ประกาศโรงพยาบาลตราด

เรื่อง นโยบายรักษาความปลอดภัยในระบบเทคโนโลยีสารสนเทศ

พ.ศ.๒๕๖๒

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ นอกจากนั้น กระทรวงสาธารณสุขได้มีนโยบายและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ ให้หน่วยงานภายใต้สังกัดใช้เป็นแนวทางในการดำเนินการเรื่องการรักษาความปลอดภัยด้านสารสนเทศ ด้วยเหตุนี้ เพื่อให้การดำเนินงานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราดเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ โรงพยาบาลตราดจึงเห็นสมควรกำหนดนโยบายดังนี้

๑. โรงพยาบาลตราดส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร
๒. โรงพยาบาลตราดมีหน้าที่กำกับดูแลให้ปฏิบัติตามระเบียบปฏิบัติ หากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติที่สำคัญ อาจทำให้ราชการเสียหาย ศูนย์เทคโนโลยีสารสนเทศจะรายงานต่อผู้มีอำนาจ เพื่อดำเนินตามกฎหมายต่อไป
๓. โรงพยาบาลตราดสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ
๔. โรงพยาบาลตราดสนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติเพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่๒๙ เมษายน พ.ศ. ๒๕๖๒

(นายสุเทวัน แพรนิมิตร)
ผู้อำนวยการโรงพยาบาลตราด

เอกสารแนบท้ายประกาศ

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลตราด

พ.ศ. ๒๕๖๒

โรงพยาบาลตราด จ.ตราด
กระทรวงสาธารณสุข
เมษายน ๒๕๖๒

คำนำ

ในปัจจุบันเทคโนโลยีสารสนเทศ นับว่าเป็นสิ่งสำคัญสำหรับองค์กรที่จะมาช่วยอำนวยความสะดวก ในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุน ในการดำเนินงานด้านต่างๆ ทั้งในเรื่องของบริหารงาน และการให้บริการ อย่างไรก็ตาม ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และช่วยอำนวยความสะดวกในด้านต่างๆ ได้มาก แต่ในขณะเดียวกันก็มีความเสี่ยงสูงที่อาจจะก่อให้เกิดอันตราย หรือสร้างความเสียหายต่อการหน่วยงาน ต่อบุคลากร และผู้รับบริการได้ เช่นกัน เพราะการใช้งานระบบสารสนเทศในปัจจุบันที่มีการเชื่อมโยงระหว่างหน่วยงานมากขึ้น ทำให้มีโอกาสถูกบุกรุกหรือโจมตีจากผู้ไม่หวังดี ซึ่งอาจจะก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลากหลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย การบุกโจมตีผ่านเครือข่ายอินเตอร์เน็ตเพื่อก่อกวนให้ระบบใช้การไม่ได้ หรือการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้สร้างความเสียหายต่อระบบสารสนเทศเป็นอย่างมาก ทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้นศูนย์เทคโนโลยีสารสนเทศโรงพยาบาลตราด จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลรักษา และควบคุมรักษาความปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น โรงพยาบาลตราด จึงจัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัยที่เชื่อถือได้ เป็นไปตามกฎหมายและข้อปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราด มีความจำเป็นต้องได้รับความร่วมมือจากทุกหน่วยงาน ในการนำนโยบายไปปฏิบัติและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้อง กับการพัฒนาของเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศโรงพยาบาลตราด จึงหวังเป็นอย่างยิ่งว่าแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบ ผู้บริหาร และผู้เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโรงพยาบาลตราดทุกคน ในการดูแลกษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

นายบุญเย็น หนูเล็ก
รองผู้อำนวยการด้านสารสนเทศ
โรงพยาบาลตราด

สารบัญ

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลตราด

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ และพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ นอกจากนั้นทางกระทรวงสาธารณสุขเอง ได้ประกาศนโยบายและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ ให้หน่วยงานภายใต้สังกัดใช้เป็นแนวทางในการดำเนินการเรื่องการรักษาความปลอดภัยด้านสารสนเทศ ด้วยเหตุนี้เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราดเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง มีการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการป้องกันการถูกคุกคามจากภัยต่างๆ โรงพยาบาลตราดเห็นสมควรให้มีการกำหนดนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน(Standard) และ แนวปฏิบัติ(Guideline) ให้ครอบคลุมด้านการรักษาความ มั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑. การจัดทำนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒. นโยบายและแนวทางปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ผู้ดูแลระบบ เจ้าหน้าที่ผู้ใช้งาน และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔. นโยบายและแนวทางปฏิบัตินี้ต้องมีการดำเนินการทบทวน ตรวจสอบ และประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓. นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ โรงพยาบาลตราด

๓.๑ โรงพยาบาลตราดส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยี สารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒ โรงพยาบาลตราดมีหน้าที่กำกับดูแลให้ปฏิบัติตามระเบียบปฏิบัติ หากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติที่สำคัญ อาจทำให้ราชการเสียหาย ศูนย์เทคโนโลยีสารสนเทศจะรายงานต่อผู้มีอำนาจ เพื่อดำเนินตามกฎหมายต่อไป

๓.๓ โรงพยาบาลตราดสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔ โรงพยาบาลตราดสนับสนุนการรักษาความปลอดภัยของข้อมูลตามระเบียบปฏิบัติเพื่อการปกป้องและรักษาข้อมูลความลับของผู้ใช้และข้อมูลผู้ป่วยอย่างเคร่งครัด

๔. องค์ประกอบของแนวทางปฏิบัติ

๔.๑. คำนิยาม

๔.๒. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๔.๓. การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศ

๔.๔. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔.๕. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๔.๖. การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

๔.๗. การรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต

๔.๘. การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

๔.๙. ความมั่นคงปลอดภัยของการสำรองข้อมูล

๔.๑๐. การรักษาความมั่นคงปลอดภัยของข้อมูลผู้ป่วยในระบบสารสนเทศ

๔.๑๑. การจัดการสื่อสารผ่านเครือข่ายสังคมออนไลน์(Social Network)

๔.๑๒. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

นโยบายรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ แต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ และแนวทางปฏิบัติ(Guideline) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลตราด

รองผู้อำนวยด้านสารสนเทศ หมายถึง รองผู้อำนวยการโรงพยาบาล ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลตราด ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ จัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราดและมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในโรงพยาบาลตราด

ศูนย์เทคโนโลยีสารสนเทศ หมายถึง ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลตราด

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราด

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติงานจริงเพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ(Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ(Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้ สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราด โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งโรงพยาบาลตราดกำหนดไว้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลตราด เช่น ผู้อำนวยการโรงพยาบาลตราด รองผู้อำนวยการโรงพยาบาล หัวหน้าตึก หัวหน้ากลุ่มงาน เป็นต้น

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีผู้ใช้ระบบ Internet เป็นต้น

เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการต่างๆ ของโรงพยาบาลตราด

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลตราด อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัด ระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่ง ข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ(Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน 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

ทรัพย์สิน หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

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

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์(Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่SMTP, POP3 และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

เครือข่ายสังคมออนไลน์ (Social Network) หมายถึง เว็บไซต์หรือโปรแกรมคอมพิวเตอร์ที่ช่วยให้คนสามารถการสื่อสารและแบ่งปันข้อมูลบนอินเทอร์เน็ต โดยใช้คอมพิวเตอร์หรือโทรศัพท์มือถือ

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตาม ความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓ ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบ เครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่าย ของหน่วยงานได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราดมีดังนี้

๒.๑. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศโรงพยาบาลตราด

๒.๑.๑. กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อรองผู้อำนวยการด้านสารสนเทศของโรงพยาบาลตราด

๒.๑.๒. ผู้ดูแลระบบ (System Administrator)ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๒.๑.๓. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึก และติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒. การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ โรงพยาบาลตราดกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ อินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๒.๓. ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๒.๒.๓.๑. กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้ งาน

๒.๒.๓.๒. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกสื์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๒.๓.๓. ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๒.๓.๔. ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๒.๓.๕. กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๒.๓.๖. ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด

๒.๒.๓.๗. ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจาก ผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ใน การควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้น ความลับ ดังต่อไปนี้

๒.๒.๘. ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการ เข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๒.๙. ต้องกำหนดรายชื่อผู้ใช้(Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้น ความลับของข้อมูล

๒.๒.๑๐. ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๒.๑๑. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๒.๒.๑๒. ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของ ระดับความสำคัญของข้อมูล

๒.๒.๑๓. ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลใน กรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่ เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๓.๑. ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๓.๒. ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๓.๓. ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอเพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๒.๓.๔. ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานมากกว่า ๑ ชม.

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
(Network and Server Policy)

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์ และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและ ข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

โรงพยาบาลตราด กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ ข่าย (Server) ดังนี้

๒.๑. ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุม ป้องกันการบุกรุกได้อย่างเป็นระบบ

๒.๒. ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๒.๓. การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่ หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำ ของระบบและผู้ใช้บริการอื่นๆ

๒.๔. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับ ระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๕. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้ อย่างมีประสิทธิภาพ ดังต่อไปนี้

๒.๕.๑. ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งาน เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการ เข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๒.๕.๒. ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

๒.๕.๓.ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมี ความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๒.๕.๔. ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๒.๕.๕. การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๒.๕.๖. เลขที่อยู่ไอพี(IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๒.๕.๗. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียด เกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๕.๘. การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๕.๙. ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และ รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือ เปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๒.๖. โรงพยาบาลตราด กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์(Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตาม แนวทาง ดังต่อไปนี้

๒.๖.๑. ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log)ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

๒.๖.๒. ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๒.๖.๒. ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๒.๖.๓. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๖.๔. เข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๗. โรงพยาบาลตราดกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย(Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๒.๗.๑. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร์ เพื่อขออนุญาตจากรองผู้อำนวยการด้านสารสนเทศของโรงพยาบาลตราด

๒.๗.๒. มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๒.๗.๓. วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากรองผู้อำนวยการด้านสารสนเทศของโรงพยาบาลตราด

๒.๗.๔. การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความ จำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๒.๗.๕. การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

๒.๘. ห้ามนำโปรแกรมใดๆมาติดตั้งภายในเครื่องคอมพิวเตอร์ หากต้องการติดตั้งเนื่องจากมีผลกับการปฏิบัติราชการต้องติดต่อศูนย์คอมพิวเตอร์

๒.๙. ห้ามใช้ Port USB กับเครื่องในระบบเครือข่าย

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย(Wireless Policy)

๑.วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการ กำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่าย ไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของโรงพยาบาลตราด มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๒.๑. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจาก ผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์ กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒.๒. ห้ามผู้ใช้งาน (User) นำอุปกรณ์Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงานไม่ ว่าจะเป็น 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 มาใช้งานและต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๒.๔.๔. ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check Lisk เกี่ยวกับ Security Configuration

๒.๔.๕. ผู้ดูแลระบบต้องกำหนดค่า WEP(Wired Equivalent Privacy) หรือ WPA(Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควร กำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๒.๔.๖. ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๒.๔.๗. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัย ของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบ ทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ ผิดปกติให้ผู้ดูแลระบบรายงานให้รองผู้อำนวยการด้านสารสนเทศทราบทันที

๒.๕. ห้ามไม่ให้ผู้ใช้งานเคลื่อนย้ายอุปกรณ์ Wireless โดยไม่ได้รับอนุญาต

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์(Firewall Policy)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆให้ เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

๒. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ของโรงพยาบาลตราดมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๒.๑. ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลตราด

๒.๒. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๒.๓. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๒.๔. ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัส ผู้ใช้(User account) และรหัสผ่าน (User password)

๒.๕. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์เช่น ค่าพารามิเตอร์การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๒.๖. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๒.๗. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่ อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อย กว่า ๙๐ วัน

๒.๘. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิด พอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลตราดอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศ ก่อน

๒.๙. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรือ อุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าศูนย์เทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลดังนี้

๒.๙.๑. หมายเลข Port ที่ต้องการขอให้เปิด

๒.๙.๒. หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒.๙.๓. วัตถุประสงค์หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

๒.๙.๔. วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

๒.๑๐. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุก สัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๒.๑๑. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้ มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๒.๑๒. โรงพยาบาลตราด มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย ที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลตราด หรือ กฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัย ของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๒.๑๓. ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบ ของโรงพยาบาลตราด หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความ ปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบ สารสนเทศของหน่วยงาน ทางศูนย์เทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

๒.๑๔. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการ ขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากโรงพยาบาลตราดก่อน

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต(Internet Security Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของโรงพยาบาลตราด ซึ่งผู้ใช้จะต้องให้ ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพ กฎเกณฑ์ที่วางไว้และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะ ทำให้การใช้งานอินเตอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเตอร์เน็ต

ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของโรงพยาบาลตราดมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๒.๑. การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการ เครือข่ายอินเตอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลตราด โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลตราด สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้าศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๒.๒. ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่ อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๓. ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และ ต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๔. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็น ผู้รับผิดชอบ

๒.๕. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๖. ระมัดระวังการดาวน์โหลด และติดตั้งโปรแกรมจากอินเตอร์เน็ต ระมัดระวังการใช้โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ไม่ดาวน์โหลดไฟล์ ขนาดใหญ่แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

๒.๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ Facebook โปรแกรมอื่น ๆที่มีลักษณะ คล้ายกันโดยต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอ ความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียง ของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๘. หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิด Web browser ที่ใช้งาน และออกจาก การเครือข่ายอินเตอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่นๆ

๒.๙. ห้ามนำคอมพิวเตอร์ที่เชื่อมต่ออินเตอร์เน็ต เชื่อต่อระบบ PMK ในทุกกรณี ยกเว้นเครื่องที่มีภาระกิจเฉพาะที่ได้รับอนุญาตจากรองผู้อำนวยการด้านสารสนเทศ

นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก(Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

๑. วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความ ปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่าย ภายในโรงพยาบาลตราด ให้มีความมั่นคงปลอดภัย

๒. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย เป็นดังนี้

๒.๑. IDS/IPS Policy ครอบคลุมทุกโฮสต์(Host) ในเครือข่ายของโรงพยาบาลตราดและ เครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่าย อินเทอร์เน็ตทุกเส้นทาง

๒.๒. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการ ตรวจสอบจากระบบ IDS/IPS

๒.๓. ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้ง และเปิดให้บริการ

๒.๔. โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๒.๕. มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

๒.๖. มีการตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึก ปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๒.๗. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่าย ของระบบเทคโนโลยีสารสนเทศตามปกติ

๒.๘. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๒.๙. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การ โจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จ และไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๒.๑๐. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๒.๑๑. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๒.๑๒. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของ เหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๒.๑๓. โรงพยาบาลตราด มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มี พฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๒.๑๔. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาล ตราด การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการ ทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลตราด จะต้องถูกดำเนินคดีตาม ขั้นตอนของกฎหมาย

แนวทางปฏิบัติการความมั่นคงปลอดภัยของการสำรองข้อมูล
(Backup Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวทางปฏิบัติในการสำรองข้อมูล

๒.๑. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการ สำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒.๒. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

๒.๓. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่ง ติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔. ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมา ได้ภายในระยะเวลาที่เหมาะสม

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลผู้ป่วยในระบบสารสนเทศ

๑.วัตถุประสงค์

กำหนดแนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูลผู้ป่วยในระบบสารสนเทศของโรงพยาบาล ให้กับบุคคลากรในโรงพยาบาลได้นำไปปฏิบัติในการป้องกันและรักษาความลับของข้อมูลผู้ป่วย เพื่อมิให้เกิดการเปิดเผยข้อมูลโดยไม่ได้รับการยินยอมจากผู้ป่วยเป็นอันขาด และป้องกันการแก้ไขหรือดัดแปลงข้อมูลของผู้ป่วยโดยไม่ได้รับอนุญาต

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลผู้ป่วยในระบบสารสนเทศ

๒.๑. เจ้าหน้าที่ของโรงพยาบาลตราดและเครือข่ายโรงพยาบาลตราดทุกคนมีหน้าที่ ป้องกัน ดูแล และรักษาความมั่งคงปลอดภัยของข้อมูลผู้ป่วย

๒.๒. ห้ามทำการเปิดเผยหรือเผยแพร่ข้อมูลของผู้มารับบริการให้กับผู้ไม่เกี่ยวข้องเป็นอันขาด

๒.๓. ห้ามทำการแก้ไข/ดัดแปลง ประวัติผู้ป่วยจากความเป็นจริง

๒.๔. ห้ามใช้เครื่องมือสื่อสารหรืออุปกรณ์ถ่ายภาพใดๆ ถ่ายภาพหน้าจอคอมพิวเตอร์ที่แสดงข้อมูลผู้ป่วยโดยไม่ได้รับการยินยอมจากผู้ป่วย

๒.๕. ห้ามทำการพิมพ์ หรือทำสำเนาข้อมูลผู้ป่วยออกจากระบบสารสนเทศโดยไม่ได้รับอนุญาตจากงานเวชระเบียน ยกเว้นในกรณีที่ใช้ประกอบในการให้บริการตรวจ รักษา สำหรับแพทย์หรือบุคลากรที่รับผิดชอบในการรักษาในครั้งนั้นๆ

๒.๖. ห้ามทำลาย หรือลบข้อมูลผู้ป่วยในทุกกรณี ยกเว้นได้รับมอบมายให้ดำเนินการจากผู้อำนวยการโรงพยาบาลตราด

๒.๗. มีการจัดทำระดับการเข้าถึงข้อมูลผู้ป่วยในผู้ใช้งานในแต่ละระดับ ในกรณีที่มีการเปลี่ยนแปลงการเข้าถึงข้อมูลผู้ป่วย ต้องได้รับอนุญาตจากรองผู้อำนวยการด้านสารสนเทศเท่านั้น และให้มีการทบทวนระดับในการเข้าถึงข้อมูลผู้ป่วยทุก ๑ ปี

แนวทางปฏิบัติการจัดการสื่อสารผ่านเครือข่ายสังคมออนไลน์(Social Network)

๑.วัตถุประสงค์

กำหนดแนวทางในการสื่อสารผ่านเครือข่ายสังคมออนไลน์(Social Network) เช่น LINE หรือ Facebook เพื่อให้เจ้าหน้าที่ของโรงพยาบาลตราดและเครือข่ายโรงพยาบาลตราดทุกคน ดำเนินการในการใช้สื่อเครือข่ายสังคมออนไลน์ด้วยความระมัดระวังโดยเฉพาะความลับผู้ป่วย ที่ต้องระวังมิให้เกิดการละเมิดความเป็นส่วนตัวหรือเปิดเผยความลับของผู้ป่วยโดยเด็ดขาด

๒. แนวทางปฏิบัติการจัดการความมั่นคงปลอดภัยของข้อมูลผู้ป่วย

๒.๑. ห้ามไม่ให้มีการส่งข้อมูลผู้ป่วยผ่านทางเครือข่ายสังคมออนไลน์ ที่แสดงรูปภาพ ข้อความ ชื่อ ตำแหน่ง หรือสถานะทางสังคม ที่สามารถระบุตัวตนของผู้ป่วยได้ หากมีความจำเป็นต้องได้รับการยินยอมจากผู้ป่วยแล้วเท่านั้น

๒.๒. ห้ามมิให้แสดงข้อความ รูปภาพที่ไม่สุภาพ การปลุกเร้าให้เกิดความแตกแยก การทำลายสถาบัน หรือการเปิดเผยเอกสารที่เป็นความลับของผู้ป่วยผ่านทางเครือข่ายสังคมออนไลน์

๒.๓. กรณีที่ต้องส่งข้อมูลผู้ป่วยในรูปแบบไฟล์อิเล็กทรอนิกส์ต้องมีการเข้ารหัสเพื่อไม่ให้ผู้ที่ไม่มีสิทธิ์เปิดอ่านได้

แนวทางปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอโดยการจัดฝึกอบรม อาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้และอาจเชิญวิทยากรจาก ภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือ ข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจ ความต้องการของผู้ใช้บริการ

แนวทางปฏิบัติการในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของโรงพยาบาลตราด ซึ่งจะนำข้อมูลการประเมินความเสี่ยงที่ได้ ใช้เป็นแนวทางการบริหารความเสี่ยงด้านสารสนเทศของโรงพยาบาลต่อไป

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ

๒.๑ จัดให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง

๒.๒ รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศให้คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและผู้บริหารทราบทุกครั้ง

๒.๓ นำผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ไปจัดทำแผนบริหารความเสี่ยงด้านสารสนเทศ และนำแผนดังกล่าวให้คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศพิจารณาเพื่อนำเสนอให้ผู้บริหารทราบต่อไป

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตราด เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

(นายสุพจน์ แพรนิมิตร)
ผู้อำนวยการโรงพยาบาลตราด
๒๙ เมษายน ๒๕๖๒