพื่อกำกับดูแลการบริหารระบบสารสนเทศให้เกิดประสิทธิภาพและประสิทธิผล ตลอดจนการกำหนดแนวทางการแก้ไขปัญหา และอุปสรรคต่างๆ ที่เกิดขึ้น อย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

3. นิยามศัพท์

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารโรงพยาบาลบ้านตาขุน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านตาขุน ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนด นโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศศูนย์สารสนเทศ หมายถึง ศูนย์สารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุงบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลบ้านตาขุน

ผู้อำนวยการศูนย์สารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านตาขุน และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในโรงพยาบาลบ้านตาขุน

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านตาขุน

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งโรงพยาบาลบ้านตาขุน กำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลบ้านตาขุน

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมา และเจ้าหน้าที่ต่างๆ ของโรงพยาบาลบ้านตาขุน หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลบ้านตาขุน อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงานโดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร การ

พัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)

พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตรี และความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

4. หน้าที่ความรับผิดชอบ

4.1 หน้าที่ของคณะกรรมการบริหาร

4.1.1 กำหนดกลยุทธ์และภาพรวม ควบคุมการปฏิบัติงานในโรงพยาบาล และอนุมัตินโยบายในการรักษา ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

4.2 หน้าที่ของคณะอนุกรรมการบริหารความเสี่ยง

4.2.1 กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลโดยกำหนดให้ ไปในทิศทางเดียวกันกับแผนและเป้าหมายของโรงพยาบาล

4.2.2 จัดการพัฒนานโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย Policy, Standard, Procedure และ Guideline เพื่อให้โรงพยาบาลได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)

4.2.3 นำเสนอผู้บริหารระดับสูง เรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.2.4 จัดให้มีการประเมิน และการบริหารความเสี่ยง ด้านสารสนเทศของโรงพยาบาล รายงานต่อ คณะกรรมการบริหาร และคณะกรรมการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการโรงพยาบาลเป็น ประจำทุกไตรมาส

4.2.5 เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

4.3 หน้าที่ของผู้อำนวยการ และหน่วยงานสารสนเทศ

4.3.1 ร่างนโยบาย แนวปฏิบัติ และระเบียบในการดำเนินการด้านนโยบายในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.3.2 ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งการจัดหา และพัฒนา ระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบโรงพยาบาล

4.3.3 ดูแลทรัพยากรด้านสารสนเทศของโรงพยาบาล ให้สามารถสนับสนุนการปฏิบัติงานภายใน อย่างมีประสิทธิภาพ

4.4 หน้าที่ของผู้ใช้งาน

4.4.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลโดยเคร่งครัด

4.4.2 ให้ความร่วมมือกับโรงพยาบาลอย่างเต็มที่ ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศ ของโรงพยาบาล สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของโรงพยาบาลให้มีความปลอดภัย

4.4.3 รายงานต่อผู้อำนวยการโรงพยาบาลทันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึง ระบบสารสนเทศที่อาจสร้างความเสียหายต่อ โรงพยาบาล

4.5 หน้าที่ของหัวหน้าหน่วยงานสารสนเทศ

4.5.1 ชี้แจงและส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัย กรณีที่พบเห็นการปฏิบัติที่ ไม่ถูกต้องเหมาะสม

4.6 หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

4.6.1 จัดให้มีการทำเอกสาร มาตรการและขั้นตอนการควบคุมการเข้าถึงข้อมูล ให้เป็นไปตาม นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล

4.6.2 ดูแลให้เจ้าหน้าที่ทุกคนปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศของโรงพยาบาล

4.6.3 ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และ ความรับผิดชอบ

4.6.4 รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

4.6.5 แจ้งงานสารสนเทศเพื่อลบ/ เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงเจ้าหน้าที่/ อำนาจหน้าที่ /โอนย้าย

4.7 หน้าที่ของทีมตรวจสอบภายใน (Internal Audit)

4.7.1 ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้อง กับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามความจำเป็น

5. นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

1. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

1.1 ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่ผู้ใช้งานได้รับอนุญาตหรือได้รับการ มอบอำนาจ ตามที่กำหนดใน “การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของ เจ้าหน้าที่”

1.2 ผู้ดูแลระบบมีการกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้ อ่านข้อมูล , สร้างข้อมูล,นำเข้า ข้อมูล แก้ไขข้อมูล, อนุมัติ และ ไม่มีสิทธิ

1.3 ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับ ชั้นความลับ

1.4 ผู้ดูแลระบบมีการถอดสิทธิการเข้าถึงเข้าถึงการใช้งานสารสนเทศ ตามที่กำหนดใน “การบริหารจัดการ สิทธิ์การใช้งานระบบและรหัสผ่าน”

1.5 ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

1.6 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จะต้องได้รับการพิจารณาจากหน่วยงานต้นสังกัด

1.7 ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ ข้อมูลภายในเป็นไป ตามลำดับขั้นความลับของข้อมูล

1.8 ผู้ดูแลระบบกำหนดลำดับชั้นความลับของข้อมูล ได้แก่ ลับที่สุด ลับมาก ลับ และทั่วไป

1.9 ผู้ดูแลระบบกำหนดระดับชั้นการเข้าถึง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ เจ้าของระบบ และผู้ใช้ระบบ

1.10 ผู้ดูแลระบบกำหนดเวลาและช่องทางที่เข้าถึงได้ ให้เหมาะสมตามแต่ละระบบงาน

2. การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

2.1 ผู้ใช้งานจะต้องได้รับอนุญาตจากหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบข้อมูลและ ระบบงานเพื่อเข้าใช้งานระบบสารสนเทศ ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

2.2 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบเฉพาะใน ส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ

2.3 เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่ จำเป็นต้องรู้ ตามหน้าที่งานหรือตามความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิ์เกินความจำเป็นในการ ใช้งาน โดยต้องมีการอนุญาตจากเจ้าของข้อมูลและหรือเจ้าของระบบงาน

3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.1 การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มี สิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้ง ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงาน ภายใน 15 วันทำการ นับจากวันที่ผู้มีอำนาจลงนามในคำสั่ง

3.2 ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศโปรแกรม ประยุกต์ (Application) ภายในโรงพยาบาล จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Ares Network*: W*AN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบ จากหน่วยงานต้นสังกัด รวมทั้ง ต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

4. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยี สารสนเทศและการสื่อสารแต่ละระบบ รวมทั้ง กำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

4.2 การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหาร จัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.3 กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิ์เพิ่มเป็นกรณีพิเศษแก่ผู้ใช้งานที่มีสิทธิ์พื้นฐาน ต้อง ได้รับความ เห็นชอบและอนุมัติจากหัวหน้าหน่วยงานต้นสังกัด และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิ พิเศษนั้น อย่างรัดกุมเพียงพอ โดยต้องดำเนินการอย่างน้อย ดังนี้

4.3.1 ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

4.3.2 กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.3.3 กรณีมีการใช้งานไม่ต่อเนื่อง ให้มีการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเสร็จสิ้นการใช้งาน ในแต่ละครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้มีการ

เปลี่ยนรหัสผ่าน ทุก 3 เดือน

4.4 กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (user registration) ดังนี้

4.4.1 มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล

4.4.2 การกำหนดชื่อผู้ใช้ กำหนดจากชื่อภาษาอังกฤษไม่ต่ำกว่า 4 อักขระ

4.4.3 มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจาก หัวหน้าหน่วยงานต้นสังกัด

4.4.4 มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ การตัดออกจาก ทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

5. วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการ ทำลายข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ

5.2 เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อย ปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

5.3 ผู้ดูแลระบบควบคุม การเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงข้อมูลโดยตรงและการเข้าถึง ผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ใน การตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN

5.5 มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่ กำหนดของระดับความสำคัญของข้อมูลตามที่ ระบุไว้ใน เอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน การกำหนดชั้นความลับข้อมูล

1. ชั้นที่ 1 ข้อมูลเปิดเผยได้

- ข้อมูลที่บุคคลทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น เป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงาน ของโรงพยาบาล สามารถนำเสนอต่อบุคคลทั่วไป สาธารณชน หรือเป็นข้อมูลที่กฎหมาย ระบุว่าต้องเปิดเผย

- การเปิดเผยข้อมูลทั้งหมดหรือบางส่วน จะไม่เกิดผลเสียหายต่อโรงพยาบาล เช่น ข้อมูลที่เผยแพร่บนเว็บไซต์ ของโรงพยาบาล เป็นต้น

2. ชั้นที่ 2 ข้อมูลใช้ภายในโรงพยาบาล

- ข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้ผู้ใช้งานภายในโรงพยาบาลรับทราบได้ แต่ไม่สมควร เปิดเผยต่อบุคคลภายนอก เพราะอาจจะสร้างความเสียหายให้กับโรงพยาบาลได้

- การเปิดเผยข้อมูล เจ้าของข้อมูลต้องใช้ดุลยพินิจในการอนุญาตหรือได้รับความเห็นชอบจากผู้บริหาร คณะทำงาน หรือหน่วยงาน

3. ชั้นที่ 3 ข้อมูลลับ

- ข้อมูลที่โรงพยาบาลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้ผู้ใช้งานทุกคนทราบได้ กำหนดให้เฉพาะผู้ที่ เกี่ยวข้อง และจำเป็นต้องใช้ในการปฏิบัติงานทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน ข้อมูลมีความสำคัญต่อการดำเนินการของโรงพยาบาล เป็นข้อมูลภายใน และไม่สามารถเปิดเผยต่อบุคคลภายนอกที่ไม่เกี่ยวข้องตามกฎหมายได้ เนื่องจากข้อมูลนี้จะสร้าง ความเสียหายให้กับโรงพยาบาลได้

- การเปิดเผยข้อมูลจะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงาน หรือกรรมการผู้จัดการ หรือคณะกรรมการ

4. ชั้นที่ 4 ข้อมูลลับมาก

- ข้อมูลที่ใช้ภายในโรงพยาบาล แต่เป็นข้อมูลลับ ใช้งานโดยผู้ใช้งานบางกลุ่มของโรงพยาบาลซึ่งมีรหัสพิเศษในการ เข้าใช้งาน และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของโรงพยาบาลจะทำให้เกิดผลเสียหายร้ายแรงต่อโรงพยาบาล

- การเปิดเผยข้อมูล จะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือคณะทำงาน หรือกรรมการผู้จัดการ หรือคณะกรรมการ

5. ชั้นที่ 5 ข้อมูลลับที่สุด

- ข้อมูลที่ใช้ภายในโรงพยาบาลแต่เป็นข้อมูลลับ ใช้งานโดยคณะกรรมการของโรงพยาบาลเท่านั้น ซึ่งมีรหัสพิเศษ ในการเข้าใช้งาน และเป็นการใช้เพื่อการวินิจฉัย และตัดสินใจที่สำคัญของโรงพยาบาล ไม่สามารถเปิดเผยต่อ บุคคลภายนอกได้ เนื่องจากข้อมูลมีความจำเป็นต่อการปฏิบัติงานของโรงพยาบาล ทำให้เกิดผลเสียหายร้ายแรง ต่อโรงพยาบาล

- การเปิดเผยข้อมูล ไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย

6. การควบคุมการเข้าใช้งานระบบจากภายนอก

6.1 ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับโรงพยาบาลอย่างเพียงพอ เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากโรงพยาบาล

6.2 งานสารสนเทศเป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)

6.3 ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากงานสารสนเทศ และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและ ข้อมูลอย่างเคร่งครัด

6.4 ผู้ดูแลระบบต้องควบคุมพอร์ต (Port) ที่ระบบสารสนเทศเทศให้บริการ ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับ การอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

6.5 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็น เท่านั้น และให้ปิด Port และ Modem เมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

7. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

ผู้ใช้งานระบบทุกคน เมื่อจะเข้าใช้งานระบบของโรงพยาบาล ต้องผ่านการพิสูจน์ตัวตนจากระบบของโรงพยาบาล โดยมี แนวทางปฏิบัติดังนี้

7.1 การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

7.2 การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

7.3 การเข้าสู่ระบบสารสนเทศของโรงพยาบาลจากอินเทอร์เน็ตนั้น จะต้องมีการตรวจสอบผู้ใช้งาน

7.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบ เพื่อ พิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัส

6. การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

การบริหารรหัสผ่าน/การใช้งานรหัสผ่าน

1. งานสารสนเทศต้องกำหนด ชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำกัน และ กำหนดชื่อผู้ใช้ ในส่วนของ ชื่อผู้ใช้ของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่นๆ ให้มีความแตกต่างกัน

2. การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นความลับ พร้อมแจ้งช่องทางการเข้าถึง “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” เพื่อสร้างความรู้ความเข้าใจ และให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

3. งานสารสนเทศกับหน่วยงานต่างๆ ของโรงพยาบาลจะทบทวนสิทธิการเข้าถึงระบบสารสนเทศของ ผู้ใช้งานอย่างน้อย ปีละ 1 ครั้ง

4. ผู้ใช้งานต้องเก็บรักษารหัสผ่าน (Password) ของตนเองและของกลุ่มไว้เป็นความลับ

5. ห้ามทำการบันทึกรหัสผ่าน (Password) ไว้ในไปรษณีย์อิเล็กทรอนิกส์ หรือแบบฟอร์มอิเล็กทรอนิกส์ต่าง ๆ

6. ไม่จดหรือบันทึกรหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

7. ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันที หลังจากได้รับมอบรหัสผ่านเริ่มต้นจากผู้ดูแล ระบบของศูนย์เทคโนโลยีสารสนเทศ

8. กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยควรมีการผสมกันระหว่าง ตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วน บุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้พจนานุกรม

9. ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่าย คอมพิวเตอร์

10. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่อง คอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

11. ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่าน ทันที หรือแจ้งให้งานสารสนเทศทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

12. หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคล นั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง

13. กรณีผู้ใช้งานของหน่วยงานภายในโรงพยาบาลลาออก ให้งานสารสนเทศที่ทำการยกเลิกสิทธิของผู้ที่ลาออก ออกจาก ระบบทันที

14. กรณีผู้ใช้งานของหน่วยงานภายในโรงพยาบาล มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การ ใช้งาน ให้หน่วยงานต้นสังกัด แจ้งงานสารสนเทศเพื่อทำการเปลี่ยนแปลงสิทธิ์ในการใช้งาน

15. ผู้ใช้งานทุกคนของโรงพยาบาล มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ ยินยอมให้บุคคล อื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ขอตน

7. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

แนวปฏิบัติ

1. การบริหารจัดการทางกายภาพ (Physical security management)

1.1 กำหนดระดับความสำคัญของพื้นที่ในศูนย์เทคโนโลยีสารสนเทศ

1.2 มีระบบป้องกัน ให้ครอบคลุมพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในหรือบริเวณที่มีความสำคัญ

1.3 ผู้ดูแลระบบ ต้องปิดประตูและ หน้าต่างห้องแม่ข่ายให้ล็อคอยู่เสมอ

2. การควบคุมการเข้า-ออก (Physical entry Controls)

2.1 ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

2.2 ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการ สูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

2.3 มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และควรมีเหตุผลที่ เพียงพอในการเข้าถึงบริเวณดังกล่าว

2.4 สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติ ระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

2.5 มีการควบคุมการเข้าถึงพื้นที่ ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

2.6 มีการพิสูจน์ตัวตน โดยการอ่านบัตรหรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

2.7 จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบในภายหลัง เมื่อมีความจำเป็น

2.8 โรงพยาบาลผู้ได้รับการว่าจ้าง ต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

2.9 ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศ

2.10 จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

3. การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

3.1 จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานให้น้อยที่สุด

3.2 อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่มีความมั่นคงปลอดภัย

3.3 ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน

3.4 ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณ

4. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

4.1 มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่เพียงพอ ต่อความต้องการใช้งาน โดยให้มีระบบสำรองกระแสไฟฟ้า (UPS) และระบบปรับอากาศ

4.2 ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนตาม 4.1 อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

5. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling security)

5.1 ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

5.2 จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

5.3 ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

6. การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

6.1 กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ 1 ครั้ง

6.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

6.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือ ประเมินในภายหลัง

6.4 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ ดังกล่าว

6.5 ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในโรงพยาบาล

6.6 ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดย ไม่ได้รับอนุญาต

6.7 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7. การนำสินทรัพย์ของโรงพยาบาล ออกไปภายนอกสถานที่ (Removal of property)

7.1 ผู้ใช้งานต้องขออนุญาตหัวหน้าหน่วยงานต้นสังกัดก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกโรงพยาบาล

7.2 ผู้ใช้งานต้องบันทึกข้อมูลการนำอุปกรณ์ของโรงพยาบาล ออกไปภายนอกสถานที่ เพื่อเก็บไว้เป็นหลักฐาน ป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนาอุปกรณ์ส่งคืน

8. การป้องกันสินทรัพย์ที่ใช้งานภายนอกโรงพยาบาล (Security of equipment off-premises)

8.1 กำหนดมาตรการความปลอดภัยของสินทรัพย์ เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของโรงพยาบาล ออกไปใช้งานภายนอก

8.2 ไม่ทิ้งสินทรัพย์ของโรงพยาบาลไว้ในที่สาธารณะโดยไม่มีผู้ดูแลรับผิดชอบ

8.3 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบดูแลสินทรัพย์ของโรงพยาบาล เสมือนเป็นสินทรัพย์ของตนเอง

9. การกำจัดสินทรัพย์หรือการนำสินทรัพย์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

9.1 ให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าว

9.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บ ข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

8. นโยบายการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

แนวปฏิบัติ

1. ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

1.1 มีการจัดทำคู่มือการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดอย่างน้อย ดังนี้

- การปฏิบัติงานในห้องแม่ข่าย
- การเปิดและปิดระบบงาน ได้แก่ การเปิด - ปิดเครื่องแม่ข่าย การเปิด - ปิดระบบงาน การเปิด - ปิดระบบให้บริการ
- การสำรองข้อมูล
- การบำรุงรักษาอุปกรณ์

- การจัดการกับสื่อบันทึกข้อมูล ได้แก่ การทำป้ายชื่อบ่งชี้ การลบ การป้องกันการนำสื่อบันทึกข้อมูล กลับมาใช้งานอีกครั้ง

- การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น

- การประมวลผลข้อมูล ได้แก่ ขั้นตอนในการนำข้อมูลเข้าระบบงานประมวลผล และ แสดงผล

- การใช้งานโปรแกรมยูทิลิตี้

- การรายงานและการจัดการกับปัญหาที่เกิดขึ้น

- การจัดการกับการทำงานล้มเหลวของระบบคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย

- การกู้คืนระบบงานและระบบเครือข่าย

1.2 มีการแจกจ่ายและควบคุมดูแลให้มีการปฏิบัติงานตามแนวทางที่กำหนดในคู่มือการปฏิบัติงาน

1.3 มีการทบทวนปรับปรุงคู่มือการปฏิบัติงานให้เหมาะสมอยู่เสมอ

2. ควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ (Change management) ต้องมีการกำหนดผู้รับผิดชอบและผู้มีอำนาจในการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยี สารสนเทศของโรงพยาบาล

3. การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

3.1 มีการกำหนดแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานของแต่ละบุคคลไว้อย่างชัดเจนโดยมิให้มีการกำหนดหน้าที่ที่สำคัญไว้ที่บุคคลเพียงคนเดียว

3.2 ให้ผู้บังคับบัญชามีการควบคุมดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

3.3 ให้มีการจัดเก็บหลักฐานการปฏิบัติงานที่สามารถใช้ตรวจสอบได้ในภายหลัง

4. การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

4.1 ให้กำหนดมาตรการแยกเครื่อง คอมพิวเตอร์ของระบบงานสำหรับการพัฒนา การทดสอบ และ การ ให้บริการออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงาน

4.2 กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนา ไปสู่เครื่องที่ใช้สำหรับการให้บริการ

4.3 กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกันสำหรับระบบงานที่ใช้ในการพัฒนาทดสอบ และใช้ ระบบงานจริง

9. การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

แนวปฏิบัติ

1. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่โรงพยาบาลไม่อนุญาตให้ใช้งาน

2. ให้ติดตั้งซอฟต์แวร์ เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

3. ให้ผู้ดูแลระบบดำเนินการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องเซิร์ฟเวอร์ให้บริการและอุปกรณ์ เทคโนโลยีสารสนเทศอื่นๆ ณ จุดทางเข้า-ออกเครือข่ายอย่างสม่ำเสมอ เพื่อดักจับโปรแกรม ไม่ประสงค์ดีที่ เข้าสู่ระบบ

4. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหาย ที่พบ เป็นต้น

5. มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

6. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและ สามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติ เมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่า ต้องดำเนินการ อย่างไร

7. เครื่องคอมพิวเตอร์ทั้งหมด ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แบบตั้ง โต๊ะ และ เครื่องคอมพิวเตอร์แบบพกพา (Note book) ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสรุ่นล่าสุดของโรงพยาบาลจากงานสารสนเทศ และจะต้องเปิดใช้งานโปรแกรมตรวจสอบและกำจัดไวรัสตลอดเวลา

8. เครื่องคอมพิวเตอร์ Server ที่ให้บริการการตรวจสอบและกำจัดไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุดของ ไวรัสอยู่เสมอ และต้องเป็นผู้ให้บริการปรับปรุงข้อมูลไวรัสล่าสุดให้แก่ เครื่องคอมพิวเตอร์ Server เครื่อง คอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพาทุกเครื่องโดยอัตโนมัติ

9. ต้องทำการตรวจสอบไวรัสกับแฟ้มข้อมูล (file) ต่างๆ ที่ download มาแฟ้มข้อมูลที่แนบมากับไปรษณีย์ อิเล็กทรอนิกส์, แฟ้มข้อมูลที่ได้มาจากสื่อบันทึกข้อมูลภายนอก (CD, Thumb Drive, Diskette or share file)

10. การเข้าถึงระบบโปรแกรมประยุกต์และสารสนเทศ (Information handling procedures)

แนวปฏิบัติ

1. การจัดการสารสนเทศ

1.1 มีการกำหนดข้อมูลตามระดับชั้นความลับ ได้แก่ ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายใน ข้อมูลลับ

1.2 มีขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ควรประกอบด้วย

วิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ ระยะเวลาที่สามารถเข้าถึง และช่องทางการเข้าถึง

1.3 มีการจำกัดการเข้าถึงข้อมูลตามระดับชั้นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1.4 มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะ นำไปใช้งานต่อไป

1.5 มีการจัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชี รายชื่อ อย่างสม่ำเสมอ

1.6 การเข้าถึงต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

1.7 ระบบไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการ ดังนี้

(1) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบและ ระดับความสำคัญต่อหน่วยงาน

(2) มีการควบคุมสภาพแวดล้อม ได้แก่ มีห้องแม่ข่ายเฉพาะมีระบบไฟสำหรับระบบเฉพาะมี ระบบป้องกันผู้มีสิทธิเข้าออกห้องแม่ข่าย

(3) มีการควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และต้องกำหนดมาตรการป้องกัน ความเสี่ยง ที่มีต่ออุปกรณ์

1.8 การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) จะต้องดำเนินการ ดังนี้

(1) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการ เข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มี ความมั่นคงปลอดภัย

(2) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

(3) ผู้ดูแลระบบมีการรักษาความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในโรงพยาบาลก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

(4) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคล อื่นๆ ใด เข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

(5) การขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

2. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

2.1 กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่

กำหนดให้ใช้งาน ได้ 2 ช.ม. ต่อ การเชื่อมต่อหนึ่งครั้ง

2.2 กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานใน สถานที่ที่มีความเสี่ยง มีการจำกัดช่วงระยะเวลาการ เชื่อมต่อ

3. การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access Control)

3.1 กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย

(1) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ ระบบจะเสร็จสมบูรณ์

(2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

(3) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความ เสียหายให้กับระบบได้

3.2 ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมี ข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตน ที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(1) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบ สารสนเทศของหน่วยงาน

(2) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม

3.3 กำหนดหลักเกณฑ์ยุติการเชื่อมต่อ เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาที เป็นอย่างน้อย หากเป็น ระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

3.4 กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อ เพื่อให้ผู้ใช้สามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 4 ชม. ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้ เฉพาะช่วงเวลาเท่านั้น

4. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging) จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศ ที่แสดงให้ทราบว่าใครทำอะไร ที่ไหน เมื่อไร และอย่างไร

11. การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

แนวปฏิบัติ

1. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

1.1 กำหนดให้มีรหัสผู้ใช้ รหัสผ่าน (Username/Password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและ ระบบปฏิบัติการ

1.2 กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบต้องทำการ Lock ไม่ให้ ใช้งาน เป็นระยะเวลาหนึ่ง

1.3 ผู้ดูแลระบบควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์ การใช้งานระบบและรหัสผ่าน

1.4 ผู้ดูแลระบบควรตั้งระบบการล็อคหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

1.5 ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

2. การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of operational software)

2.1 มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของโรงพยาบาล เพื่อป้องกันความเสียหายหรือการ หยุดชะงักที่มี ต่อระบบงานนั้น

2.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการ เปลี่ยนแปลง ต่อระบบงานของโรงพยาบาล

2.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงาน ต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

2.4 กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่าง ครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

2.5 ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการ ติดตั้งบนเครื่องให้บริการระบบงาน

3. ให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

3.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคล เหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลง ระบบปฏิบัติการ

3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณ ที่จำเป็นต้องใช้ในกรณีที่โรงพยาบาลต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

4. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

4.1 จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

4.2 ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมี การพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

4.3 ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้ง

ก่อนดำเนินการ ติดตั้ง

5. การเฝ้าดูและตรวจสอบ

5.1 ต้องดำเนินการเก็บ Log และ Audit Trails ของเหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

5.1.1 Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็น เวลา 90 วัน

5.1.2 ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า 90 วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้ เมื่อเจ้าหน้าที่ต้องการต้องสามารถนำออกมามอบให้กับเจ้าหน้าที่ได้

5.2 ผู้ดูแลระบบ ต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับ ผู้บังคับบัญชาทราบ ดังนี้

5.2.1 การโจมตีในรูปแบบ Port-Scan

5.2.2 การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิในการใช้งานระบบนั้น

5.2.3 เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์ Server ที่เกิดขึ้น

5.3 ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

5.4 ต้องมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอ ผู้บังคับบัญชา

12. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

แนวทางปฏิบัติ

1. การปฏิบัติทั่วไป

1.1 เครื่องคอมพิวเตอร์ที่โรงพยาบาลอนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของโรงพยาบาล ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของโรงพยาบาล

1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของโรงพยาบาล ต้องเป็นโปรแกรมที่โรงพยาบาลได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

1.3 ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ ของโรงพยาบาล และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.4 ไม่อนุญาตให้ ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมยูทิลิตี้ ในเครื่องคอมพิวเตอร์ส่วนบุคคลของโรงพยาบาล เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากงานสารสนเทศ

1.5 การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องได้รับการพิจารณาจากงานสารสนเทศ

1.6 ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

1.7 ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

1.8 ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ 15 นาทีเพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

1.9 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของโรงพยาบาล ยกเว้นจะให้รับการพิจารณาอนุมัติจากงานสารสนเทศ ก่อนการใช้งาน

1. 10 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคลต้องมีการ Update service pack และ hot fix ที่เป็นversion ล่าสุดเสมอ โดยเจ้าหน้าที่งานสารสนเทศ

1.11 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่งานสารสนเทศเท่านั้น

1.12 การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายในโรงพยาบาล จะต้องแจ้งงานสารสนเทศดำเนินการให้เท่านั้น

1.13 กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้งานสารสนเทศเป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของโรงพยาบาล

1.14 ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของโรงพยาบาลทุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากเจ้าหน้าที่งานสารสนเทศ

1.15 เครื่องคอมพิวเตอร์ทุกเครื่องต้องไห้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของโรงพยาบาลจากเจ้าหน้าที่งานสารสนเทศ

1.16 ผู้ใช้งานไม่ควรสร้าง short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของโรงพยาบาล

1.17 ผู้ใช้งานมีหน้าที่และความรับผิดรอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้อง

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ disk drive

1.18 ห้ามเจ้าหน้าที่ทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลของโรงพยาบาลทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้งานสารสนเทศทราบทันที

1.19 ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่อง

คอมพิวเตอร์(ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

2. แนวทางปฏิบัติในการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และ รหัสผ่าน

2.1 ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

2.2 ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตาม "การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน"

2.3 ผู้ใช้งาน ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

3.1 ผู้ใช้งาน ควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

3.2 ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

3.3 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

4. การสำรองข้อมูลและการกู้คืน

4.1 ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่อง มีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลภายนอก

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

13. การใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

แนวปฏิบัติ

1. การใช้งานทั่วไป

1.1 เครื่องคอมพิวเตอร์โรงพยาบาล อนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของโรงพยาบาล ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของโรงพยาบาล

1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์โรงพยาบาล ต้องเป็นโปรแกรมที่โรงพยาบาลให้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.3 ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

1.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) จะต้องกำหนดโดยเจ้าหน้าที่สารสนเทศ เท่านั้น

1.5 กรณีส่งเครื่องคอมพิวเตอร์ตรวจซ่อมโดยผู้รับจ้างต้องได้รับการพิจารณาจากงานสารสนเทศ เมื่อตรวจซ่อมเสร็จแล้วต้องให้งานสารสนเทศ เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวซื้อกับการใช้งานระบบสารสนเทศของโรงพยาบาล

1.6 ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ต้องมีการ Update service pack และ hot fixที่เป็น version ล่าสุดเสมอ โดยเจ้าหน้าที่งานสารสนเทศเท่านั้น

1.7 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ ในเครื่องคอมพิวเตอร์ของโรงพยาบาล เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากเจ้าหน้าที่งานสารสนเทศ

1.8 ห้ามตัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ทุกเครื่อง เว้นแต่ให้รับความเห็นชอบจากเจ้าหน้าที่งานสารสนเทศ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ ให้มีสภาพเดิม

1.9 เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสโดยโปรแกรมป้องกันไวรัสของโรงพยาบาลจากเจ้าหน้าที่งานสารสนเทศ

1.10 การนำเครื่องคอมพิวเตอร์ทุกเครื่องออกไปใช้งานนอกโรงพยาบาล เมื่อนำกลับมาที่โรงพยาบาล ต้องทำการเชื่อมต่อระบบเครือข่ายภายในโรงพยาบาล เพื่อทำการอัพเดท (Update) ข้อมูลไวรัสล่าสุด และต้องมีการป้องกันความเสี่ยงจากการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาตจากบุคคลภายนอกโรงพยาบาล ซึ่งรวมถึงครอบครัวและเพื่อน

1.11 ห้ามผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลารองเครื่องคอมพิวเตอร์ของโรงพยาบาลทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดรอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้งานสารสนเทศทราบทันที

1.12 การเชื่อมต่อเพื่อใช้ระบบงานจากภายนอกให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

1.13 ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของเครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และต้องทำการแจ้งการเปลี่ยนแปลงแก่ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

2. ความปลอดภัยทางด้านกายภาพ

2.1 ผู้ใช้งาน มีหน้าที่รับผิดรอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

2.2 ผู้ใช้งาน ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์ที่ในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

2.3 ไม่ควรใส่เครื่องคอมพิวเตอร์ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจ จากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

2.4 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

2.5 หลีกเสี่ยงการใช้ของแข็งกดสัมผัสหน้าจอ ให้เป็นรอยขีดขวน หรือทำให้หน้าจอของเครื่องคอมพิวเตอร์แตกเสียหายได้

2.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.7 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าที่มีรอยขีดข่วนได้

2.8 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.9 ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

2.10 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์ใกล้สิ่งที่เป็นของเหลว

2.11 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.12 ไม่ควรวางเครื่องคอมพิวเตอร์ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้

2.13 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน

3. การเข้าใช้เครื่องคอมพิวเตอร์ (ระบบปฏิบัติการ) และ รหัสผ่าน

3.1 ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

3.2 ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ในเอกสาร "ข้อกำหนดการจัดการชื่อผู้ใช้และรหัสผ่านของระบบสารสนเทศของโรงพยาบาล"

3.3 ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ 15 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

3.4 ผู้ใช้งานต้องทำการ Logout (ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน)

3.3 ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้ใช้งานใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4. การสำรองข้อมูลและการกู้คืน

4.1 งานสารสนเทศ มีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่นฮาร์ดดิสก์แบบติดตั้งภายนอก เป็นต้น

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.2 ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

5.3 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีจุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

14. การใช้งานอินเทอร์เน็ต (Use of the Internet)

แนวทางปฏิบัติ

1. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall. Proxy และ IPS/IDS

2. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser), ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการจุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

3. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของโรงพยาบาล เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

4. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดรอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของโรงพยาบาล โดยผ่านความเห็นชอบจากผู้บริหารของหน่วยงานต้นสังกัด

5. ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของโรงพยาบาล ที่ไม่เข้าหลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ต

6. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความนำเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

7. การใช้งานเว็บบอร์ด (Web Board) ของโรงพยาบาล ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของโรงพยาบาล

8. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

9. ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ พ.ศ. 2560อย่างเคร่งครัด

15. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย *(Wireless Policy)*

แนวปฏิบัติ

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของโรงพยาบาลบ้านตาขุนมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

1. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุดห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

2. ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

3. กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

3.1 ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

3.2 ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

3.3 ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

3.4 ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

3.5 ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

3.6 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

3.7ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์สารสนเทศทราบทันที

16. นโยบายและแนวปฏิบัติการสำรองและกู้คืนข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and Recovery and IT Continuity Plan)

แนวทางปฏิบัติ

1. การสำรองข้อมูลและกู้คืนข้อมูลในสถานการณ์ปกติ เมื่อมีระบบงานใหม่หรือข้อมูลใหม่หรือข้อมูลที่มีการ
เปลี่ยนแปลงใหม่ กำหนดให้ใช้แนวทางปฏิบัติในการจัดทำนโยบายการสำรอง และกู้คืนข้อมูล ดังต่อไปนี้

1.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนทศ และกำหนดความถี่ในการสำรองข้อมูล โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วันเวลา อุปกรณ์ที่ใช้ในการสำรอง เป็นต้น
-ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ระบบปฏิบัติการซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน
-ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
-ตรวจสอบและทดลอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

1.3 กำหนดผู้รับผิดรอบในการสำรองข้อมูล

1.4 กำหนดชนิดของระบบงานนั้น ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อย ต้องประกอบด้วยข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นตัน

1.5 กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบ

1.6 กำหนดชั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

1.7 การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้บริเวณพื้นที่ภายนอกอาคารของโรงพยาบาล

1.8 ต้องจัดทำฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อสำรองข้อมูล เพื่อให้สามารถค้นหาได้โดยเร็ว

1.9 ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลในการสำรองข้อมูลทุกครั้ง

1.10 ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

1.11 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

1.12 การสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสารและมีการตรวจสอบความถูกต้องเป็นระยะๆ

1.13 ต้องมีการตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปี

1.14 สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

1.15 การขอใช้งานสื่อบันทึกข้อมูลสำรองจะต้องได้รับอนุมัติจากผู้มีอำนาจหน้าที่และจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยต้องมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติประเภทข้อมูล
และเวลา

2. ต้องจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ให้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

2.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลด
ความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว น้ำท่วม การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนทศ

(4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(6) การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวร้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่
ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกันการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

3. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดรอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สมารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

4. เจ้าหน้าที่ที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน ต้องเข้ารับการอบรม หรือสร้างความตระหนักเพื่อให้รู้หรือทราบวิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉินในกรณีต่างๆ

5. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

6. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

7. การกำหนดผู้รับผิดชอบ หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

7.1 รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดขอบการปฏิบัติงาน ได้แก่

7.1.1. ผู้อำนวยการโรงพยาบาลบ้านตาขุน

7.1.2 หัวหน้ากลุ่มงานหลักประกัน ยุทธศาสตร์และสารสนเทศทางการแพทย์

7.2 รับผิดชอบการปฏิบัติงาน การสำรองข้อมูล การประสานงาน ประกอบด้วย

7.2.1 นายสรศักดิ์ นาคจิตร ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ

7.2.2 นางสาวจิติมา ศรีสาคร ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ

7.2.3 นางสาวเบญจวรรณ ชูพรม ตำแหน่งนักวิชาการคอมพิวเตอร์

|

17. ความมั่นคงปลอดภัยของ Firewall

แนวปฏิบัติ

1. งานสารสนเทศมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Fire wal) ทั้งหมด

2. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

3. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

4. ผู้ใช้งานอินเทอร์เน็ตจากภายนอก จะต้องมีการ Login account ก่อนการใช้งานทุกครั้ง

5. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

6. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการ เท่านั้น

7. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูล จราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

8. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อ พื้นฐานของโปรแกรมทั่วไปที่แผนกไอที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือที่กำหนด จะต้องได้รับการพิจารณาอนุมัติจากงานสารสนเทศ

9. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้อง กำหนด ค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับ เครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

10. ต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุก ครั้งที่มี การเปลี่ยนแปลงค่า

11. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อ ใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

12. งานสารสนเทศ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ ผิดนโยบาย หรือเกิดจากการทางานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

13. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์ เครือข่าย ภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับ เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และได้รับความเห็นชอบจากสำนักงานก่อน

14. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ต

18. ความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

แนวปฏิบัติ

1. ให้จัดทำ Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสานักงาน และเครือข่ายข้อมูลทั้งหมดรวมถึง เส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

2. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจาก ระบบ IDS/IPS

3. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบ สารสนเทศตามปกติ

4. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมี การรายงานให้ผู้บังคับบัญชาทราบทันที่ที่ตรวจพบ

5. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีก ในอนาคต

6. สำนักงาน มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการ บุกรุก ระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

19. นโยบายการตรวจสอบและประเมินความเสี่ยง

การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

1. งานสารสนเทศต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารข้อมูล อย่างน้อยปีละ 1 ครั้ง

2. งานสารสนเทศต้องจัดให้มีการตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยระบบสารสนเทศทั้งจาก ผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor)

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลได้รับความเสียหาย หรืออันตรายใดๆ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาล ผู้กระทำการดังกล่าว ต้องรับผิดชอบและชดใช้ ค่าเสียหายที่เกิดขึ้นทั้งหมด

4. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลก่อให้เกิดความเสียหายหรืออันตรายใดๆ แก่โรงพยาบาลหรือ ผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้กระทำการดังกล่าวต้องรับผิดชอบและชดใช้ ค่าเสียหายที่เกิดขึ้นทั้งหมด

5. กำหนดให้ผู้อำนวยการ และคณะกรรมการบริหารความเสี่ยง มีหน้าที่กำกับดูแล รับผิดชอบการ ดำเนินงานด้านสารสนเทศ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายใดๆ ที่เกิดขึ้นกับระบบ คอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาล

20. การใช้สิทธิในการเข้าถึงข้อมูลสารสนเทศในการตรวจสอบและประเมินความเสี่ยง

แนวปฏิบัติ

1. งานสารสนเทศมีหน้าที่เก็บและตรวจสอบข้อมูลสารสนเทศที่มีอยู่ในระบบ รวมทั้ง มีหน้าที่เก็บบันทึก ข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานภายในโรงพยาบาล ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบ คอมพิวเตอร์ โดยจะเก็บรักษาไว้ไม่น้อยกว่า 90 วัน

2. งานสารสนเทศและหน่วยงานที่เกี่ยวข้อง มีหน้าที่กำหนดสิทธิการเข้าใช้ระบบงานสารสนเทศของโรงพยาบาลทุกระบบ ให้แก่ผู้ใช้งานทั้งผู้ใช้งานภายในและผู้ใช้งานภายนอกทุกระดับ ได้แก่ ระดับผู้ใช้งานทั่วไป ระดับ เจ้าของระบบงาน และระดับผู้ดูแลระบบ หรืออื่นใดตามการมอบหมายจากผู้บริหาร

3. เจ้าหน้าที่ของโรงพยาบาลทุกคน เมื่อพบข้อบกพร่องด้านความมั่นคงปลอดภัยของโรงพยาบาล หรือเหตุการณ์ละเมิด ความมั่นคงปลอดภัยต่างๆ หรือการละเมิดข้อกำหนดนี้ ให้งานสารสนเทศ

4. ห้ามเจ้าหน้าที่กระทำการใดๆ ที่มีผลให้เกิดอันตราย เป็นภัยคุกคาม หรือเป็นโทษกับผู้อื่น ได้แก่ การทำให้ ลดประสิทธิภาพในการทำงานของเครือข่ายคอมพิวเตอร์ การกีดกัน ถอดถอนสิทธิในการใช้งานเครือข่าย คอมพิวเตอร์ของเจ้าหน้าที่ที่มีสิทธิในการใช้งาน การเพิ่มสิทธิในการใช้งานเกินกว่าสิทธิที่กำหนดไว้ หรือการ ใช้อุบายดักการตรวจสอบความมั่นคงปลอดภัยของคอมพิวเตอร์ของโรงพยาบาล

5. เจ้าหน้าที่ของโรงพยาบาลทุกคน ต้องไม่พยายามที่จะเข้าถึงข้อมูลใดๆ หรือระบบงานใดๆ ที่มีอยู่ในระบบ เครือข่ายคอมพิวเตอร์ของโรงพยาบาล ที่เจ้าหน้าที่นั้น ไม่มีสิทธิในข้อมูลหรือระบบงานนั้นๆ เว้นแต่จะได้รับอนุญาตจากผู้มีอำนาจอนุญาต

6. การเข้าใช้งานของระบบสารสนเทศ ต้องมีการกำหนดชื่อผู้ใช้งานและ รหัสผ่าน และสิทธิการเข้าใช้งาน

7. รหัสผู้ใช้งาน และรหัสผ่านหรือข้อมูลประเภทที่คล้ายกัน หรืออุปกรณ์ที่ใช้ในการยืนยันสิทธิในการใช้งาน ซึ่งยืนยันตัวบุคคลถือว่าเป็นข้อมูลลับ โดยห้ามทำการเผยแพร่ต่อบุคคลภายนอก ให้ทราบและเจ้าของรหัส ไม่สามารถปฏิเสธความรับผิดชอบได้ในกรณีที่เกิดความเสียหายของข้อมูลหรือระบบข ดังกล่าว

21. การให้การสนับสนุนต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพ.ศ. 2560 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

แนวปฏิบัติ

ผู้ใช้งานเครือข่ายและสารสนเทศของโรงพยาบาล ต้องไม่กระทำการอันเป็นการกระทำความผิดตาม พ.ร.บ.ฯ คอมพิวเตอร์ และ พ.ร.บ. การรรักษาความมั่นคงปลอดภัยไซเบอร์ฯ ดังนี้

1. เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะของผู้อื่นโดยมิชอบด้วยนโยบายด้าน การเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์

2. พยายามหรือ ทำให้ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการ เฉพาะแล้ว นำไปเปิดเผยโดยมิชอบ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

3. เข้าถึงโดย มิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการ นั้นมิได้มีไว้ สำหรับตน

4. กระทำด้วยประการใดโดยมิชอบ ด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือ เพื่อให้บุคคลทั่วไปใช้ประโยชน์

5. ทำให้เสียหาย, ทำลาย, แก้ไข, เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ

6. กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอขัดขวาง หรือรบกวนจนไม่สามารถทางานตามปกติได้

7. ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของ การส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดย ปกติสุข

8. กระทำความผิดตามข้อ 5 หรือ ข้อ 6 แล้ว

- ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือภายหลัง
- เป็นการกระทำที่เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในเศรษฐกิจของประเทศ และกระทำความผิดดังที่กล่าวมาแล้วเป็นเหตุให้ผู้อื่นถึงแก่ความตาย

9. จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำ ความผิดตาม ข้อ 1 ถึง ข้อ 7

10. นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ตามที่ระบุไว้ดังต่อไปนี้

10.1 ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความ เสียหายแก่ผู้อื่นหรือประชาชน

10.2 ข้อมูลอันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความ ตื่นตระหนกแก่ประชาชน

10.3 ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตาม ประมวลกฎหมายอาญา

10.4 ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

10.5 เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตามข้อ 10.1 - 10.4

10.6 จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามข้อ 10 ในระบบคอมพิวเตอร์ที่อยู่ในความ ควบคุมของตน

11. นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพ ของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูก เกลียดชัง หรือได้รับ ความอับอาย

12. ไม่ทำการใดๆ ที่เข้าข่ายลักษณะของภัยคุกคามทางไซเบอร์ ที่มีการแบ่งเป็น 3 ระดับดังต่อไปนี้

12.1 ภัยคุกคามทางไซเบอร์ในระดับเฝ้าระวัง หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่อาจก่อให้เกิด ความเสียหาย แต่ยังไม่ก่อให้เกิดผลกระทบต่อบุคคล ทรัพย์สิน หรือข้อมูลที่เกี่ยวข้องที่สำคัญในระดับ ร้ายแรง

12.2 ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามในระดับร้ายแรงที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงที่จะทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบ คอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือการให้บริการของโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ

(ข) เป็นภัยคุกคามที่ก่อให้เกิดความเสี่ยงภัยจนอาจทำให้คอมพิวเตอร์ ระบบคอมพิวเตอร์ที่ ให้บริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงของรัฐ การป้องกันประเทศความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชน ถูกแทรกแซงอย่างมีนัยสำคัญ หรือถูกระงับการทำงาน

(ค) เป็นภัยคุกคามที่มีความรุนแรงที่ก่อหรือ อาจก่อให้เกิดความเสี่ยงภัย หรือความเสียหาย ต่อ บุคคล หรือต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่สำคัญหรือมีจำนวนมาก

12.3 ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิด และส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สาธารณูปโภคขั้นพื้นฐาน ความมั่นคงของรัฐ หรือชีวิตความเป็นอยู่ของประชาชน

(ข) เป็นภัยคุกคามทางไซเบอร์ที่ฉุกเฉิน เร่งด่วน ที่ใกล้จะเกิดอันอาจเป็นผลให้บุคคลจำนวน มากเสียชีวิต หรือระบบคอมพิวเตอร์จำนวนมากถูกทำลายในวงกว้างระดับประเทศ

(ค) เป็น ภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือ เป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนหนึ่งส่วนใดของประเทศตกอยู่ในภาวะ คับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกครองระบบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่ง ราชอาณาจักรไทย เอกราชและบูรณภาพแห่ง อาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การ ดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ ส่วนรวม หรือการป้องปัด หรือ แก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่าง ฉุกเฉินและร้ายแรง

22. การแจกจ่ายเอกสารนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. แผนการเผยแพร่นโยบาย

1.1 เอกสารนโยบายและแนวปฏิบัติฉบับนี้ จะจัดทำให้ผู้ใช้งานทุกคนได้อ่าน และทำความเข้าใจ และ ประกาศบนเว็บไซต์ของโรงพยาบาล

2. แผนการฝึกอบรม

2.1 รวบรวมข้อมูล วิเคราะห์ว่าพนักงานหน่วยงานใดได้รับผลกระทบจากนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.2 พนักงานที่ได้รับผลกระทบดังกล่าว ต้องได้รับการฝึกอบรมเรื่องนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.3 ต้องสร้างความรู้ความเข้าใจกับผู้ใช้งานให้ทราบถึงความมั่นคงปลอดภัยสารสนเทศ เพื่อให้เกิดความ ตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือ รู้เท่าไม่ถึงการณ์ โดยฝึกอบรมการใช้งานระบบสารสนเทศของโรงพยาบาล หรือฝึกอบรมนโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามความจำเป็น

23. บทลงโทษ

ผู้ใช้งานคนใดฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้ โรงพยาบาล จะพิจารณาลงโทษทางวินัยตามระเบียบ บริหารงานบุคคล รวมทั้งอาจมีความรับผิดทั้งทางแพ่ง และทางอาญา

24. การทบทวนนโยบาย

งานสารสนเทศ ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำ อย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้ คณะอนุกรรมการบริหารความเสี่ยง และผู้อำนวยการอนุมัติ หากมีการเปลี่ยนแปลง

ประกาศใช้ ณ วันที่ 1 ตุลาคม พ.ศ. 2564 เป็นต้นไป

(นายเอกพล พิศาล)

ผู้อำนวยการโรงพยาบาลบ้านตาขุน