กรมสุขภาพจิต
โรงพยาบาลสวนสราญรมย์
สุราษฎร์ธานี

นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาลสวนสราญรมย์

๒๘ กุมภาพันธ์ ๒๕๖๓

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 คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โรงพยาบาลสวนสราญรมย์ จึงจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์ ขององค์กร และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์ และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) จากทุกหน่วยและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้อง กับการพัฒนาของเทคโนโลยีที่เปลี่ยน แปลงไปอย่างรวดเร็ว คณะกรรมการพัฒนาการบริหารจัดการงานสารสนเทศและเวชระเบียน ซึ่งมีหน้าที่ในการดูแล กำกับ ในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร จึงหวังเป็นอย่างยิ่งว่า แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือ ให้กับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสวนสราญรมย์ทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

(นายสุรัติ ลูกรักษ์)
พยาบาลวิชาชีพชำนาญการ
รองประธานคณะกรรมการรักษาความมั่นคงปลอดภัย
ของระบบเทคโนโลยีสารสนเทศ
มีนาคม ๒๕๖๓

สารบัญ

หน้า

คำนำ

หลักการและเหตุผล ๑

วัตถุประสงค์ ๑

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๒

องค์ประกอบของนโยบาย ๒

คำนิยาม ๓

นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ๖

นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ ๗

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ๑๐

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย ๑๓

นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ ๑๕

นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ ๑๗

นโยบายการรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต ๑๙

นโยบายการรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก ๒๑

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล ๒๓

นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ๒๔

นโยบายการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี ๒๕

นโยบายการคุ้มครองข้อมูลส่วนบุคคล ๒๖

นโยบายการปฏิบัติงาน-การประชุมทางไกลจากภายนอกหน่วยงาน (Tele conference) ๒๗

นโยบายการพัฒนาเว็บไซต์ให้เป็นมาตรฐานเว็บไซต์ภาครัฐ ๒๘

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๓๒

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) ๓๓

ภาคผนวก ๔๑

ก คำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ข คำสั่งมอบหมายเจ้าหน้าที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โรงพยาบาลสวนสราญรมย์

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และ แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสุขภาพจิต ปี ๒๕๕๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลสวนสราญรมย์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ โรงพยาบาลสวนสราญรมย์ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๒.๓. นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๕. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิด หรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามแ ละตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๔. เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๓.๕. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. องค์ประกอบของนโยบาย

๔.๑. คำนิยาม

๔.๒. การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๔.๓. การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

๔.๔. การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔.๕. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๔.๖. การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

๔.๗. การรักษาความมั่นคงปลอดภัยของอีเมล์

๔.๘. การรักษาความมั่นคงปลอดภัยของอินเตอร์เน็ต

๔.๙. การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

๔.๑๐. ความมั่นคงปลอดภัยของการสำรองข้อมูล

๔.๑๑.นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๔.๑๒.การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

๔.๑๓.นโยบายการคุ้มครองข้อมูลส่วนบุคคล

๔.๑๔.นโยบายการปฏิบัติงาน-การประชุมทางไกลจากภายนอกหน่วยงาน (Tele conference)

๔.๑๕.นโยบายการพัฒนาเว็บไซต์ให้เป็นมาตรฐานเว็บไซต์ภาครัฐ

๔.๑๖. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๑๗ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของโรงพยาบาลสวนสราญรมย์

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของโรงพยาบาลสวนสราญรมย์ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์สารสนเทศ หมายถึง งานคอมพิวเตอร์และสารสนเทศซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้ คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในโรงพยาบาลสวนสราญรมย์

ผู้อำนวยการศูนย์สารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสวนสราญรมย์ และมีอำนาจตัดสินใจเกี่ยวกับระบบ สารสนเทศภายในโรงพยาบาลสวนสราญรมย์

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสวนสราญรมย์

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่ง โรงพยาบาลสวนสราญรมย์กำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของโรงพยาบาลสวนสราญรมย์ เช่น ผู้อำนวยการโรงพยาบาล รองผู้อำนวยการ เป็นต้น

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

เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานกระทรวงสาธารณสุข เป็นต้น ของโรงพยาบาลสวนสราญรมย์

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลสวนสราญรมย์ อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

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

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำ หน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

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 การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและ การสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาต ให้มีการใช้งานระบบเท คโนโลยีสารสนเทศ โดยแบ่งเป็น พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอม พิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ 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) การห้าม ปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของ ข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

Remote Access หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลสวนสราญรมย์ (ผ่านช่องทางการสื่อสารภายในโรงพยาบาล) หรือ จากภายนอกโรงพยาบาล (ผ่าน Internet

VDO Teleconference หมายถึง การประชุมทางไกล โดยการนำเทคโนโลยีสาขาต่างๆ เช่น คอมพิวเตอร์ เครื่องถ่ายโทรทัศน์ และเครือข่ายอินเตอร์เน็ต เพื่อสนับสนุนในการประชุมให้มีประสิทธิภาพ ถูกออกแบบมาเพื่อให้คนหรือกลุ่ม คน ซึ่งอยู่กันคนละสถานที่สามารถติดต่อกันได้ทั้งภาพและเสียง โดยผ่านทางจอภาพซึ่งอาจเป็นคอมพิวเตอร์หรือโทรทัศน์ ผู้ชมที่ฝั่งหนึ่งจะเห็นภาพของอีกฝั่งหนึ่งปรากฏอยู่บนจอโทรทัศน์ของ

นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้ศูนย์สารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒ ให้ศูนย์สารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓ ให้ศูนย์สารสนเทศกำหนดมาตรการควบคุมการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ
(Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ แนวทางปฏิบัติในการ ควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสวนสราญรมย์ มีดังนี้

๒.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ โรงพยาบาลสวนสราญรมย์ กำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร ต่อผู้อำนวยการศูนย์สารสนเทศ

๒.๑.๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

๒.๑.๔ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๒.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ โรงพยาบาลสวนสราญรมย์ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์

การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๒.๒ ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๒.๒.๓.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๒.๓.๒ ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๒.๓.๓ ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๒.๓.๔ ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบ คอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๒.๓.๕ กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๒.๒.๓.๖ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจาก ผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒.๔ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้า ถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๒.๔.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการ เข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๒.๔.๒ ต้องกำหนดร ายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อ ใช้ในการตรว จสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้น ความลับของข้อมูล

๒.๒.๔.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าว

๒.๒.๔.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการ เข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๒.๒.๔.๕ ควรกำหนดการเปลี่ยน รหัสผ่าน ตามระยะเวลาที่กำหนดของ ระดับความสำคัญของข้อมูล

๒.๒.๔.๖ ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่อง คอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๒.๓.๑ ผู้ใช้บ ริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่าน ในการ เข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๒.๓.๒ ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๒.๓.๓ ผู้ใช้บริการควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

๒.๓.๔ ผู้ใช้บริการควรทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

(Network and Server Policy)

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้บริการ ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. แนวทางปฏิบัติในการใช้งานเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

โรงพยาบาลสวนสราญรมย์ กำหนดมาตรการความปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

๒.๑ ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้สามารถควบคุม ป้องกันการบุกรุกได้อย่างเป็นระบบ โดยจะมีมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

๒.๑.๑ สำหรับผู้ดูแลระบบ ก่อนเข้าห้องเครือข่าย จะต้องการสแกนลายนิ้วมือที่อุปกรณ์หน้าห้องทุกครั้ง เพื่อเป็นการบันทึกประวัติการเข้าใช้งานห้องเครือข่าย

๒.๑.๒ ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร“บันทึกการเข้าออกพื้นที่” และจะต้องมีผู้ดูแลควบคุมตอดเวลา

๒.๒ ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์สารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๒.๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์สารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

๒.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๒.๕ ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๒.๕.๑ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๒.๕.๒ ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

๒.๕.๓ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๒.๕.๔ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๒.๕.๕ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๒.๕.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๒.๕.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๕.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๕.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๒.๖ โรงพยาบาลสวนสราญรมย์ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๒.๖.๑ ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

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

๒.๖.๓ ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๒.๖.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒.๗ โรงพยาบาลสวนสราญรมย์ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตาม

แนวทาง ดังต่อไปนี้

๒.๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่าย และ เครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขอ อนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการศูนย์สารสนเทศ

๒.๗.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๒.๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ อนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการศูนย์สารสนเทศ

๒.๗.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความ จำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๒.๗.๕ การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

๒.๘ โรงพยาบาลสวนสราญรมย์ กำหนดมาตรการการรายงานอุบัติการณ์ที่ไม่พึงประสงค์จากระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายให้ผู้บังคับบัญชาทราบโดยเร็ว ดังนี้

๒.๘.๑ ใช้อุปกรณ์ Send Quick Alert เป็นระบบแจ้งเตือนผ่าน SMS ไปยังมือถือเมื่ออุปกรณ์มีปัญหาใช้งานไม่ได้ ระบบจะส่ง SMS หรือข้อความผ่านโทรศัพท์มือถือให้ผู้ดูแลระบบและผู้บังคับทราบในทันที

๒.๘.๒ รายงานเหตุการณ์ที่เกิดขึ้นในกลุ่มไลน์เทคนิคที่มีผู้บังคับบัญชาและผู้ดูแลระบบแต่ละคนอยู่ในกลุ่ม

นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของโรงพยาบาลสวนสราญรมย์ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

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

๒.๒ ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงาน ไม่ว่าจะเป็น 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 มาจาก โรงงานผลิตทันทีที่นำ 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 (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๒.๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๒.๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์สารสนเทศทราบทันที

นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่างๆให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในองค์กร

๒. แนวทางปฏิบัติในการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์(Firewall) ของโรงพยาบาลสวนสราญรมย์ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้ศูนย์สารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมดของโรงพยาบาลสวนสราญรมย์

๒.๑ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๒.๒ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตาม นโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

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

๒.๔ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่า ใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๒.๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๒.๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๒.๗ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางโรงพยาบาลสวนสราญรมย์ อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศ ก่อน

๒.๘ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรือ

อุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์สารสนเทศ โดยต้องระบุข้อมูลดังนี้

๒.๘.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๒.๘.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒.๘.๓ วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

๒.๘.๔ วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

๒.๙ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๒.๑๐ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๒.๑๑ โรงพยาบาลสวนสราญรมย์ มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของโรงพยาบาลสวนสราญรมย์ หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๒.๑๒ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของโรงพยาบาลสวนสราญรมย์ หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของหน่วยงาน ทางศูนย์สารสนเทศจะยกเลิกการให้บริการทันที

๒.๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากโรงพยาบาลสวนสราญรมย์ก่อน

นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนัก ถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมาย อิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของโรงพยาบาลสวนสราญรมย์ มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์สารสนเทศโรงพยาบาลสวนสราญรมย์

๒.๑ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

๒.๒ ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๒.๓ ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๒.๔ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

๒.๕ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของโรงพยาบาลสวนสราญรมย์ ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลสวนสราญรมย์เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบ จดหมายอิเล็กทรอนิกส์ของโรงพยาบาลสวนสราญรมย์ ขัดข้องและได้รับการอนุญาต จากผู้บังคับบัญชาแล้วเท่านั้น

๒.๖ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่นยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของโรงพยาบาลสวนสราญรมย์ หรือก่อให้เกิดความเสียหายต่อโรงพยาบาลสวนสราญรมย์

๒.๗ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของโรงพยาบาลสวนสราญรมย์ เพื่อเผยแพร่ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของโรงพยาบาลสวนสราญรมย์ ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของโรงพยาบาลสวนสราญรมย์

๒.๘ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๙ การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน ๑๐ เมกะไบท์

๒.๑๐ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

นโย บายการรักษาค วาม มั่น คง ปล อดภัย ของ อินเต อร์เน็ต

(Internet Security Policy)

๑.

วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานอินเตอร์เน็ตของโรงพยาบาลสวนสราญรมย์ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์กระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเตอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการใช้เครือข่ายอินเตอร์เน็ต

ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของโรงพยาบาลสวนสราญรมย์ มีหน้าที่และความรับผิดชอบที่ ต้องปฏิบัติ ดังนี้

๒.๑ การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเตอร์เน็ตของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้างานคอมพิวเตอร์และสารสนเทศ โรงพยาบาลสวนสราญรมย์ โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดโรงพยาบาลสวนสราญรมย์ สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศหรือผู้ที่ได้รับมอบหมาย และก่อนเข้าใช้งานอินเตอร์เน็ตจะต้องยืนยันตัวบุคคลเข้าใช้งาน (Authentication) ทุกครั้ง เพื่อให้เป็นไปตาม พรบ. คอมพิวเตอร์ ๒๕๖๐

๒.๒ ไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือ ภาพที่มีลักษณะอันลามกและไม่ทาการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

๒.๓ ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๒.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๖ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

๒.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๘ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากการใช้งาน เครือข่ายอินเตอร์เน็ตด้วยการ Logout จากการ Authentication เพื่อป้องกัน การเข้าใช้งานโดยบุคคลอื่นๆ

๒.๙ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๒.๑๐ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๒.๑๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น และต้องแบ่งประเภทการใช้งานอินเทอร์เน็ต เป็นกลุ่มใช้งานทั่วไป กับกลุ่มปฏิบัติงานสำคัญในองค์กร

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

๑. วัตถุประสงค์

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาลสวนสราญรมย์ ให้มีความมั่นคงปลอดภัย

๒. แนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย

แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย เป็นดังนี้

๒.๑ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของโรงพยาบาลสวนสราญรมย์และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ใน เครือข่ายอินเทอร์เน็ตทุกเส้นทาง

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 จะต้องมีการรายงานให้ผู้ ประธาน และกรรม คณะกรรมการ รักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๒.๑๑ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๒.๑๒ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๒.๑๓ โรงพยาบาลสวนสราญรมย์ มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๒.๑๔ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลสวนสราญรมย์ การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิด ความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลสวนสราญรมย์ จะต้อง ถูกดำเนินคดีตามขั้นตอนของกฎหมาย

นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล
(Backup Policy)

๑.
วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๒. แนวทางปฏิบัติในการสำรองข้อมูล

๒.๑ จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตาม ลำดับความจำเป็น ของการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

๒.๒ มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบเทคโนโลยีสารสนเทศ โดยขั้นตอนปฏิบัติแยก ตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

๒.๓ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูล นั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลแ ละผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๔ กำหนดให้มีการสารองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสารองข้อมูล หา กระบบใดที่มีการเปลี่ ยนแปลงบ่อยกำ หนดให้มีความถี่ในการสารองข้อมูลมากขึ้น โดยให้มีวิธีการสารองข้อมูล

๒.๕ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบ กลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๖ แนวทางการปฏิบัติ สำหรับสำรองข้อมูลระบบบริการผู้ป่วยของผู้ดูแลระบบ มีดังนี้

๒.๖.๑ ระบบฐานข้อมูลโปรแกรมพัฒนาบริการผู้ป่วยจิตเวช HIS โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลโดยอัตโนมัติ ไปยังเครื่อง Server Backup ทุกวัน

๒.๖.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรองข้อมูล ทั้งจัดให้มีระบบการบำรุงรักษา (Restructure/Reformat) ระบบฐานข้อมูลตามระยะเวลาที่กำหนด ดังนี้

๑.การสำรองข้อมูลประจำวัน จะทำการสำรองข้อมูลและโครงสร้างข้อมูลอัตโนมัติทุกเที่ยงคืน)

๒.การสำรองข้อมูลประจำสัปดาห์ จะทำการสำรองข้อมูล โครงสร้างข้อมูลและ Source Code โดยบันทึกข้อมูลลงใน External Hard disk

๓.การสำรอง Source Code โปรแกรมประจำเดือน

๔.การสำรองข้อมูลประจำปี (การสำรองข้อมูลด้วยระบบ Manual)

นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application and Information Access Control Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตร การใน การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ของโรงพยา บาลสวนสราญรมย์ และสร้างแนวทางป้องกัน โดย ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์กระทำการใ ดๆ ที่จะสร้างปัญ หา หรือไม่เคารพ กฎเกณฑ์ที่วางไว้จนนำมาซึ่งปัญหาที่ทำให้ระบบบริการผู้ป่วยต้องหยุดให้บริการ

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒.๑ ผู้ดูแลระบบ ต้องกำ หนดการลงทะเบียนผู้ใช้งา นใหม่ ในการใช้งานตามค วามจาเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก เป็นต้น

๒.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) โดยโรงพยาบาลจะให้ความกับโปรแกรมบริการงานผู้ป่วย (HIS) และระบบเรียกรายงานตามตัวชี้วัดต่างๆ

๒.๓ ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

๒.๔ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทาลายข้อมูลแต่ละประเภทชั้นความลับ โดยกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

๒.๕ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นาสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดาเนินการสารองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

นโยบายการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

(Software Licensing and intellectual property

and Preventing MalWare Policy)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการใน การบริหารจัดการซอฟต์แ วร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี ให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการป้องกัน และไม่ละเมิดสิทธิ์กระทำการใดๆ ที่อาจก่อให้เกิดผลกระทบต่อระบบคอมพิวเตอร์

๒. แนวทางปฏิบัติใน การในการบริหารจัดการซอ ฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

๒.๑ โรงพยาบาลสวนสราญรมย์ ได้ให้ความสำ คัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจาเป็น และห้ามไม่ให้ผู้ใช้งานทาการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๒.๒ ซอฟต์แวร์ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ ใช้งาน ถือเป็นสิ่งจาเป็นต่อการทำ งานห้ามมิให้ผู้ใช้งานทาการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทาสาเนาเพื่อนาไปใช้งานที่อื่น ๆ

๒.๓ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมปูองกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่หน่วยงานได้ประกาศให้ใช้

๒.๔ ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนามาใช้งานหรือเก็บบันทึกทุกครั้ง

๒.๕ ผู้ใช้งานต้องทาการปรับปรุงข้อมูล สาหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการปูองกันความเสียหายที่อาจเกิดขึ้น

๒.๖ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๒.๗ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๒.๘ ห้ามทาการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

(Personal Data Protection Policy)

๑. วัตถุประสงค์

กำหนดมาตรการหรือแนวทางการดำ เนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ของผู้ใช้บริการโรงพยาบาลสวนสราญรมย์ เพื่อให้เป็นไปตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ๒๕๖๒ โดยเจ้าหน้าที่ผู้ใช้งาน และผู้รับบริการจะต้องเข้าใจกฎเกณฑ์ รวมถึงแนวทางปฏิบัติสำหรับผู้ดูแลระบบ

๒. แนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

๒.๑ เจ้าหน้าที่ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๒.๒ เจ้าหน้าที่ผู้มีหน้าที่เก็บข้อมูลจะต้องทำ การแจ้งรายละเอียด และแจ้งสิทธิต่อเจ้าของข้อมูล ให้ทราบทุกครั้ง

๒.๓ เจ้าหน้าที่ต้องได้รับความยินยอมจากผู้รับ บริการก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล หรือหากผู้ให้ข้อมูลเป็นผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ แต่ในกรณีที่ผู้มีอายุไม่ถึงสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

๒.๔ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ ให้ขอความยินยอมจากผู้อนุบาล

๒.๕ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ ให้ขอความยินยอมจากผู้พิทักษ์

๒.๗ ต้องให้ความเป็นอิสระในการให้ความยินยอมกับเจ้าของข้อมูล

๒.๖ เจ้าหน้าที่ที่เกี่ยวข้องการออกแบบแบบฟอร์มความยินยอม (consent form) ต้องแยกส่วน ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง

๒.๗ เจ้าของข้อมูลส่วนบุคคลมีอำนาจในการถอนความยินยอมเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเมื่อได้ก็ได้ เว้นแต่มีข้อจำกัดสิทธิ

๒.๘ ผู้ดูแลระบบจะต้องทำการ รักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ไม่ให้มีก ารเปลี่ยนแปลงแก้ไข หรือเข้าถึงโดยผู้ที่ไม่เกี่ยวข้อง

๒.๙ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือทำผ่านระบบอิเล็กทรอนิกส์ โดยโรงพยาบาลสวนสราญรมย์มีแนวทางปฏิบัติดังนี้

๒.๙.๑. เจ้าหน้าที่นำหนังสือใบยินยอมเปิดเผยข้อมูลส่วนบุคคลใส่แฟ้มประวัติของผู้ป่วย

๒.๙.๒. เจ้าหน้าที่นำใบยินยอมเปิดเผยข้อมูลส่วนบุคคลของแต่ละรายสแกนไฟล์ในรูปแบบ PDF ไฟล์ แล้วนำเข้าระบบอัพโหลดจัดเก็บไฟล์เอกสารยินยอม โรงพยาบาลสวนสราญรมย์ ซึ่งจะออกแบบไว้รองรับใบยินยอมเปิดเผยข้อมูลของแต่ละระบบบริการ ดังนี้ด้วย

๑.ระบบ H๔U ๒.ระบบ tele-conference

๓.ระบบรับยาร้านยาใกล้บ้าน ๔.ระบบยินยอมใช้ยานอกบัญชี

นโยบายการปฏิบัติงานการประชุมทางไกลจากภายนอกหน่วยงาน
(Tele Conference Policy)

๑. วัตถุประสงค์

กำหนดมาตรการหรือแนวทางการดำ เนินการเกี่ยวกับ การปฏิบัติงาน หรือการประชุมทางไกล จากภายนอกหน่วยงาน เพื่อให้เป็นแนวทางวิธีในการประชุมทางไกล รว มถึงการกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำ ของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด

๒. แนวทางปฏิบัติในการปฏิบัติงาน-การประชุมทางไกลจากภายนอกหน่วยงาน

๒.๑ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้ องกันไวรัสและกา รใช้งานไฟร์วอลล์ตามที่หน่วยง านกำหนด

๒.๒ ผู้ดูแลระบบจะ ต้องมีการจัดเตรียมอุปกรณ์ และห้องปฏิบัติการ สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

๒.๓ ผู้ใช้งานจะต้องใช้โปรแกรมประยุกต์สำหรับการ Tele Conference ที่ผู้ดูแลระบบจัดเตรียมไว้ให้แล้วเท่านั้น เช่น Session Call , line , skype เป็นต้น

๒.๔ ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๒.๕ ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

๒.๖ ต้องกำหนดชนิดของงาน ชั่วโมงการทางาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

๒.๗ ต้องกำหนดขั้นตอนปฏิบัติสาหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

นโยบายการพัฒนาเว็บไซต์ให้เป็นมาตรฐานเว็บไซต์ภาครัฐ

(Government Website Standard **Policy)**

๑. วัตถุประสงค์

กำหนดมาตรการ พัฒนาเว็บไซต์โรงพยาบาล สวนสราญรมย์ให้เป็นไปตามมาตรฐานเว็บไซต์ภาครัฐ (Government Website Standard) ตามแนวทางการพัฒนาเว็บไซต์ที่ทุกคนเข้าถึงได้ Web Accessibility และปรับปรุงโครงสร้างเว็บ ไซต์ให้มีความชัดเจน ง่ายต่อการเข้าใจที่ช่วยให้ผู้ ใช้งานค้นหาข้อมูลได้ง่าย และรองรับการใช้งานกับทุกอุปกรณ์ที่ใช้งาน

๒. แนวทางปฏิบัติในการพัฒนาเว็บไซต์ให้เป็นมาตรฐานเว็บไซต์ภาครัฐ

มาตรฐานเว็บไซต์ภาครัฐ หรือ Government Web Site Standard เป็นมาตรฐานสำหรับเว็บไซต์หน่วยงานภาครัฐ เพื่อให้เป็นเว็บไซต์ภาครัฐของประเทศไทย มีมาตรฐานเดียวกันและเป็นมาตรฐานสากล และจะเป็นการยกระดับการพัฒนา e-Government ให้ก้าวหน้าสู่ระดับสากลต่อไป โดยเนื้อหาจะกล่าวถึงเนื้อหาของเว็บไซต์ Contents คุณลักษณะของเว็บไซต์ภาครัฐที่ควรจะมี) Recommended Features) รวมถึงแนวทางการรักษาความมั่นคงปลอดภัยสารสนเท Information Security ซึ่งได้รวบรวมและประมวลจากกฎหมาย ระเบียบ ข้อบังคับในประเทศที่เกี่ยวข้องกับการทำธุรกรรมอิเล็กทรอนิกส์ การคุ้มครองข้อมูลส่วนบุคคล และข้อกำหนดองค์การสหประชาชาติ)United Nations) ในการจัดอันดับการพัฒนา e-Government ของกลุ่มประเทศสมาชิก ตลอดจนแนวทางปฏิบัติที่ดีที่สุดในระดับนานาชาติ (International Best Practice) โดยมาตรฐานเว็บไซต์ภาครัฐนี้ จัดทำโดย สำนักงานรัฐบาลอิเล็กทรอนิคส์)http://www.ega.or.th ตามหลักการที่กล่าวว่า “ที่เดียว ทันใด ทั่วไทย ทุกเวลา ทั่วถึง เท่าเทียม และธรรมาภิบาล” มาตรฐานประกอบด้วย ด้านเนื้อหา เว็บไซต์ภาครัฐว่าเนื้อหาของเว็บไซต์ควรมีการเผยแพร่ผ่านเว็บไซต์ภาครัฐ เพื่อให้บริการกับประชาชน ตลอดจนหน่วยงานภาครัฐ โดยแบ่งออกเป็น ๓ ส่วน ดังนี้

๑. ข้อมูลพื้นฐาน

๑. เกี่ยวกับหน่วยงาน
๒. ข้อมูลผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)CIO)
๓. ข่าวประชาสัมพันธ์
๔. เว็บลิงค์
๕. กฎ ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับหน่วยงาน
๖. ข้อมูลการบริการ
๗. แบบฟอร์มที่ให้ดาวน์โหลดได้)Download Formats)
๘. คลังความรู้
๙. คำถามที่ถามบ่อย)FAQ)
๑๐. ผังเว็บไซต์)Site map)

.๒การสร้างปฏิสัมพันธ์กับผู้ใช้บริการ

๑. ถาม) ตอบ-Q&A)
๒. ระบบสืบค้นข้อมูล)Search)
๓. ช่องทางการติดต่อสื่อสารกับผู้ใช้บริการ
๔. แบบสำรวจออนไลน์

๓. การให้บริการในรูปแบบอิเล็กทรอนิคส์)e-Service)

๑. การลงทะเบียนออนไลน์)Register Online)

๒. e-Forms / Online Forms

๓. ระบบให้บริการในรูปแบบอิเล็กทรอนิคส์)e-Service)

๔. การให้บริการเฉพาะบุคคล)Personalized e-Service)

คุณลักษณะที่ควรมีเรื่องหนึ่ง คือ ข้อกำหนดมาตรฐาน

ข้อกำหนดมาตรฐาน

- เว็บไซต์ควรสอดคล้องกับข้อกำหนดขององค์การมาตรฐาน เวิลด์ ไวด์ เว็บ)World Wide Web Consortium: W๓C) คณะริเริ่มดำเนินการทำให้เว็บเข้าถึงและใช้ประโยชน์ได้)Web Accessibility Initiative: WAI) ตามข้อกำหนดการทำให้เนื้อหาเว็บสามารถเข้าถึงและใช้ประโยชน์ได้ รุ่น ๒.๐ (Web Content Accessibility Guidelines ๒.๐ : WCAG ๒.๐) ในเกณฑ์ความสำเร็จ ระดับ เอ)A)
- สำหรับประเทศไทย สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยสำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและสารสื่อสารได้มีการจัดทำรูปแบบการพัฒนาเว็บไซต์ให้เป็นเว็บไซต์ที่ทุกคนสามารถเข้าถึงได้และเกณฑ์มาตรฐานฉบับภาษาไทยขึ้น ภายใต้ชื่อ “Thai Web Content Accessibility Guidelines ๒๐๑๐ (TWCAG ๒๐๑๐)”
- เว็บไซต์ควรสอดคล้องกับข้อกำหนดของ W๓C สำหรับ HyperText Markup Language (HTML) อย่างน้อย HTML ๔.๐๑
- หากเว็บไซต์ใช้ Cascading Style Sheets (CSS) ควรสอดคล้องกับข้อกำหนดของ W๓C สำหรับ CSS ระดับ ๑

การพัฒนาเว็บไซต์ให้ปลอดภัย) Web Security(สำหรับผู้ดูแลระบบมีรายละเอียดดังนี้

1. **Remote Code Execution** ป้องกันการโจมตีระยะไกลด้วยคำสั่ง Shell Script

คือการรันคำสั่งการโจมตีระยะไกล คำว่าระยะอาจจะเป็นการรั นคำสั่งเพื่อโจมตีเว็บไซต์จากอีก server หนึ่ง หากว่าไม่มีการป้องกันและตรวจสอบว่าคำสั่งนั้นเกิดขึ้นจาก location เดียวกับเว็บไซต์เราหรือไม่สำหรับเว็บไซต์โรงพยาบาลสวนสราญรมย์พัฒนาด้วยภาษา PHP ใช้codeigniter Frameworkซึ่งมีวิธีป้องกันการโจมตีระยะไกลจาก Shell Script ที่ดี คือทุก ๆ ไฟล์ .php ของ codeigniter จะถูกเขียนกำกับไว้ในบรรทัดแรกเพื่อตรวจสอบแหล่งที่มาของ script คำสั่งการทำงานต่าง ๆ ก่อนที่จะเริ่มต้นทำงานในไฟล์ .php

2. **SQL injection** ป้องกันการโจมตีด้วยคำสั่ง SQL

คือการโจมตีเว็บไซต์โดยการส่งคำสั่ง SQL เข้าไปใน input ต่าง ๆ ภายในเว็บไซต์ สำหรับ php codeigniterมีการป้องกันการโจมตีแบบนี้อยู่แล้ว เพียงแต่ต้องใช้คำสั่งในการ Query ของ Codeiginiter โดยถ้าหากว่าใช้การรับค่าตัวแปรผ่านเมธอดของเฟรมเวิร์ค ตัวเฟรมเวิร์คจะทำการ validate XSS ข้อมูลทั้งแบบ get และ post ให้อัตโนมั ติเช่น เมื่อมีการส่งค่าตัวแปรมาแบบ post ควรที่จะใช้การรับค่าตัวแปรใน controller ด้วยเมธอด **$this->input->post(‘ตัวแปร ’);**แทนที่จะไปรับค่าแบบ $_POST หรือ $_REQUEST และเมื่อมีการ query ข้อมูลก็ควรที่จะใช้คำสั่งของ CI เอง เช่นใช้ $this->db->escape() ครอบตัวแปรก่อนจะทำการ select ข้อมูลโดยกระบวนการข้างต้นที่กล่าวมาการ ใช้งาน Global XSS Filtering ป้องกันการโจมตีแบบ XSS

การพัฒนา เว็บไซต์โรงพยาบาลสวนสราญรมย์พัฒนาด้วย codeigniter framework (PHP)มีระบบป้องกันการโจมตีแบบ XSS คือการฝังโค๊ดสคริปต์ต่าง ๆ ส่ง เข้ามาให้ controllerก่อนส่งออกไปที่ front end ทำการแสดงผล ถ้ามี script อันตรายติดมาด้วย script ก็จะเริ่มทำงานทันทีเมื่อเราเปิดใช้งาน Global XSS Filtering ซึ่งอยู่ในไฟล์ **application ส่วนของ config** แล้วระบบจะทำการกรองข้อมูลต่าง ๆ ที่ส่งเข้ามาทั้งแบบ get และ post ให้อัตโนมัติ ด้วยการเปิดใช้งานคำสั่ง

3. **เปิดใช้งาน CSRF Protection** ตรวจสอบ cookie อันตรายจากไซต์อื่น

เป็นการป้องกันการโจมตีแบบ CSRF Cross Site Request Forgery ที่อาศัยการทำงานของ cookie ในเครื่องของ userในการโจมตีเป็นหัวใจสำคัญ ซึ่งทำการกำหนดตัวแปร token และตรวจสอบข้อมูลรูปแบบนี้ในทุก ๆ ครั้งที่มีการ submit form data. การพัฒนาเว็บไซต์ของ ร พัฒนาโดย.พ.เปิดการใช้งานคุณสมบัตินี้

4. ความปลอดภัยของ URI

URI คือ ข้อมูลที่ใช้ระบุตัวตนของทรัพยากร)resource)โดยที่ resource อาจจะเป็น data, image, file, service, website, หนังสือ, คน หรือ หน่วยงาน ก็ได้เรียกว่าอะไรก็ได้ เอามาระบุตัวตน)identify) โดยทำให้ออกมาเป็นรูปแบบเดียวกัน)uniform)

การพัฒนาเว็บไซต์ โรงพยาบาลสวนสราญรมย์ ด้วย CodeIgniter จำกัดตัวอักษรบางอย่างซึ่งตัวอักษรนั้นถูกยอมรับใน URI เพื่อช่วยในการลดข้อมูลที่มุ่ งร้าย ที่จะสามารถผ่านไปยังแอพพลิเคชั่นของร.พ.ได้ URIs สามารถใช้ได้ดังต่อไปนี้:

ตัวอักษรและตัวเลข -

- Tilde: ~- Period: .

- Colon: :- Underscore: _

- Dash: -

5. การกำหนดสิทธิ์การเข้าใช้งานเว็บไซต์โรงพยาบาลสวนสราญรมย์

การพัฒนาระบบจะแบ่งสิทธิ์การเข้าใช้งานหลัก ๆ อยู่ ระดับ ดังนี้ 3

- Super Admin
- Admin
- User

โดยที่ Super Adminสามารถจัดการเว็บไซต์ได้ทั้งระบบ และดูตรวจ Even ต่างๆ ที่เกิดขึ้นได้ และ ผู้ใช้งานระดับ Admin จะเป็นผู้ใช้งานจากหน่วยงาน หรือฝ่าย ที่ได้รับสิทธิ์ให้เข้าจัดการข้อมูล ได้เฉพาะบางโมดูลของระบบงานนั้น ผู้ใช้งานระดับ User คือผู้เยี่ยมชมทั่วไปที่สมัครสมาชิกเข้ามาเพื่อถามคำตามหรือตอบคำถามในส่วนของเว็บบอร์ด (ตอบ-ถาม)

6. มาตรฐานการรักษาความปลอดภัยสำหรับการเข้าใช้งานและการบันทึก มีดังนี้

1. Authentication สามารถตรวจสอบตัวตนโดยการใช้ Username และ Password ได้
2. Authorization สามารถกำหนดสิทธิ์ให้กับผู้ใช้ระบบแต่ละคน ได้หลายระดับแตกต่างกันในแต่ฟังก์ชั่นการทำงาน
3. Confidentiality สามารถทำ data hashing หรือ encryption การเข้ารหัสผ่านของผู้ใช้ก่อนเก็บลงฐานข้อมูล
4. Non-repudiation สามารถบันทึก Audit log การบันทึก/แก้ไข และการเข้าใช้งานระบบได้
5. ระบบสามารถจัดการ section ให้ logout ออกจากระบบทันที เมื่อผู้ใช้ไม่ได้ใช้งานต่อเนื่องเป็นเวลา นาที เพื่อป้องกันการลืม 30 logout และอันตรายอื่นๆที่อาจเกิดขึ้น

7. การเก็บ Log เข้าใช้งานของผู้ใช้งาน

ในการพัฒนาเว็บไซต์โรงพยาบาลสวนสราญรมย์จะมีเก็บประวัติการเข้าใช้งานทั้งหมดของผู้ที่มีสิทธิ์ให้เข้าจัดการเว็บไซต์ได้และเก็บผู้ใช้งานทุกระบบ เพื่อเป็นตรวจสอบข้อมูลภาพหลังและการป้องกันการไม่หวังดี โดยระบบจะกำหนดการเข้าใช้งานต่อวันไม่เกิน ครั้ง ถ้าเกินกว่าน 20ั้นจะบล็อก IP เพื่อป้องกันการเจาะระบบ และแสดงรายการการเข้าใช้งานดังภาพ

8. การจัดทำ Web Stats ระบบรายงาน สถิติเว็บไซต์ แบบ Realtime พร้อมข้อมูลสถิติ

การพัฒนาเว็บไซต์โรงพยาบาลสวนสราญรมย์ พัฒนาโดยนำส่วนของ Web Stats มาใช้งาน เพื่อดูความเคลื่อนไหวเผ้าติดตามผู้ใช้งาน ใช้ในการตรวจสอบและวิเคราะห์เชิงลึก โดยมีกระบวนการต่าง ๆ ดังนี้

- รายงาน สถิติผู้เข้าชมเว็บไซต์ โดยละเอียด รายชั่วโมง รายวัน รายเดือน รายปี ในรูปแบบกราฟ แผนภูมิแท่ง และตาราง
- รายงาน ข้อมูลผู้เข้าชม แหล่งที่มา ไอพี ไอเอสพี ประเทศ ระบบที่ใช้
- รายงาน ข้อมูลสถิติ การเปิดชมเพ็จ)Pageview)/จำนวนผู้เข้าชม ราย)Session/UIP)
- Keyword แยกตาม search engine ตามโดเมน พร้อมแสดงอันดับเพ็จบนเซิร์จเอ็นจิ้น ที่เว็บไซต์ท่านแสดง
- Robot Access หรือ สถิติการเก็บข้อมูลของ Spiders/Robots โดยทำการแสดงจำนวนครั้งและวันที่ล่าสุด

(เพิ่มเติม)ลิงค์ภายใน / อื่นลิงค์ที่ออกไปยังเว็บไซต์ / ลิงค์ ที่เชื่อมโยงมายังเว็บไซต์ของท่าน -

- Click Area (พื้นที่คลิกเพิ่มเติ)แสดงพื้นที่ภาพรวม ที่ผู้เข้าเว็บไซต์ชอบคลิก (ม(

โดยแสดงรายละเอียดบางส่วนดังภาพด้านล่างนี้

๙. การสำรองฐานข้อมูลระบบเว็บไซต์โรงพยาบาล และโปรแกรมเว็บไซต์โรงพยาบาล

1. การสำรองฐานข้อมูล**ระบบเว็บไซต์โรงพยาบาล**ผู้ดูแลระบบจะตั้งค่าการสำรองบน Server ผู้ให้บริการให้สำรองข้อมูลทุก 1 อาทิตย์

2. การสำรองฐานข้อมูลโปรแกรม**เว็บไซต์โรงพยาบาล**ผู้ดูแลระบบจะตั้งค่าการสำรองบน Server ผู้ให้บริการให้สำรองข้อมูลทุก 1 เดือน

3. ผู้ดูแลระบบอาจสำรองฐานข้อมูลและโปรแกรมผ่านการเข้า FTP File เพื่อทำการสำรองข้อมูลตามควมถี่ที่ต้องการ

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจน สามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรืองการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือ ข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวแนวปฏิบัติป้องกันความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและการสื่อสารสำหรับโรงพยาบาลสวนสราญรมย์ขึ้น โดยยึดหลักตามแผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมสุขภาพจิตฉบับปัจจุบัน ซึ่งประกาศใช้เมื่อวันที่ 1 มิถุนายน 2562 เป็นหลัก เพื่อใช้เป็นแนวปฏิบัติ สำหรับบุคลากรที่ปฏิบัติงานทางด้านสารสนเทศ และผู้เกี่ยวข้องทุกคนในโรงพยาบาลสวนสราญรมย์ต่อไป

๒. แนวทางปฏิบัติในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๑.วัตถุประสงค์

บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒.ผู้รับผิดชอบ

๒.๑ คณะกรรมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒.๒ คณะกรรมบริหารความเสี่ยง

๓ คำจำกัดความ

๓.๑ ความเสี่ยง (Risk) หมายถึง โอกาสที่จะประสบกับความสูญเสียหรือสิ่งที่ไม่พึงประสงค์ด้านเทคโนโลยี สารสนเทศและการสื่อสาร

๓.๒ บุคลากรทุกคน หมายถึง ผู้ใช้งานคอมพิวเตอร์ในระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาลสวนสราญรมย์

๓.๓ ระบบเครือข่ายคอมพิวเตอร์ หมายถึง ระบบงานซึ่งเชื่อมโยงคอมพิวเตอร์ต่าง ๆ ในองค์กรเข้าด้วยกัน เพื่อประโยชน์ในการใช้ทรัพยากรร่วมกัน ซึ่งประกอบด้วย คอมพิวเตอร์แม่ข่าย ลูกข่าย ระบบเชื่อมต่อสัญญาณ และระบบปฏิบัติการที่ใช้ในโรงพยาบาลสวนสราญรมย์

๓.๔ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ หมายถึง ผู้ปฏิบัติงานในงานคอมพิวเตอร์และสารสนเทศที่มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงาน

๓.๕ Hardware หมายถึง อุปกรณ์ต่าง ๆ ที่นำมารวมกันเข้าให้กลายเป็นครุภัณฑ์คอมพิวเตอร์ ซึ่งแบ่งเป็น ๓หน่วยใหญ่ ๆ ได้แก่ หน่วยรับข้อมูล เช่น แป้นพิมพ์ (Key board) หน่วยความจำ เช่น Chip จานบันทึก(Hard disk) และหน่วยแสดงผล เช่น จอภาพ (Monitor) เครื่องพิมพ์ (Printer) ฯลฯ นอกนี้ยังมีอุปกรณ์ประกอบอื่น ๆ เช่น Modem Switch เป็นต้น

๓.๖ Software หมายถึง โปรแกรมคอมพิวเตอร์ หรือชุดคำสั่งต่าง ๆ ที่ทำให้คอมพิวเตอร์ทำงานได้ ซึ่ง นำมาใช้กับโรงพยาบาลสวนสราญรมย์ เช่นระบบบริการงานผู้ป่วยจิตรเวช (HIS)

๓.๗ อุปกรณ์ต่อพ่วง หมายถึง เครื่องมือหรืออุปกรณ์ที่ใช้ทำงานร่วมกับเครื่องคอมพิวเตอร์ ได้แก่ UPS (เครื่องควบคุม และสำรองไฟฟ้าสำหรับคอมพิวเตอร์) SCANNER อุปกรณ์รักษาความปลอดภัยแก่ระบบ ฯลฯ

๓.๘ เจ้าหน้าที่พัฒนาข้อมูลและสารสนเทศ หมายถึง บุคลากรที่ปฏิบัติงานประจำฝ่ายแผนงานและสารสนเทศ เช่น หัวหน้าศูนย์สารสนเทศฯ หรือหัวหน้าศูนย์ข้อมูล ผู้ดูแลระบบเครือข่าย และบุคลากรที่ปฏิบัติงานด้านข้อมูล ตามคำสั่งแต่งตั้งของผู้อำนวยการโรงพยาบาลสวนสราญรมย์

๓.๙ การบันทึกข้อมูลที่สำคัญ (ตามภารกิจ) ลงใน Data Center หมายถึง การนำข้อมูลที่สำคัญตามภารกิจของแต่ละหน่วยงานไปจัดเก็บไว้ในเครื่อง Server กลางของหน่วยงาน เช่น ข้อมูลผู้ป่วยจิตเวช, ข้อมูลที่สำคัญตามภารกิจ ลงใน เครื่องคอมพิวเตอร์กลาง

๔. วิธีปฏิบัติงานควบคุมความเสี่ยงในระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของโรงพยาบาลสวนสราญรมย์

๔.๑ การควบคุมห้อง Server ประเภทของงาน การควบคุมห้อง Server แบ่งออกเป็น ๒ ลักษณะ คือ

(๑) ห้องศูนย์ปฏิบัติการคอมพิวเตอร์

(๒) จัดกั้นพื้นที่เป็นการเฉพาะ

วิธีปฏิบัติ

(๑) ผู้อำนวยการโรงพยาบาลสวนสราญรมย์ ลงนามในเอกสารมอบหมายหรือคำสั่งแต่งตั้งหรือกำหนดตารางการปฏิบัติงานของ Administrator ประจำวัน ให้มีหน้าที่ควบคุมดูแลห้อง Server ตลอดจนการปฏิบัติการดูแลเครื่อง Server

(๒) เจ้าหน้าที่พัฒนาข้อมูลและสารสนเทศ ประกาศเขตพื้นที่ห้ามบุคคลภายนอกที่ไม่มีส่วนเกี่ยวข้องเข้า ไปในบริเวณห้อง Server ให้ชัดเจน เช่น การขีดเส้นสีแสดงสัญลักษณ์ไว้หน้าประตูเข้าห้อง หรือมีกุญแจ Key card ในการเข้าออกห้อง Server หรือสัญลักษณ์อย่างอื่นเช่น นำตู้มากั้น ฯลฯ

(๓) กรณีบุคคลภายนอกหรือบุคคลอื่นนอกเหนือจาก Administrator ที่มีหน้าที่รับผิดชอบในแต่ละวัน มีความจำเป็นต้องเข้าไปภายในห้อง Server จะต้องขออนุญาตจาก Administrator ประจำวัน และจะต้องลงชื่อใน รายการกิจกรรมที่ปฏิบัติภายในห้อง Server ในแบบบันทึกขอเข้าห้อง Server ๐๘๐๔-๔๐๑-๐๒๘หรือแบบบันทึกอื่นๆ ที่ หน่วยงานกำหนด

(๔) Administrator ประจำวันหรือผู้ที่ Administrator มอบหมายจะต้องเข้าไปพร้อมกับบุคคลภายนอกในการเข้าปฏิบัติงานภายในห้อง Server ด้วยทุกครั้ง

(๕) กรณีที่ต้องอนุญาตให้บุคคลภายนอกเข้าห้อง Server เช่น ทำความสะอาดห้อง , ตรวจเช็คและ Maintenance ระบบงานที่ห้อง Server เช่น ซ่อม ปรับปรุงระบบไฟฟ้า เครื่องปรับอากาศ/เพิ่มเติมอุปกรณ์ระบบ เครือข่ายเช่น Fiber Optic,สาย UTP, Switching, Router, Modem เป็นต้น จะต้องลงชื่อในแบบฟอร์มที่หน่วยงาน กำหนด

(๖) ความถี่ในการปฏิบัติทุกวันทำการ หรือทุกครั้งที่เข้าไปปฏิบัติงานภายในห้องServer

(๗) ช่วงเวลาที่ปฏิบัติช่วงเช้าของวันทำการ และวันหยุดตามเวรปฏิบัติงาน

(๘) การบันทึกผลการปฏิบัติแบบบันทึกตามที่หน่วยงานกำหนด

๔.๒ การควบคุม ดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย)Server) ประเภทของ Server แบ่งออกเป็น ๒ ประเภท คือ

(๑) Server ที่สำคัญที่จะใช้กับ(ระบบบริการงานผู้ป่วยจิตเวช ระบบงานรังสีวิทยา ระบบงานชันสูตร)

(๒) Server ทั่วไป

วิธีปฏิบัติ

(๑) Administrator ประจำวัน มีหน้าที่ปฏิบัติการดูแลและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่แต่ละหน่วยงานมีอยู่ เช่น)Data Center,Proxy Server, Web Server, Database Server, Mail Server ฯลฯ และอุปกรณ์บริหารจัดการเครือข่าย (

(๒) ตรวจสอบการทำงานของเครื่อง ดูไฟแจ้งเตือนสถานะทำงานทุกวันทำการ

(๓) ทำความสะอาดภายนอกสัปดาห์ละครั้ง อาจใช้ไม้ขนไก่ปัดฝุ่น

(๔) ตรวจสอบการทำงานของอุปกรณ์ที่เกี่ยวข้อง เช่น สายเชื่อมต่อ, อุปกรณ์เครือข่าย เช่น Switch, Hub, Access Point, UPS ฯลฯ)UPS ต้องทดสอบปิดไฟ ซ่อมแซมเปลี่ยนแบตเตอรี่(

(๕) ตรวจสอบสถานการณ์ทำงานของเครื่อง Server ผ่านระบบเครือข่าย โดยทดสอบการเชื่อมต่อจาก เครื่องลูกข่ายเข้ามาที่เครื่อง Server และ ทดสอบการเชื่อมต่อจาก Server ไปยัง Web site อื่นๆ ที่ไม่ได้อยู่ภายใต้ การดูแลของ WebServer หน่วยงาน

(๖) ทดสอบสถานการณ์ทำงานของเครื่อง Server จากต่างเครือข่าย มีมากกว่ากรณีที่)๑ เครือข่าย(

(๗) ตรวจสอบ ปรับปรุงโปรแกรมป้องกัน/Virus ทุกสัปดาห์หากเป็นระบบปฏิบัติการ Linux ให้อัพเดต แพตซ์ใหม่อย่างน้อยเดือนละ ๑ ครั้ง

(๘) ปรับปรุงโปรแกรมอุดช่องโหว่ของระบบปฏิบัติการ ทุก ๑ เดือน

(๙) เมื่อพบข้อผิดพลาดในแต่ละ Server หรือ Server หยุดให้บริการให้ดำเนินการแก้ไข (ล่ม) เบื้องต้น หากไม่แล้วเสร็จให้รีบแจ้งหัวหน้ากลุ่มพัฒนาข้อมูลและสารสนเทศ เพื่อหาแนวทาง (ผู้รับผิดชอบ) จัดการปัญหาต่อไป พร้อมบันทึกไว้เป็นหลักฐานในแบบบันทึกขอเข้าห้อง Server ที่หน่วยงานกำหนด

(๑๐) กรณีปัญหาที่เกิดกับ Server หรือ อุปกรณ์เครือข่าย เช่น Switch, Router,Modem, สาย UTP เป็นปัญหาความเสี่ยงที่เกินความสามารถของเจ้าหน้าที่กลุ่มพัฒนาข้อมูลและสารสนเทศ ให้ทำตามระเบียบพัสดุโดย จัดจ้างช่างหรือผู้เชี่ยวชาญจากภายนอกเพื่อแก้ไขปัญหาให้แล้วเสร็จ

ความถี่ในการปฏิบัติ

(๑) ทุกวันทำการ ได้แก่ตรวจสอบการทำงานของเครื่อง

(๒) สัปดาห์ละครั้ง ได้แก่การทำความสะอาดภายนอก ตรวจสอบ ปรับปรุงโปรแกรมป้องกัน/Virus

(๓) ทุกเดือน ได้แก่ ปรับปรุงโปรแกรมอุดช่องโหว่ของระบบปฏิบัติการ,ตรวจสอบ Event Viewer

ช่วงเวลาที่ปฏิบัติ

(๑) วันหยุด

(๒) ช่วงที่มีการใช้งานน้อยที่สุด เช่น หลังเลิกงาน แบบฟอร์มการบันทึกผลการปฏิบัติ

แบบบันทึกการดูแลบำรุงเครื่องคอมพิวเตอร์แม่ข่ายของโรงพยาบาลสวนสราญรมย์ที่หน่วยงานกำหนด

๔.๓ การควบคุมการสำรองข้อมูลสำหรับเครื่อง Server

ประเภทของข้อมูล

(๑) ข้อมูลที่เป็น Database

(๒) ข้อมูลของ Web Server

วิธีปฏิบัติ

(๑) มีหนังสือแต่งตั้งผู้มีหน้าที่สำรองข้อมูลและมีคู่มือปฏิบัติโดยเจ้าหน้าที่กลุ่มพัฒนาข้อมูลและ สารสนเทศ ปฏิบัติตามคู่มือการควบคุมการสำรองข้อมูลสำหรับเครื่อง Server ของหน่วยงาน โดย ผู้มีสิทธิ์จะทำ การสำรองข้อมูลจะต้องมีรายชื่อเป็น Administrator ตามตารางการดูแลและปฏิบัติหน้าที่ในห้อง Serve ในแต่ละ เดือนหรือผู้ที่ได้รับการแต่งตั้งให้มีหน้าที่ดูแลและสำรองฐานข้อมูล

(๒) ผู้มีหน้าที่ในการสำรองข้อมูลจะต้องทำการสำรอง)Backup) ข้อมูลในServer ที่มีอยู่ เช่น)Data Center, Proxy Server, Web Server, Database Server, Mail Server ฯลฯ (

(๓) ก่อนการสำรองในแต่ละครั้ง จะต้องตรวจสอบข้อมูลให้ดีก่อนว่า ข้อมูลสมบูรณ์ดีและต้องรอให้ ผู้ใช้งานฐานข้อมูล ได้ทำการ Update เรียบร้อยก่อนและฐานข้อมูลไม่มีการเปิดใช้งาน

(๔) กรณีที่เป็น Database เช่น MySQL, SQL Server, Access, Oracle, ฯลฯ ให้ทำการสำรอง (Backup) ตามแนวปฏิบัติที่ได้จัดทำไว้ในเรื่องนโยบายการสำรองข้อมูล และทำการจดบันทึกการปฏิบัติงานไว้เป็นหลักฐานทุกครั้ง ตามแบบบันทึกการสำรอง ข้อมูลของหน่วยงาน

(๕) กรณี Web Server ให้ทำการสำรอง)Backup) ตามแนวปฏิบัติที่ได้จัดทำไว้ในเรื่อง นโยบายการสำรองข้อมูล หรือทุกครั้งที่มีการ เปลี่ยนแปลง และทำการ Manual Update เดือนละครั้ง และจดบันทึกการปฏิบัติงานไว้เป็นหลักฐานทุกครั้ง ตาม แบบบันทึกการสำรองข้อมูลตามแบบฟอร์มที่หน่วยงานกำหนด

(๖) สื่อที่ใช้ในการ Backup ข้อมูลใน Server ได้แก่แผ่น CD, แผ่น DVD, TapeBackup , External Hard disk หรือเครื่องคอมพิวเตอร์เครื่องอื่นๆ จะต้องถูกจัดเก็บไว้ในที่ปลอดภัย และสามารถนำข้อมูลกลับมา Restore ใช้งานได้ทันทีเมื่อเกิดความเสี่ยงหรือภาวะวิกฤต เช่น ถูกโจรกรรมข้อมูล , อัคคีภัยและมีการทดสอบ Restore อย่างน้อย ๖ เดือนต่อครั้ง

ความถี่ในการปฏิบัติ

(๑) ทุกวันทำการ ได้แก่การสำรอง)Backup) ข้อมูลที่เป็น Database ถ้าเป็นฐานข้อมูลคนไข้ควร Backup ทุกวัน

(๒) สัปดาห์ครั้ง ได้แก่ ข้อมูลของ Web Server หรือทุกครั้งที่มีการเปลี่ยนแปลง

(๓) ทุกเดือน ได้แก่ข้อมูลของ Web Server ในลักษณะ Manual Update

ช่วงเวลาที่ปฏิบัติ

(๑) วันหยุด

(๒) ช่วงที่มีการใช้งานน้อยที่สุด แบบฟอร์มการบันทึกผลการปฏิบัติ

แบบบันทึกการสำรองข้อมูลตามแบบฟอร์มหน่วยงานกำหนด วิธีการ Backup โดยใช้โปรแกรม

(๑) Schedule

(๒) Tools อื่นตามความเหมาะสม

(๓) Manual

อุปกรณ์ที่ใช้ Backup

(๑) External Hard disk

(๒) DVD

(๓) เครื่องคอมพิวเตอร์

สถานที่จัดเก็บจะต้องจัดเก็บไว้ในที่ปลอดภัย และสามารถนำข้อมูลกลับมา : Restore ใช้งานได้ทันทีเมื่อเกิด ความเสี่ยงหรือภาวะวิกฤต เช่น ถูกโจรกรรมข้อมูล, อัคคีภัย เป็นต้น

๔.๔ การวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์

วิธีปฏิบัติ

(๑) ดำเนินการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์โดยใช้เครื่องคอมพิวเตอร์ชนิด Client ที่มีการ Fix IP Address

(๒) ใช้โปรแกรม Internet Browser ในการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์โดยเข้าไปที่ Address ตามที่หน่วยงานกำหนด

(๓) ใส่ User Name และ Password ตามที่กำหนด

(๔) ที่หน้าจอของโปรแกรม ตรวจสอบสถานะของอุปกรณ์ว่าเข้าสู่ระบบได้หรือไม่ และระบบช้าหรือไม่

(๕) ตรวจสอบสถานะของ System Resource CPU Usage ใช้ไปแล้วร้อยละเท่าไร หรือดูจาก Gauge (Meter) ว่าชี้ในช่วงใด หรือแสดงลัก (สีเขียว หรือ สีเหลือง หรือ สีแดง)ษณะอื่นที่บ่งบอกสถานะและระดับการใช้งาน - Memory Usage ใช้ไปแล้วร้อยละเท่าไร หรือดูจาก Gauge (Meter) ว่าชี้ในช่วงใด สีเขียว หรือ สีเหลือง หรือ สี) แดงหรือแสดงลักษณะอื่นที่บ่งบอกสถานะและ (

ระดับการใช้งาน - Fortianalyser Usage ใช้ไปแล้วร้อยละเท่าไร หรือดูจาก Gauge (Meter) ว่าชี้ในช่วงใด สีเขียว หรือ สีเหลือง หรือ) สีแดง(

(๖) ตรวจสอบสถานะของ Top Session จะแสดง Bar chart เลือกกด Bar chartที่สูงสุดหรือที่สนใจ จะ ได้report และพิมพ์ผลของ report

(๗) ตรวจสอบสถานะของ Usage จะแสดง Bar chart เลือกกด Bar chart ที่สูงสุดหรือที่สนใจ จะได้ report และพิมพ์ผลของ report

(๘) ตรวจสอบสถานะของ Alert Message Console เพื่อดูMessage ที่ผิดปกติเลือกกด Detail จะได้ report และพิมพ์ผลของ report

(๙) ตรวจสอบสถานะของ Log and Architecture เพื่อดูProtocol ที่สนใจ เช่นHttp, Https, E-mail, FTP, Log-Average, IPS- Intension Prevention System,Event Occur เลือกกด Detail จะได้report และพิมพ์ ผลของ report

(๑๐) ดำเนินการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ตามผลจาก Report ที่ได้รับเสนอให้ผู้อำนวยการ ทราบและพิจารณาเป็นประจำทุกสัปดาห์หรือตามความเหมาะสม

ความถี่ในการปฏิบัติ

(๑) สัปดาห์ละครั้ง ตามกำหนดการที่วางไว้

ช่วงเวลาที่ปฏิบัติ

(๑) วันหยุด

(๒) ตามความเหมาะสมของแต่ละช่วงเวลา

แบบฟอร์มการบันทึกผลการปฏิบัติรายงานผลการวิเคราะห์ :

วิธีการวิเคราะห์โดยใช้โปรแกรม

(๑) Schedule

(๒) Manual

สถานที่จัดเก็บ แฟ้มรวบรวมผลการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์ :

๔.๕ การควบคุมผู้ใช้คอมพิวเตอร์

ประเภทของผู้ใช้คอมพิวเตอร์แบ่งออกเป็น ๒ กลุ่ม คือ

(๑) บุคลากรของหน่วยงาน

(๒) บุคลากรที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้รับผิดชอบในการดูแลเครื่องคอมพิวเตอร์และ อุปกรณ์

วิธีปฏิบัติในการควบคุมผู้ใช้คอมพิวเตอร์

(๑) หัวหน้าส่วนราชการ/กำหนด/ผู้อำนวยการของแต่ละหน่วยงาน ลงนามในหนังสือมอบหมาย/คำสั่ง แต่งตั้งผู้รับผิดชอบหลักและรอง ควรมีข้าราชการ)๑ คนร์และอุปกรณ์ต่อพ่วงดูแลเครื่องคอมพิวเตอ (ภายใน หน่วยงาน

(๒) หัวหน้าฝ่ายหัวหน้ากลุ่มงาน ภายในแต่ละหน่วยงานมีหน้าที่ดูแลและควบคุมกำกับ ผู้รับผิดชอบ/ดูแล เครื่องคอมพิวเตอร์นั้น ให้ปฏิบัติตามวิธีปฏิบัติงานบำรุงรักษาเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ ตามกำหนดเวลา

(๓) กรณีเจ้าหน้าที่นำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้ปฏิบัติงานภายในหน่วยงานในระบบเครือข่าย/คอมพิวเตอร์ของหน่วยงาน กำหนดให้ดำเนินการตามระเบียบปฏิบัติเรื่อง การบริหารความเสี่ยงด้านเทคโนโลยี สารสนเทศและการสื่อสาร เช่นเดียวกับเครื่องคอมพิวเตอร์ภายในหน่วยงาน

ความถี่ในการปฏิบัติทุกแห่ง

ช่วงเวลาที่ปฏิบัติหลังจากที่ได้รับการจัดสรรครุภัณฑ์คอมพิวเตอร์

๔.๖ การควบคุมผู้ใช้บริการ

(๑) ผู้ขอใช้บริการบันทึกขอมี UserName และ Password เพื่อเสนอต่อผู้อำนวยการฯเป็นผู้ลงนามอนุญาต โดยใช้แบบฟอร์มการขอเข้าระบบเครือข่ายและการเข้าใช้งานในระบบคอมพิวเตอร์ตามแบบฟอร์มตามที่ หน่วยงานกำหนด

(๒) ผู้อำนวยการ มอบหมายให้หัวหน้าศูนย์สารสนเทศ เพื่อพิจารณาอนุญาต

(๓) กรณีไม่อนุญาต หัวหน้าศูนย์สารสนเทศฯ แจ้งกลับผู้ขอใช้บริการทราบ

(๔) กรณีอนุญาต เจ้าหน้าที่ศูนย์สารสนเทศฯ ดำเนินการ Add userให้บันทึกลงในรายชื่อผู้ขอใช้ระบบ โดยใช้แบบฟอร์มจากเครื่องคอมพิวเตอร์แม่ข่ายเรียงตามลำดับตัวอักษร

(๕) จัดส่ง Username และ Password ที่เป็นความลับของแต่ละบุคคลที่สามารถเข้าระบบเครือข่ายและ ซักซ้อมความเข้าใจเรื่องการใช้บริการระบบเครือข่ายท้องถิ่น)LAN) ของหน่วยงาน

๔.๗ การยกเลิกการเข้าใช้งานในระบบเครือข่าย

ประเภทของงาน การยกเลิกการเข้าใช้งานในระบบเครือข่าย แบ่งออกเป็น ๒ ประเภท คือ

(๑) บุคลากรของหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯ

(๒) บุคลากรที่ไม่ปฏิบัติตามข้อกำหนด

วิธีปฏิบัติในการยกเลิกการเข้าใช้งานในระบบเครือข่าย

(๑) กลุ่มพัฒนาข้อมูลและสารสนเทศ ของแต่ละหน่วยงาน สำรวจรายชื่อสมาชิกโดยส่งรายชื่อสมาชิกที่ เข้าระบบเครือข่ายฯให้แต่ละหน่วยงานตรวจสอบรายชื่อผู้ที่ปฏิบัติงานจริงปีละ ๑ ครั้ง ประมาณเดือนกันยายน

(๒) กรณีสมาชิกฯในแต่ละหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯให้แจ้งหัวหน้าฝ่ายกลุ่ม/ พัฒนาข้อมูลและสารสนเทศ ทราบ และดำเนินการคัดชื่อออกหรือปิดการให้บริการ

(๓) กำหนดระเบียบปฏิบัติเมื่อสมาชิกไม่ปฏิบัติตามข้อกำหนด กลุ่มพัฒนาข้อมูลและสารสนเทศ แจ้ง รายชื่อผู้ที่ไม่ปฏิบัติตามข้อกำหนดให้แก่ผู้บังคับบัญชาได้รับทราบ

- กลุ่มพัฒนาข้อมูลและสารสนเทศ ทบทวนเรื่องกฎ ระเบียบ บทลงโทษ และดำเนินการตามขั้นตอน ที่กำหนดไว้ในระเบียบ
- ตรวจสอบการไม่ปฏิบัติตามข้อกำหนดของสมาชิก
- หากไม่เป็นไปตามข้อกำหนดให้ปฏิบัติตามที่ระเบียบกำหนด
- หากปฏิบัติตามตามข้อกำหนด สามารถเข้าใช้ระบบได้ตามระเบียบ

ความถี่ในการปฏิบัติ

(๑) ตรวจสอบรายชื่อผู้ที่ปฏิบัติงานจริงปีละ ๑ ครั้ง

(๒) เมื่อมีสมาชิกฯในแต่ละหน่วยงานมีการลาออก ย้ายหน่วยงาน เสียชีวิต ฯลฯ ช่วงเวลาที่ปฏิบัติประมาณเดือนกันยายน หรือเมื่อมีสมาชิกฯในแต่ละหน่วยงานมีการลาออก ย้าย หน่วยงาน เสียชีวิต ฯลฯ

การบันทึกผลการปฏิบัติแบบสำรวจรายชื่อสมาชิก

๕.กลุ่มผู้รับผิดชอบดูแลระบบคอมพิวเตอร์

๕.๑ งานบำรุงรักษาเครื่องคอมพิวเตอร์

ประเภทของเครื่องคอมพิวเตอร์

(๑) เครื่องคอมพิวเตอร์ของหน่วยงานราชการ

(๒) เครื่องคอมพิวเตอร์ที่เช่า

วิธีปฏิบัติ การทำความสะอาด กำหนดให้ ทำความสะอาด อุปกรณ์ภายนอก

(๑) ตัวเครื่องและจอภาพ ใช้ผ้าแห้งหรือใช้น้ำยาเฉพาะจอภาพ เช็ดทำความสะอาด อย่าง : น้อยเดือน ละ ๑ ครั้ง

(๒) อุปกรณ์ต่อพ่วงต่างๆ เช่น Mouse Keyboard (มีการเคาะฝุ่นด้วย (UPS Printer Scanner ใช้ผ้าแห้ง ทำความสะอาด หรือใช้น้ำยาเฉพาะ โดยทำความสะอาดอย่างน้อยเดือนละ ๑ ครั้ง

ทำความสะอาดอุปกรณ์ภายใน

(๑) ใช้วิธีการเป่าอย่างน้อยปีละ ๑ ครั้ง โดยเจ้าหน้าที่ ITหรือจ้างหน่วยงานภายนอก การบำรุงรักษา Hard Disk

(๒) กำหนดให้ลบไฟล์ที่เป็นไฟล์ขยะ เช่น TemporaryFiles, Temporary Internet Files, Cookies Files และทำการ Empty ไฟล์ใน Recycle Bin เพื่อลบอย่างถาวรอย่างน้อยเดือนละ ๑ ครั้ง

(๓) กำหนดให้ทำการตรวจสอบ จัดระเบียบ/Hard Diskด้วยโปรแกรม Scandisk / Disk Defragmenter ในSystem tools อย่างน้อยเดือนละ ๑ ครั้ง ทั้งนี้เพื่อรักษาประสิทธิภาพในการจัดเก็บเข้าถึงข้อมูล/

ความถี่ในการปฏิบัติ

(๑) ทำความสะอาดอุปกรณ์ภายนอก และ ภายใน อย่างน้อยเดือนละ ๑ ครั้ง

(๒) การบำรุงรักษา Hard Disk อย่างน้อยเดือนละ ๑ ครั้ง

ช่วงเวลาที่ปฏิบัติตามความเหมาะสม

การบันทึกผลการปฏิบัติ

(๑) สร้าง Folder ใหม่ขึ้นที่ Desktop ของเครื่องคอมพิวเตอร์ชื่อ“Maintenance” และภายใน Maintenance สร้าง Folder เพิ่มเติมชื่อ“Defragmenter” แต่ในกรณีwindow ใหม่ ให้ capture ไว้ที่ Desktop เพื่อป้องกัน Drive C มีปัญหา

(๒) ในวิธีปฏิบัติเรื่อง การบำรุงรักษา Hard Disk เมื่อดำเนินการDefragmenter เสร็จเรียบร้อยแล้ว ให้ เลือกกด View เพื่อดูผลของการ จัดระเบียบ Hard Disk ด้วยโปรแกรม Disk Defragmenter กดSave ไปเก็บไว้ที่ Folder Maintenance/ Defragmenter ที่สร้างไว้โดยตั้งชื่อ File ว่า “ DDMMYYYY.txt “ ตามวันเดือนปีที่ ดำเนินการ แต่ในกรณีwindow ใหม่ ให้capture ไว้ที่ Desktop

๖.การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer

ประเภทของงาน การติดตั้งและปฏิบัติตามวิธีปฏิบัติในการป้องกัน Virus Computer

(๑) เครื่องคอมพิวเตอร์ของหน่วยงาน

(๒) เครื่องคอมพิวเตอร์ที่เช่า

(๓) เครื่องคอมพิวเตอร์ส่วนตัวที่นำมาใช้ในหน่วยงาน ยกเว้น เครื่องคอมพิวเตอร์ที่ไม่ได้ต่อเข้ากับระบบ LAN ของหน่วยงาน

วิธีปฏิบัติ

(๑) คอมพิวเตอร์ที่นำมาใช้งานในระบบเครือข่ายคอมพิวเตอร์ของแต่ละหน่วยงานจะต้องมีการติดตั้ง โปรแกรมป้องกัน Virus Computer (๒) การตรวจจับ Virus Computer กำหนดให้ (๑) Update / ตรวจสอบการ Update รายชื่อ Virus computer (DefinitionAntivirus Table Files) อย่างน้อยสัปดาห์ละ ๑ ครั้ง

(๒) Scan Virus แบบ Full System อย่างน้อยสัปดาห์ละ ๑ ครั้ง

ความถี่ในการปฏิบัติ

(๑) ติดตั้งโปรแกรมป้องกัน Virus Computer เมื่อได้รับเครื่องคอมพิวเตอร์

(๒) การตรวจจับ Virus Computer อย่างน้อยสัปดาห์ละ ๑ ครั้ง

ช่วงเวลาที่ปฏิบัติตามความเหมาะสมของแต่ละหน่วยงาน

การบันทึกผลการปฏิบัติโดยดำเนินการ

(๑) สร้าง Folder ใหม่ขึ้นที่ Desktop ของเครื่องคอมพิวเตอร์ชื่อ“Maintenance” และภายใน Maintenance สร้าง Folder เพิ่มเติมชื่อ“Scan Virus”

(๒) ในวิธีปฏิบัติเรื่อง การตรวจจับ Virus computer เมื่อดำเนินการScan virus ให้เลือกกด View หรือ Capture ผลไว้เพื่อดูผลของการScan Virus แบบ Full System กด Save ไปเก็บไว้ที่ Folde Maintenance/Scan Virus ที่สร้างไว้โดยตั้งชื่อ File ว่า “DDMMYYYY.txt “ ตามวันเดือนปีที่ดำเนินการ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์ ฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการสารสนเทศด้านเวชปฏิบัติโรงพยาบาลสวนสราญรมย์ ซึ่งมีหน้าที่ใน การ กำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลสวนสราญรมย์ เพื่อใช้เป็น แนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ขอให้เจ้าหน้าที่ที่เกี่ยวข้องทราบและถือปฏิบัติ อย่างเคร่งครัดต่อไป

(นายจุมภฏ พรมสีดา)

ผู้อำนวยการโรงพยาบาลสวนสราญรมย์

๓ มีนาคม ๒๕๖๓

ภาคผนวก ก

คำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์

ภาคผนวก ข

คำสั่งมอบหมายเจ้าหน้าที่ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาลสวนสราญรมย์

๒๕๖๓ กุมภาพันธ์ ๒๘