



โรงพยาบาลสมเด็จพระยุพราชเวียงสระ

ประกาศนโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

พ.ศ. ๒๕๖๕

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๕๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย ในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ จึงเห็นสมควรกำหนดนโยบาย ดังนี้

๑. โรงพยาบาลสมเด็จพระยุพราชเวียงสระส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๒. โรงพยาบาลสมเด็จพระยุพราชเวียงสระ มีหน้าที่ จำกัด ระบุ รับ เพิกถอนสิทธิหรือบทลงโทษตามความเหมาะสม หากมี การละเมิดหรือฝ่าฝืนแนวปฏิบัติ ในกรณีที่สำคัญคณะกรรมการสารสนเทศและคอมพิวเตอร์รายงานการฝ่าฝืนให้ต้นสังกัดหรือโรงพยาบาลพิจารณาลงโทษ

๓. โรงพยาบาลสมเด็จพระยุพราชเวียงสระ สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๔. โรงพยาบาลสมเด็จพระยุพราชเวียงสระ สนับสนุนการรักษาความปลอดภัยของข้อมูลตามแนวปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๕ มกราคม พ.ศ.๒๕๖๕

(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



ประกาศ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ

เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๕๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้ง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ จึงเห็นสมควรกำหนดนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑.การจัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒.กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓.นโยบายและแนวทางปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๕.นโยบายและแนวทางปฏิบัตินี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓. นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ

๓.๑.โรงพยาบาลสมเด็จพระยุพราชเวียงสระ ส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒.โรงพยาบาลสมเด็จพระยุพราชเวียงสระ มีหน้าที่จำกัด ระบุ รับ เหิกถอนสิทธิหรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญศูนย์เทคโนโลยีสารสนเทศรายงานการฝ่าฝืนให้ต้นสังกัดหรือโรงพยาบาลเพื่อพิจารณาลงโทษ

๓.๓.โรงพยาบาลสมเด็จพระยุพราชเวียงสระ สนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๔.โรงพยาบาลสมเด็จพระยุพราชเวียงสระ สนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

๔. องค์ประกอบของแนวทางปฏิบัติ

๔.๑. คำนิยาม

๔.๒. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๔.๓. การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

๔.๔. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔.๕. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๔.๖. การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

๔.๗. การรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

๔.๘. การรักษาความมั่นคงปลอดภัยของการตรวจจัดการบุกรุก

๔.๙. ความมั่นคงปลอดภัยของการสำรองข้อมูล

๔.๑๐. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief information officer) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศ หมายถึง ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

หัวหน้าศูนย์เทคโนโลยีสารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษา

ระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งโรงพยาบาลสมเด็จพระยุพราชเวียงสะกำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลสมเด็จพระยุพราชเวียงสะ

เช่น ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสะ รองผู้อำนวยการโรงพยาบาล หัวหน้าตึก หัวหน้ากลุ่มงาน เป็นต้น

ผู้ดูแลระบบ (System administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ Email account เป็นต้น

เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการต่าง ๆ ของโรงพยาบาลสมเด็จพระยุพราชเวียงสะ

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลสมเด็จพระยุพราชเวียงสะอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

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

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

ระบบอินเทอร์เน็ต (internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information system workplace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็นพื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้ง

อุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (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 เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่เข้มงวด หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

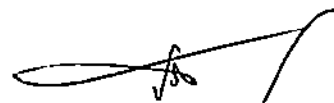
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดอาจทำให้ระบบขององค์กรถูกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ประกาศ ณ วันที่ ๕ มกราคม พ.ศ. ๒๕๖๕



(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



เรื่อง แนวทางปฏิบัติการรักษาความมั่นคง ปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and environment security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ให้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ให้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ประกาศ ณ วันที่ ๕ มกราคม พ.ศ. ๒๕๖๕

(นายปรีชา/สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



ประกาศ แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงักรวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่ใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระมีดังนี้

๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์เทคโนโลยีสารสนเทศ

๒.๑.๒ ผู้ดูแลระบบ (System administrator) ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ โรงพยาบาลสมเด็จพระยุพราชเวียงสระกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่นระบบคอมพิวเตอร์ โปรแกรมประยุกต์(Application) จดหมายอิเล็กทรอนิกส์ (Email) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๒.๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๒.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคล

อื่นหรือการส่งจดหมายอิเล็กทรอนิกส์(email) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๒.๓.๓ ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๒.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๒.๔.๒ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๒.๔.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๒.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPNหรือ XML Encryption เป็นต้น

๒.๒.๔.๕ กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๒.๔.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่นส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๓.๓ ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเพื่อทำการ Lock หน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ หากไม่อยู่ที่หน้าจอ ระบบจะออกจากระบบ ภายใน ๕ นาที

ประกาศ ณ วันที่ ๕ มกราคม พ.ศ. ๒๕๖๕



(นายปรีชา ฤมาถัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



เรื่อง การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

ผู้รับผิดชอบ : คณะกรรมการดำเนินงานพัฒนาระบบสารสนเทศโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

วัตถุประสงค์

๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๓ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๔ เพื่อเป็นการลดความเสียหายและเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศ

๑. กรณีไฟฟ้าดับและเครื่องปั่นไฟสำรองไม่ทำงาน ระยะเวลาไม่เกิน ๓๐ นาที

เจ้าหน้าที่คอมพิวเตอร์

๑. ประสานงานกับงานซ่อมบำรุง เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก้ไข หากสามารถแก้ไขได้ภายใน ๓๐ นาที ให้ตรวจสอบการทำงานของ UPS ที่ห้อง server

๒. ประกาศแจ้งทางวิทยุสื่อสาร/Line ข่าวสาร/แจ้งด้วยวาจา ให้หน่วยงานต่าง ๆ ทราบเพื่อปิดคอมพิวเตอร์และเครื่องสำรองไฟชั่วคราว

๓. เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย SwitchHUB, Access Point

๔. ตรวจสอบการเข้าใช้งานโปรแกรม HIS

๕. ประกาศแจ้งให้หน่วยงานต่าง ๆ เปิดคอมพิวเตอร์ใช้งาน HIS ได้ตามปกติ

เจ้าหน้าที่หน่วยงานอื่นๆ

๑. เมื่อได้รับแจ้งจากงานคอมพิวเตอร์ให้ ปิดคอมพิวเตอร์และ UPS

๒. ประชาสัมพันธ์ให้ประชาชนที่รอรับบริการทราบ ถ้าเป็นผู้ป่วยไม่ฉุกเฉินให้รอรับบริการ

๓. กรณีเครื่องสำรองไฟฟ้า (UPS) มีปัญหาไม่สำรองไฟ ให้แจ้งงานคอมพิวเตอร์เมื่อเหตุการณ์ปกติแล้ว

๒. กรณีไฟฟ้าดับและเครื่องปั่นไฟสำรองไม่ทำงาน ระยะเวลาเกิน ๓๐ นาที

เจ้าหน้าที่งานคอมพิวเตอร์

๑. ประสานงานกับงานซ่อมบำรุง เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก้ไข หากไม่สามารถแก้ไขได้ภายใน ๓๐ นาที ให้แจ้งผู้อำนวยการ /ประธานกรรมการสารสนเทศทราบ
๒. หัวหน้ากลุ่มงาน ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ให้หน่วยงานต่างๆทราบ
๓. ปิดเครื่อง SERVER และอุปกรณ์ต่างๆ
๔. เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย และข้อมูลในโปรแกรม HIS
๕. หัวหน้ากลุ่มงาน ประกาศแจ้งยกเลิกแผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ให้หน่วยงานต่างๆทราบ เมื่อระบบสามารถใช้งาน HIS ได้ตามปกติ
๖. สรุปรายงานนำเสนอผู้อำนวยการและคณะกรรมการบริหารทราบ

เจ้าหน้าที่เวชระเบียน

๑. เมื่อได้ยินประกาศประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ จัดเตรียมแบบฟอร์มใบสั่งยาสำหรับออกหน่วย ,แบบฟอร์มลงทะเบียนผู้ป่วยใหม่, ปากกา ,ตราป้อมวันที่ คอมพิวเตอร์โน้ตบุ๊กของงานเวชระเบียนที่ติดตั้งฐานข้อมูล HIS สำหรับค้นข้อมูล HN ของผู้ป่วย เพื่อใช้บันทึกข้อมูลชั่วคราว
๒. เมื่อระบบสามารถกลับมาใช้งานได้ตามปกติ ให้นำข้อมูลจากแบบฟอร์มใบสั่งยาสำหรับออกหน่วย และแบบฟอร์มลงทะเบียนผู้ป่วยใหม่ ลงบันทึกส่งตรวจย้อนหลังจนเป็นปัจจุบัน

เจ้าหน้าที่ห้องจ่ายยา

๑. เมื่อได้รับแจ้งประกาศใช้แผนฉุกเฉินกรณีระบบล่ม ให้หยุดการลงบันทึกข้อมูลในคอมพิวเตอร์ ปรีนใบสั่งยาและสติ๊กเกอร์ฉลากยาที่แพทย์สั่งยาแล้วออกมาทุกคน ปิดเครื่องคอมพิวเตอร์และเครื่องสำรองไฟฟ้า
๒. แจ้งประชาสัมพันธ์ให้ผู้รับบริการทราบ
๓. ลงบันทึกการจ่ายเวชภัณฑ์ กิจกรรมลงในใบสั่งยาและเขียนซองยา
๔. เก็บใบสั่งยาไว้ที่ห้องจ่ายยา เพื่อลงบันทึกข้อมูลย้อนหลังเมื่อระบบสามารถใช้งานได้ตามปกติ

เจ้าหน้าที่ห้องการเงิน

๑. กรณีมีค่าใช้จ่ายที่สามารถสรุปค่าใช้จ่ายได้ เช่น ใบรับรองแพทย์ให้เก็บเงินโดยใช้ใบเสร็จเล่มเขียว
๒. กรณีไม่สามารถสรุปค่าใช้จ่ายได้ ให้แยกใบสั่งยาไว้และแจ้งผู้ป่วย/ญาติทราบว่า จะลงบันทึกเป็นผู้ป่วยค้างชำระไว้ก่อนชั่วคราว
๓. เมื่อระบบคอมพิวเตอร์สามารถใช้งานได้ตามปกติ และหน่วยงานต่าง ๆ ลงบันทึกข้อมูลบริการในโปรแกรม HIS เรียบร้อย การเงินสรุปค่าใช้จ่าย ทำค้างชำระ

เจ้าหน้าที่หน่วยงานอื่นๆ

๑. เมื่อได้รับแจ้งประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายไม่สามารถใช้งานได้ให้หยุดการลงบันทึกข้อมูลในคอมพิวเตอร์ ปิดเครื่องคอมพิวเตอร์และเครื่องสำรองไฟฟ้า
๒. แจ้งประชาสัมพันธ์ให้ผู้รับบริการทราบ
๓. บันทึกบริการ/กิจกรรม/เวชภัณฑ์ ในใบสั่งยาแทน
๔. เมื่อระบบสามารถใช้งานได้ตามปกติ ให้นำข้อมูลการให้บริการลงบันทึกลงในโปรแกรม HIS ย้อนหลัง

๓. กรณีเครื่อง Server /Database มีปัญหา สามารถแก้ไขได้ภายใน ๓๐ นาที

เจ้าหน้าที่งานคอมพิวเตอร์

๑. ตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากสามารถแก้ไขได้ภายใน ๓๐ นาที แจ้งประกาศให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HIS ชั่วคราว
๒. ดำเนินการแก้ไข ตรวจสอบความพร้อมให้เรียบร้อย
- กรณี server หลักรุ่นและไม่สามารถแก้ไขได้ภายใน ๓๐ นาที ให้เปลี่ยนไปใช้ server สำรอง
๓. เมื่อระบบ HIS ใช้งานได้ให้ประกาศให้ทุกหน่วยงานสามารถใช้งาน HIS ได้ตามปกติ
๔. สรุปสาเหตุของปัญหา และลงบันทึกในโปรแกรมความเสี่ยง

เจ้าหน้าที่หน่วยงานต่างๆ

๑. เมื่อได้รับแจ้งจากงานคอมพิวเตอร์ให้หยุดการใช้งานคอมพิวเตอร์ชั่วคราว
๒. ประชาสัมพันธ์ให้ประชาชนที่รอรับบริการทราบ และจัดบริการที่สามารถทำได้โดยบันทึกลงในแบบฟอร์มใบสั่งยาชั่วคราวและเก็บเอกสารเพื่อรอลงบันทึก เมื่อได้รับแจ้งให้ใช้งานคอมพิวเตอร์ได้ตามปกติ ให้เริ่มนำข้อมูลบริการลงบันทึกในโปรแกรม HIS

๔. กรณีเครื่อง Server /Database มีปัญหา ไม่สามารถแก้ไขได้ภายใน ๓๐ นาที

เจ้าหน้าที่งานคอมพิวเตอร์

๑. เจ้าหน้าที่งานคอมพิวเตอร์ตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากไม่สามารถแก้ไขได้ภายใน ๓๐ นาที ให้แจ้งผู้อำนวยการ /ประธานกรรมการสารสนเทศทราบ
๒. ประธานกรรมการสารสนเทศ ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้ โดยใช้กรณีเดียวกับข้อกรณีไฟฟ้่าดับ มากกว่า ๓๐ นาที ให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HIS
๓. งานคอมพิวเตอร์ดำเนินการแก้ไขปัญหา Server ให้สามารถใช้งานได้ตามปกติภายใน ๒๔ ชม.
๔. เมื่อเครื่อง Server สามารถทำงานได้ตามปกติ ให้ตรวจสอบความพร้อมของ Server และอุปกรณ์เครือข่าย
๕. ประกาศแจ้งให้หน่วยงานต่าง ๆ ใช้งาน HIS และเริ่มบันทึกข้อมูลย้อนหลัง
๖. ติดตามตรวจสอบความพร้อมของการลงบันทึกข้อมูลของหน่วยงานต่างๆ จนกระทั่งระบบข้อมูลเป็นปัจจุบัน และสามารถให้บริการได้ตามปกติ
๗. ประธานกรรมการสารสนเทศประกาศยกเลิกใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้
๘. ลงบันทึกในโปรแกรมความเสี่ยงสรุปรายงานนำเสนอผู้อำนวยการและคณะกรรมการบริหารทราบ

หมายเหตุ กรณีเครื่อง Server/Database กำหนดให้ผู้มีรายชื่อดังต่อไปนี้เป็นผู้ตรวจสอบและแก้ไขปัญหา

๑. นายพรชพล ตาชื่อ โทร.๐๘๓๑๗๔๒๐๑๖
๒. น.ส.อภิญา รักษายศ โทร.๐๘๕๖๙๒๕๕๐๕

๕. กรณีเกิดอัคคีภัย

เจ้าหน้าที่งานคอมพิวเตอร์

ดำเนินการขนย้ายอุปกรณ์ตามลำดับความสำคัญตามแผนอัคคีภัย ดังนี้

๑. ขนย้ายอุปกรณ์ในห้อง Server ดังนี้

- ตู้ Server
- Switch HUB
- เครื่องสำรองไฟฟ้า

๒. เมื่อสามารถควบคุมอัคคีภัยได้แล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย ,ระบบไฟฟ้า และติดตั้งอุปกรณ์ให้พร้อมใช้งาน

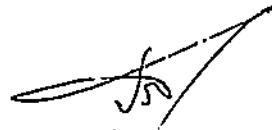
๓. ตรวจสอบความพร้อมใช้ของเครื่องลูกข่าย หากยังไม่พร้อมใช้งานให้ดำเนินการตามระเบียบปฏิบัติกรณีไฟฟ้าดับ หรือ กรณีเครื่อง Server /Database มีปัญหา

เจ้าหน้าที่อื่นๆ

หากเจ้าหน้าที่งานคอมพิวเตอร์ไม่อยู่ เจ้าหน้าที่อื่นสามารถดำเนินการได้ดังนี้

๑. ให้เปิดประตูห้อง Server หรือทั้งประตูเพื่อเข้าไปในห้อง server
๒. ทำการตัดสาย LAN โดยใช้คีมตัดสาย LAN ออกให้หมด
๓. ทำการถอดสายไฟที่อยู่ภายนอกตู้ Server ออกให้หมด
๔. ทำการเคลื่อนย้ายตามแผนป้องกันอัคคีภัย

ประกาศ ณ วันที่ ๖ มกราคม พ.ศ. ๒๕๖๕



(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย Wireless Policy

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการทำงานของระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless policy) ของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒.๒ ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็ Access point, Wireless router, Wireless USB client หรือ Wireless card

๒.๓ ห้ามผู้ใช้งาน (User) เปิด Ad-hoc หรือ peer to peer network

๒.๔ กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๒.๔.๑ ผู้ดูแลระบบต้องวาง Access point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

๒.๔.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น และตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๒.๔.๓ ให้เปลี่ยนค่า SSID (Service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access point ด้วย

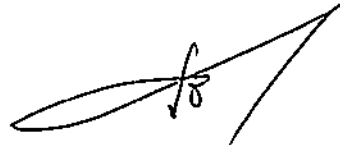
๒.๔.๔ ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check list เกี่ยวกับ Security configuration

๒.๔.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wireless Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ Access point และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๒.๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต Intranet และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

๒.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ
เครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่ง
รายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้
ผู้ดูแลระบบรายงานให้หัวหน้าศูนย์เทคโนโลยีสารสนเทศทราบทันที

ประกาศ ณ วันที่ ๖ มกราคม พ.ศ. ๒๕๖๕



(นายปรีชา สุมาลย์)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall policy)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้นเพื่อสร้างความมั่นคงปลอดภัยของการทำงานของระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

๒. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของโรงพยาบาลสมเด็จพระยุพราชเวียงสระมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๒.๑ ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ

๒.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๒.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

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

๒.๕ ค่าการเปลี่ยนแปลงทั้งหมดใหม่ไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๒.๖ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๒.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๒.๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลสมเด็จพระยุพราชเวียงสระ อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศ ก่อน

๒.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้นโดยข้อยกเว้นจะต้องระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายชื่อเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์เทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลดังนี้

๒.๙.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๒.๙.๒ หมายเลข IP address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒.๙.๓ วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้นๆ

๒.๙.๔ วันที่เริ่มใช้ และวันที่สิ้นสุดการใช้

๒.๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

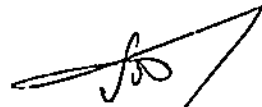
๒.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๒.๑๒ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ มีสิทธิที่จะระงับหรือบล็อกรการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๒.๑๓ ภายหลังจากอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบของโรงพยาบาลสมเด็จพระยุพราชเวียงสระหรือกฎหมาย หรืออาจจะทำให้เกิดความเสียหายด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศหรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางศูนย์เทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

๒.๑๔ การเชื่อมต่อในลักษณะของการ Remote loginจากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากโรงพยาบาลสมเด็จพระยุพราชเวียงสระ ก่อน

ประกาศ ณ วันที่ ๒ มกราคม พ.ศ. ๒๕๖๕



(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet security policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ ซึ่งผู้ใช้งานต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

ผู้ใช้งานเครือข่ายอินเทอร์เน็ตของโรงพยาบาลสมเด็จพระยุพราชเวียงสระมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๒.๑ การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ หรือทำการสมัครผ่านระบบอินเทอร์เน็ตของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ โดยสามารถใช้งานได้ ๑ วัน เพื่อรอการตรวจสอบตัวบุคคลและอนุมัติการใช้งานโดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลสมเด็จพระยุพราชเวียงสระ สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๒.๒ ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลนี้อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๓ ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลเครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมายเจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๒.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๖ ระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัปเดต (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

๒.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์แฟลชโปรแกรมอื่นๆที่มีลักษณะคล้ายกัน โดยต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ให้อาย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๘ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ที่ใช้งาน และออกจากการเครือข่ายอินเทอร์เน็ตด้วยการ logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ประกาศ ณ วันที่ ๒ มกราคม พ.ศ. ๒๕๖๕

(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

(Intrusion Detection System / Intrusion Prevention Systems: IDS/IPS policy)

๑. วัตถุประสงค์

IDS/IPS policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาลสมเด็จพระยุพราชเวียงสระ ให้มีความมั่นคงปลอดภัย

๒. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย เป็นดังนี้

๒.๑ IDS/IPS policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลสมเด็จพระยุพราชเวียงสระและเครือข่ายทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๒.๒ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๒.๓ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๒.๔ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๒.๕ มีการตรวจสอบและ Update patch/Signature ของ IDS/IPS เป็นประจำ

๒.๖ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๒.๗ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

๒.๘ เครื่องแม่ข่ายที่มีการติดตั้ง host based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๒.๙ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๒.๑๐ พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

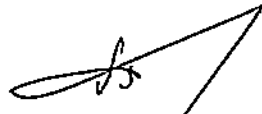
๒.๑๑ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๒.๑๒ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มัลแวร์ที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๒.๑๓ โรงพยาบาลสมเด็จพระยุพราชเวียงสระ มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๒.๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำ ความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลสมเด็จพระยุพราชเวียงสระ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ประกาศ ณ วันที่ ๗ มกราคม พ.ศ. ๒๕๖๕



(นายปรีชา สุมาลย์)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล
(Backup Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวทางปฏิบัติในการสำรองข้อมูล

๒.๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒.๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

๒.๓ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ประกาศ ณ วันที่ ๗ มกราคม พ.ศ. ๒๕๖๕

(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ



นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ทดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ประกาศ ณ วันที่ ๗ มกราคม พ.ศ. ๒๕๖๕

(นายปรีชา สุมาลัย)

ผู้อำนวยการโรงพยาบาลสมเด็จพระยุพราชเวียงสระ