

นโยบายและแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลทุ่งเสลี่ยม

นโยบายและแนวปฏิบัติ

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโรงพยาบาลทุ่งเสลี่ยม

เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทุ่งเสลี่ยมเป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรม ทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ โรงพยาบาลทุ่งเสลี่ยมได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของโรงพยาบาลทุ่งเสลี่ยมประกอบด้วยนโยบายหลัก 4 ด้าน และแนวทางปฏิบัติภายในกรอบนโยบายหลัก ดังต่อไปนี้

๑. ด้านนโยบายและแผน
๒. ด้านการควบคุมระบบเทคโนโลยีสารสนเทศ
๓. ด้านการเข้าถึงผู้ใช้งาน
๔. ด้านการเข้าถึงระบบเครือข่าย

๑. ด้านการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

เป็นนโยบายในการกำหนดการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๒. ด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

เป็นนโยบายในการธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน(availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และ ความน่าเชื่อถือ (reliability) รวมถึงกรณีที่เกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย

๓. ด้านการตรวจสอบและประเมินความเสี่ยง เป็นนโยบายในการตรวจสอบและประเมินความเสี่ยง เพื่อกำกับดูแลการบริหารระบบสารสนเทศให้เกิดประสิทธิภาพและประสิทธิผล ตลอดจนการกำหนดแนวทางการแก้ไขปัญหา และ อุปสรรคต่าง ๆ ที่เกิดขึ้น อย่างน้อยปีละ ๑ ครั้ง เพื่อทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน
นิยามศัพท์

ผู้ใช้งาน หมายถึง ผู้บริหาร ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบโรงพยาบาลทุ่งเสลี่ยม รวมทั้ง ผู้รับบริการ ผู้ใช้งานทั่วไป ที่ได้รับอนุญาต(Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของสำนักงานโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ที่สำนักงานกำหนดไว้

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

สิทธิของผู้ใช้งาน

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของโรงพยาบาลทุ่งเสลี่ยม

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาต เช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

สำนักงาน หมายถึง โรงพยาบาลทุ่งเสลี่ยม

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลทุ่งเสลี่ยม

ผู้ถือครองเครื่องคอมพิวเตอร์ หมายถึง ผู้ได้รับเครื่องคอมพิวเตอร์ไว้ใช้ประจำในการปฏิบัติงานและผู้ถือครองรับผิดชอบ ดูแลเครื่อง/อุปกรณ์คอมพิวเตอร์

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของ โรงพยาบาลทุ่งเสลี่ยมนำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ และอื่น ๆ

เจ้าของข้อมูล หมายถึง เจ้าหน้าที่ของหน่วยงานในโรงพยาบาลทุ่งเสลี่ยมผู้ได้รับมอบหมายจากผู้บังคับบัญชา ให้รับผิดชอบดูแลปรับปรุงข้อมูลของระบบงานนั้นๆ ซึ่งเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึงระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่SMTP, POP^๓ และ IMAP

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

นโยบายด้านการใช้งานสารสนเทศ

การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control)

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๑ ผู้ดูแลระบบต้องดำเนินการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่ผู้ใช้งานได้รับอนุญาตหรือได้รับการมอบอำนาจ ตามที่กำหนดใน “การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่”

๑.๒ ผู้ดูแลระบบมีการกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้อ่านข้อมูล, สร้างข้อมูล, นำเข้าข้อมูล, แก้ไขข้อมูล, อนุมัติและ ไม่มีสิทธิ

๑.๓ ผู้ดูแลระบบดำเนินการควบคุมการเข้าถึงที่เหมาะสมต่อหมวดหมู่ของสารสนเทศที่จัดไว้ตามระดับชั้นความลับ

๑.๔ ผู้ดูแลระบบมีการถอดสิทธิการเข้าถึงการใช้งานสารสนเทศ ตามที่กำหนดใน “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

๑.๕ ผู้ดูแลระบบเป็นผู้ควบคุมการเข้าถึงจากประเภทของการเชื่อมต่อทั้งหมด

๑.๖ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน จะต้องได้รับการพิจารณาจากผู้บริหารของหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่โรงพยาบาลทุ่งเสลี่ยม

๑.๗ ผู้ดูแลระบบกำหนดประเภทของข้อมูล ได้แก่ ข้อมูลภายนอกสามารถเปิดเผยได้ข้อมูลภายในเป็นไปตามลำดับชั้นความลับของข้อมูล

๑.๘ ผู้ดูแลระบบกำหนดลำดับชั้นความลับของข้อมูล ได้แก่ลับที่สุด, ลับมาก, ลับ และทั่วไป

๑.๙ ผู้ดูแลระบบกำหนดลำดับความสำคัญของข้อมูล ได้แก่ สำคัญมากที่สุด, สำคัญมาก และทั่วไป

๑.๑๐ ผู้ดูแลระบบกำหนดระดับชั้นการเข้าถึง ได้แก่ ผู้บริหาร, ผู้ดูแลระบบ, เจ้าของระบบและผู้ใช้ระบบ

๑.๑๑ ผู้ดูแลระบบกำหนดเวลาและช่องทางที่เข้าถึงได้ให้เหมาะสมตามแต่ละระบบงาน

๒ การควบคุมการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

๒.๑ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บริหารของหน่วยงานต้นสังกัด และเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานเพื่อเข้าใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษรและหรือตามแบบฟอร์มที่โรงพยาบาลทุ่งเสลี่ยมกำหนดตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น โดยต้องคำนึงถึงประเภทข้อมูลและชั้นความลับ โดยต้องมีการอนุญาตเข้าใช้งานเป็นลายลักษณ์อักษรจากผู้อำนวยการโรงพยาบาลทุ่งเสลี่ยม เพื่อการจัดเก็บไว้เป็นหลักฐาน

๒.๓ เจ้าของข้อมูลและหรือเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานหรือตามความจำเป็นขั้นต่ำเท่านั้น โดยไม่อนุญาตให้กำหนดสิทธิเกินความจำเป็นในการใช้งาน โดยต้องมีการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและหรือเจ้าของระบบงาน

๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงาน ภายใน ๑๕ วันทำการ นับจากวันที่ผู้มีอำนาจลงนามในคำสั่ง

๓.๒ ผู้ดูแลระบบกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบสารสนเทศโปรแกรมประยุกต์ (Application) ภายในสำนักงาน จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต ระบบเครือข่ายไร้สาย (Wireless LAN) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงาน เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๔.๑ ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๔.๒ การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๔.๓ กรณีผู้ดูแลระบบมีความจำเป็นต้องให้สิทธิ์เพิ่มเป็นกรณีพิเศษแก่ผู้ใช้งานที่มีสิทธิ์พื้นฐานต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน และต้องมีการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยต้องดำเนินการอย่างน้อย ดังนี้

๔.๓.๑ ควบคุมการใช้งานอย่างเข้มงวดและอนุญาตให้เข้าใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๔.๓.๒ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔.๓.๓ กรณีมีการใช้งานไม่ต่อเนื่อง ให้มีการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเสร็จสิ้นการใช้งานในแต่ละครั้ง หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้มีการเปลี่ยนรหัสผ่านทุก ๓ เดือน

๔.๔ กำหนดขั้นตอนในการลงทะเบียนผู้ใช้งาน (user registration) ดังนี้

๔.๔.๑ มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคล

๔.๔.๒ การกำหนดชื่อผู้ใช้ กำหนดจากชื่อภาษาอังกฤษไม่เกิน ๖ อักขระ และตามด้วยอักษร ๒ ตัวแรกของนามสกุล หากซ้ำ ให้เปลี่ยนในอักขระสุดท้ายเป็นตัวอักษรถัดไปของนามสกุล

๔.๔.๓ มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงาน

๔.๔.๔ มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศการการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดสัญญาจ้าง เป็นต้น

๕. วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๕.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ หากข้อมูลมีความลับ

๕.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๕.๓ ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงข้อมูลโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน(Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

๕.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN

๕.๕ มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๖. การควบคุมการเข้าใช้งานระบบจากภายนอก

๖.๑ ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอ เพื่อขอใช้สิทธิ์ในการเข้าถึงระบบจากระยะไกล และต้องได้รับอนุมัติจากสำนักงาน

๖.๒ ผู้ดูแลระบบงานโรงพยาบาลทุ่งเสลี่ยม เป็นผู้ควบคุมการเข้าถึงระบบจากระยะไกล (Remote access)

๖.๓ ผู้ใช้งานที่มีความจำเป็นต้องเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับอนุมัติจากผู้อำนวยการโรงพยาบาลทุ่งเสลี่ยม และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบและข้อมูลอย่างเคร่งครัด

๖.๔ ผู้ดูแลระบบต้องควบคุมพอร์ต (Port) ที่ระบบสารสนเทศให้บริการ ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้านั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๖.๕ การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ผู้ดูแลระบบต้องอนุญาตตามพื้นฐานของความจำเป็นเท่านั้น และให้ปิด Port และ Modem เมื่อผู้ใช้งานได้ใช้งานเสร็จสิ้นแล้วทันที

๗. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบของสำนักงาน ต้องผ่านการพิสูจน์ตัวตนจากระบบของสำนักงาน โดยมีแนวทางปฏิบัติดังนี้

๗.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

๗.๒ การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

๗.๓ การเข้าสู่ระบบสารสนเทศของสำนักงานจากอินเทอร์เน็ตนั้น จะต้องมีการตรวจสอบผู้ใช้งาน

๗.๔ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน โดยใช้รหัสผ่าน หรือวิธีการเข้ารหัสการบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านการบริหารรหัสผ่าน

๑. ศูนย์เทคโนโลยีสารสนเทศต้องกำหนด ชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์เฉพาะบุคคลไม่ซ้ำกัน และกำหนดชื่อผู้ใช้ในส่วนของ ชื่อผู้ใช้ของผู้ใช้งาน ชื่อผู้ใช้ของผู้ดูแลระบบ ชื่อผู้ใช้ของผู้ดูแลฐานข้อมูล ชื่อผู้ใช้ของผู้พัฒนาระบบ ชื่อผู้ใช้ของเจ้าหน้าที่ทางเทคนิค หรืออื่นๆ ให้มีความแตกต่างกัน

๒. การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องใส่ซองปิดผนึกและประทับตรา “ลับ” ส่งไปยังผู้ใช้งานพร้อมแจ้งช่องทางการเข้าถึง “แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” เพื่อสร้างความรู้ความเข้าใจ และให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด

๓. ศูนย์เทคโนโลยีสารสนเทศทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานทุก ๑ ปีการใช้งานรหัสผ่าน

๔. ผู้ใช้งานต้องเก็บรักษา รหัสผ่าน (Password) ของตนเองและของกลุ่มไว้เป็นความลับ

๕. ห้ามทำการบันทึก รหัสผ่าน (Password) ไว้ในโปรเซสซีอีเล็กทรอนิกส์ หรือแบบฟอร์มอิเล็กทรอนิกส์ต่าง ๆ

๖. ไม่จดหรือบันทึก รหัสผ่าน (Password) ส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๗. ผู้ใช้งานทุกคนต้องเปลี่ยนรหัสผ่าน (Password) เริ่มต้นทันทีหลังจากได้รับมอบรหัสผ่านเริ่มต้นจากผู้ดูแลระบบของโรงพยาบาลทุ้งเสีี่ยม

๘. กำหนดให้รหัสผ่าน (Password) ต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยควรมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน และไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

๙. ไม่ใช้รหัสผ่าน (Password) ส่วนบุคคลสำหรับการใช้เพิ่มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑๐. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่

๑๑. ในกรณีที่ลืมรหัสผ่าน หรือสงสัยว่ารหัสผ่าน (Password) ถูกผู้อื่นทราบ ให้รีบทำการเปลี่ยนแปลงรหัสผ่านทันทีหรือแจ้งให้ผู้ดูแลระบบทราบ เพื่อทำการเปลี่ยนรหัสผ่าน (Password) ทั้งหมดที่เกี่ยวข้อง

๑๒. หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้น ตามกฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้อง

๑๓. กรณีผู้ใช้งานของหน่วยงานภายในสำนักงานลาออก ให้ผู้ดูแลระบบทำการยกเลิกสิทธิของผู้ที่ลาออก ออกจากระบบทันที

๑๔. กรณีผู้ใช้งานของหน่วยงานภายในสำนักงาน มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้หน่วยงานต้นสังกัด แจ้งผู้ดูแลระบบเพื่อทำการเปลี่ยนแปลงสิทธิ์ในการใช้งาน

๑๕. ผู้ใช้งานทุกคนของสำนักงาน มีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยต้องไม่ยินยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากชื่อผู้ใช้ (Username) ระบบคอมพิวเตอร์ของตน

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

๑. การบริหารจัดการทางกายภาพ (Physical security management)

๑.๑ กำหนดระดับความสำคัญของพื้นที่ในส่วนหน่วยจัดเก็บข้อมูล

๑.๒ มีระบบป้องกัน และสัญญาณแจ้งเตือน เมื่อมีการบุกรุกให้ครอบคลุมพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศ อยู่ภายใน (Data Center) หรือบริเวณที่มีความสำคัญ

๑.๓ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพ อย่างน้อยปีละ ๒ ครั้งเพื่อให้ระบบป้องกัน พร้อมใช้งานได้เสมอ

๑.๔ ผู้ดูแลระบบ ต้องปิดประตูและหน้าต่างห้องแม่ข่ายให้ล็อกอยู่เสมอ

๒. การควบคุมการเข้า-ออก (Physical entry controls)

๒.๑ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาเยือน (Visitors)

๒.๒ ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไปเพื่อป้องกันการ สูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และควรมีเหตุผลที่ เพียงพอในการเข้าถึงบริเวณดังกล่าว

๒.๔ สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆที่ต้องปฏิบัติ ระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๒.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๒.๖ มีการพิสูจน์ตัวตน โดยการอ่านบัตรหรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มี ความสำคัญ (Data Center)

๒.๗ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการ ตรวจสอบในภายหลังเมื่อมีความจำเป็น

๒.๘ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๒.๙ ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในห้อง Data Center

๒.๑๐ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๓. การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

๓.๑ จำกัดพื้นที่หรือบริเวณสำหรับการเข้าถึงเพื่อการส่งมอบหรือขนถ่ายผลิตภัณฑ์โดยบุคคลภายนอก

๓.๒ ดูแลบุคลากรซึ่งสามารถเข้าถึงพื้นที่บริเวณส่งมอบหรือขนถ่ายผลิตภัณฑ์

๓.๓ ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบ

พัสดุฯ

๔. การจัดวางและการป้องกันอุปกรณ์(Equipment sitting and protection)

๔.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในห้อง Data Center ให้น้อยที่สุด

๔.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่ง ที่ความมั่นคงปลอดภัย

๔.๓ ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center)

๔.๔ ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณ

๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของสำนักงาน ที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบสำรองกระแสไฟฟ้า (UPS) และระบบปรับอากาศและควบคุมความชื้น

๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนตาม ๕.๑ อย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีทีระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling security)

๖.๑ ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย หรือป้องกันสัตว์ต่างๆ กัดสาย

๖.๒ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๖.๓ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๖.๔ จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๖.๕ ตู้Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๗. การบำรุงรักษาอุปกรณ์(Equipment maintenance)

๗.๑ กำหนดให้มีการบำรุงรักษาอุปกรณ์อย่างน้อยปีละ ๓ ครั้ง

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงาน

๗.๖ ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗.๗ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘. การนำสินทรัพย์ของสำนักงาน ออกไปภายนอกสถานที่ (Removal of property)

๘.๑ ผู้ใช้งานต้องขออนุญาตหัวหน้าหน่วยงานต้นสังกัดก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกสำนักงาน

๘.๒ ผู้ใช้งานต้องบันทึกข้อมูลการนำอุปกรณ์ของสำนักงานออกไปภายนอกสถานที่ เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๙. การป้องกันสินทรัพย์ที่ใช้งานภายนอกสำนักงาน (Security of equipment off-premises)

๙.๑ กำหนดมาตรการความปลอดภัยของสินทรัพย์ เพื่อป้องกันความเสี่ยงจากการนำสินทรัพย์ของสำนักงานออกไปใช้งานภายนอก

๙.๒ ไม่ทิ้งสินทรัพย์ของสำนักงาน ไว้ในที่สาธารณะโดยไม่มีผู้ดูแลรับผิดชอบ

๙.๓ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อดูแลสินทรัพย์ของสำนักงาน เสมือนเป็นสินทรัพย์ของตนเอง

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

๑๐.๑ ให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

นโยบายด้านการบริหารจัดการระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน

การบริหารจัดการด้านการสื่อสารและการดำเนินงานเครือข่ายสารสนเทศ (Communications and operations management)

แนวปฏิบัติ

๑. ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

๑.๑ มีการจัดทำคู่มือการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดอย่างน้อยดังนี้

- การปฏิบัติงานในห้องแม่ข่าย
- การเปิดและปิดระบบงาน ได้แก่ การเปิด - ปิดเครื่องแม่ข่าย การเปิด - ปิด

ระบบงาน การเปิด

- ปิดระบบให้บริการ
- การสำรองข้อมูล
- การบำรุงรักษาอุปกรณ์
- การจัดการกับสื่อบันทึกข้อมูล ได้แก่ การทำป้ายชื่อบ่งชี้การลบ การป้องกันการนำสื่อบันทึกข้อมูลกลับมา

ใช้งานอีกครั้ง

- การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์และการจัดการกับข้อผิดพลาดที่เกิดขึ้น
- การประมวลผลข้อมูล ได้แก่ ขั้นตอนในการนำข้อมูลเข้าระบบงาน ประมวลผลและแสดงผล
- การใช้งานโปรแกรมยูลิติตี
- การรายงานและการจัดการกับปัญหาที่เกิดขึ้น
- การจัดการกับการทำงานล้มเหลวของระบบคอมพิวเตอร์ ระบบงาน และระบบเครือข่าย
- การกู้คืนระบบงานและระบบเครือข่าย

๑.๒ มีการแจกจ่ายและควบคุมดูแลให้มีการปฏิบัติงานตามแนวทางที่กำหนดในคู่มือการปฏิบัติงาน

๑.๓ มีการทบทวนปรับปรุงคู่มือการปฏิบัติงานให้เหมาะสมอยู่เสมอ

๒. ควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ (Changemanagement)

ต้องมีการกำหนดผู้รับผิดชอบและผู้มีอำนาจในการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศของสำนักงาน

๓. การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

๓.๑ มีการกำหนดแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานของแต่ละบุคคลไว้อย่างชัดเจน โดยมีให้มีการกำหนดหน้าที่ที่สำคัญไว้ที่บุคคลเพียงคนเดียว

๓.๒ ให้ผู้บังคับบัญชามีการควบคุมดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหาย

๓.๓ ให้มีการจัดเก็บหลักฐานการปฏิบัติงานที่สามารถใช้ตรวจสอบได้ในภายหลัง

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

๔.๑ ให้กำหนดมาตรการแยกเครื่องคอมพิวเตอร์ของระบบงาน สำหรับการพัฒนา การทดสอบและการให้บริการออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงาน

๔.๒ กำหนดมาตรการควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการให้บริการ

๔.๓ ให้มีการป้องกันการเข้าถึงเครื่องมือในการพัฒนาและอรรถประโยชน์ (Software tool and Utility) ที่ใช้สำหรับการพัฒนาระบบงาน โดยไม่ได้รับอนุญาต

๔.๔ กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากกัน สำหรับระบบงานที่ใช้ในการพัฒนาทดสอบ และใช้ระบบงานจริง

การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

แนวปฏิบัติ

๑. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการ ใช้ไฟล์อื่น ที่สำนักงานไม่อนุญาตให้ใช้งาน

๒. ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศของสำนักงาน

๓. ให้ผู้ดูแลระบบดำเนินการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องเซิร์ฟเวอร์ให้บริการ และอุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ณ จุดทางเข้า-ออกเครือข่ายอย่างสม่ำเสมอ เพื่อตรวจจับโปรแกรม ไม่ประสงค์ดีที่เข้าสู่ระบบ

๔. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรม ไม่ประสงค์ดีได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดีการวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

๕. มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่ที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๗. เครื่องคอมพิวเตอร์ทั้งหมด ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา (Note book) ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสล่าสุดของสำนักงาน จากเจ้าหน้าที่ผู้ดูแลระบบของหน่วยงานภายในสำนักงาน และจะต้องเปิดใช้งานโปรแกรมตรวจสอบและกำจัดไวรัสตลอดเวลา

๘. เครื่องคอมพิวเตอร์ Server ที่ให้บริการการตรวจสอบและกำจัดไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุดของไวรัสอยู่เสมอ และต้องเป็นผู้ให้บริการปรับปรุงข้อมูลไวรัสล่าสุดให้แก่ เครื่องคอมพิวเตอร์ Server เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพาทุกเครื่องโดยอัตโนมัติ

๙. ต้องทำการตรวจสอบไวรัสกับแฟ้มข้อมูล (file) ต่าง ๆ ที่ download มา แฟ้มข้อมูลที่แนบมากับไปรษณีย์ อิเล็กทรอนิกส์, แฟ้มข้อมูลที่ได้มาจากสื่อบันทึกข้อมูลภายนอก (CD, Thumb Drive, Diskette or share file)

๑๐. ศูนย์เทคโนโลยีสารสนเทศ ต้องกำหนดให้เครื่องลูกข่ายทุกเครื่องในสำนักงาน ทำการตรวจสอบไวรัส (Scan Virus) โดยอัตโนมัติในเวลาที่กำหนดเป็นประจำทุกวัน ดังนั้นต้องแจ้งให้ผู้ใช้งานเปิดเครื่องคอมพิวเตอร์เพื่อทำการ Scan Virus ในเวลาดังกล่าว

การเข้าถึงระบบโปรแกรมประยุกต์และสารสนเทศ (Information handling procedures)

แนวปฏิบัติ

๑. การจัดการสารสนเทศ

- ๑.๑ มีการกำหนดข้อมูลตามระดับชั้นความลับ ได้แก่ ข้อมูลทั่วไป ข้อมูลส่วนบุคคล ข้อมูลใช้ภายในข้อมูลลับ
- ๑.๒ มีขั้นตอนปฏิบัติเพื่อจัดการกับข้อมูลตามระดับชั้นความลับ ควรประกอบด้วยวิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ ระยะเวลาที่สามารถเข้าถึง และช่องทางการเข้าถึง
- ๑.๓ มีการจำกัดการเข้าถึงข้อมูลตามระดับชั้นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ๑.๔ มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่น่าออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป
- ๑.๕ มีการจัดทำบัญชีรายชื่อผู้มีสิทธิเข้าถึงข้อมูลและสื่อบันทึกข้อมูลสำคัญ และมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ
- ๑.๖ การเข้าถึงต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย
- ๑.๗ ระบบไวต่อกรรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการ ดังนี้
 - (๑) ต้องแยกระบบซึ่งไวต่อกรรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน
 - (๒) มีการควบคุมสภาพแวดล้อม ได้แก่ มีห้องแม่ข่ายเฉพาะ มีระบบไฟสำหรับระบบเฉพาะ มีระบบป้องกันผู้มีสิทธิเข้าออกห้องแม่ข่าย และมีระบบควบคุมความชื้นและอุณหภูมิเพื่อป้องกันการหยุดชะงักของระบบ
 - (๓) มีการควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา และต้องกำหนดมาตรการป้องกันความเสี่ยงที่มีต่ออุปกรณ์
 - ๑.๘ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) จะต้องดำเนินการ ดังนี้
 - (๑) ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานของผู้ใช้งานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องเพื่อให้มีความมั่นคงปลอดภัย
 - (๒) ผู้ดูแลระบบเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
 - (๓) ผู้ดูแลระบบมีการรักษาความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในสำนักงาน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกลตามแนวปฏิบัติการควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศ

(๔) ผู้ปฏิบัติงานจากระยะไกลต้องรักษาความลับของหน่วยงาน ไม่อนุญาตให้ครอบครัวหรือบุคคลอื่นๆได้เข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

(๕) การขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุง สิทธิการเข้าถึงระบบงาน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๒. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system Documentation)

๒.๑ มีการจัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๒.๒ มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โดยผู้เป็นเจ้าของระบบนั้น

๒.๓ มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนสาธารณะ ได้แก่อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๓. นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

๓.๑ จัดทำนโยบายหรือแนวทางการใช้อย่างเหมาะสมสำหรับการใช้งานระบบหรืออุปกรณ์ที่ใช้ในการสื่อสาร

๓.๒ มีวิธีการป้องกันข้อมูลสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลงแก้ไข ถูกเปิดเผยความลับ โดยไม่ได้รับอนุญาต

๓.๓ มีการจัดทำแนวทางสำหรับการจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารโต้ตอบ และแนวทางตรวจสอบคล้อยกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่เจ้าหน้าที่สำนักงานต้องปฏิบัติตาม

๔. ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)

๔.๑ กำหนดข้อตกลงสำหรับการแลกเปลี่ยนสารสนเทศระหว่างสำนักงานกับหน่วยงานภายนอก

๔.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการแลกเปลี่ยนป้องกันข้อมูล และมาตรฐานในการส่งสื่อบันทึกข้อมูลไปยังภายนอก

๔.๓ กำหนดมาตรฐานที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๕. การกำหนดเวลาสิ้นสุดการใช้งานระบบสารสนเทศ (Session time-out)

๕.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานภายหลังจากที่ไม่มีกิจกรรมการใช้งานตามช่วงระยะเวลาที่กำหนดไว้

๕.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบงานที่มีข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

๖.๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น ได้แก่ กำหนดให้ใช้งานได้ ๒ ชม. ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น หรือช่วงนอกเวลาทำงาน เป็นต้น

๖.๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๗. การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control)

๗.๑ กำหนดขั้นตอนปฏิบัติเพื่อใช้งานที่มั่นคงปลอดภัย

(๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๗.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับใช้งานระบบสารสนเทศของหน่วยงาน

(๒) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม

๗.๓ กำหนดหลักเกณฑ์ยุติการเชื่อมต่อ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อยหากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๗.๔ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อ เพื่อให้ผู้ใช้สามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๓ ชม. ต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะช่วงเวลาเท่านั้น

๘. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging) จัดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศ ที่แสดงให้เห็นว่า ใครทำอะไร ที่ไหน เมื่อไร และอย่างไร

การบริหารจัดการการเข้าถึงระบบเครือข่ายสื่อสารข้อมูล

แนวปฏิบัติ

๑. มาตรการทางเครือข่ายสื่อสารข้อมูล (Network controls)

๑.๑ มีการกำหนดหน้าที่ ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล และกำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

๑.๒ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญ เมื่อต้องส่งผ่านข้อมูลนั้นทาง เครือข่ายสาธารณะ

๑.๓ กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

๑.๔ มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๒. การควบคุมการเข้าถึงระบบเครือข่าย

๒.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) และ DMZ Zone เป็นต้น เพื่อเป็นการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๒ การเข้าสู่ระบบเครือข่ายภายในของสำนักงาน โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพตำบลคลองหลวงแพ่ง ก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๒.๓ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒.๔ ผู้ดูแลระบบ ต้องจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๒.๕ ผู้ดูแลระบบ จัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๒.๖ กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไข หรือเปลี่ยนแปลงค่าparameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๒.๗ ระบบเครือข่ายทั้งหมดของสำนักงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering

๒.๘ มีการจำกัดการเชื่อมต่อทางเครือข่ายโดยมีการติดตั้ง Firewall เป็นเกตเวย์สำหรับเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ เพื่อทำการกรองข้อมูลจราจรในเครือข่ายให้เป็นไปตามความเหมาะสมกับการใช้งานระบบเครือข่ายได้อย่างปลอดภัย

๒.๙ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงาน ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒.๑๐ การเข้าสู่ระบบงานเครือข่ายภายในสำนักงานผ่านทางอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๒.๑๑ IP address ภายในของระบบงานเครือข่ายภายในของสำนักงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบได้โดยง่าย

๒.๑๒ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ ตามกลุ่มของเครือข่ายที่แยกตามกลุ่มเครือข่ายพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๑๓ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากสำนักงาน และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๑๔ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

๒.๑๕ อุปกรณ์เครือข่ายหากมีการเชื่อมต่อด้วย SNMP ต้องกำหนดค่า Community String ไม่เป็นค่าพื้นฐาน

๒.๑๖ การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๒.๑๗ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๒.๑๘ มีการแบ่งเครือข่ายย่อยๆ ภายในองค์กรแบบ VLAN

๓. การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์

๓.๑ ต้องลงทะเบียน Mac Address ประจำเครื่องเพื่อระบุอุปกรณ์บนเครือข่าย และต้องใช้หมายเลข IP Address ที่กำหนดให้โดยผู้ดูแลระบบเท่านั้น

๓.๒ เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งอยู่หลัง Firewall เพื่อป้องกันการละเมิดความมั่นคงปลอดภัยจากเครือข่ายภายนอก

๓.๓ ห้ามผู้ใช้งานที่ใช้งานอยู่ภายในเครือข่ายคอมพิวเตอร์ของสำนักงาน ใช้ Modem หรืออุปกรณ์อื่นใดในการเชื่อมต่อระบบเครือข่ายภายนอก ในขณะเดียวกัน

๓.๔ ห้ามผู้ใช้งานทำการต่อขยายหรือเชื่อมการบริการเครือข่าย (Switch Hub) โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ และห้ามเจ้าหน้าที่เปลี่ยนแปลงหรือแก้ไข (configuration) อุปกรณ์ใด ๆ ในระบบเครือข่ายคอมพิวเตอร์

๓.๕ ห้ามติดตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ หรือ Software ที่ให้บริการเครือข่ายคอมพิวเตอร์ โดยไม่ได้รับการอนุญาตจากผู้ดูแลระบบ

๓.๖ ห้ามผู้ใช้งานทำการ Download ติดตั้ง หรือทำการใช้โปรแกรมตรวจสอบทางด้านความมั่นคงปลอดภัย ในเครือข่ายคอมพิวเตอร์ของสำนักงานโดยไม่ได้รับอนุญาต

๓.๗ เครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายทุกเครื่องจะต้องมีการกำหนดผู้รับผิดชอบประจำแต่ละเครื่อง หากเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายที่ใช้เป็นส่วนกลางต้องกำหนดเจ้าหน้าที่ฝ่ายบริหารงานทั่วไปหรือเจ้าหน้าที่ในหน่วยงานที่ได้รับมอบหมายเป็นเจ้าของเครื่อง พร้อมทั้งจัดทำบัญชีการใช้งานสำหรับเครื่องดังกล่าวไว้เป็นหลักฐาน โดยต้องเก็บข้อมูลชื่อผู้ใช้งาน วันที่ใช้งาน เวลาเริ่มและสิ้นสุดการใช้งาน

๓.๘ กรณีได้รับเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายมาใหม่ หรือจากหน่วยงานอื่น และต้องการเข้าใช้งานระบบเครือข่ายสำนักงาน เจ้าของเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายนั้น ๆ จะต้องปฏิบัติดังนี้

๓.๘.๑ หน่วยงานทำหนังสือขอเข้าใช้ระบบเครือข่ายต่อผู้อำนวยการโรงพยาบาลทุ่งเสลี่ยม

๓.๘.๒ ผู้ดูแลระบบของทุ่งเสลี่ยมเป็นผู้บริหารจัดการการใช้งานระบบเครือข่าย

๓.๘.๓ ผู้ได้รับมอบหมายควบคุมดูแลบัญชีการใช้งานของหน่วยงานในสำนักงานต้องจัดทำบัญชีเครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายของหน่วยงานของตน พร้อมทั้งต้องปรับปรุงสถานการณ์ใช้งานของแต่ละเครื่อง ได้แก่ ชื่อเจ้าของเครื่อง วันที่เริ่มต้นเจ้าของเครื่องรับผิดชอบ วันที่สิ้นสุดเจ้าของเครื่องรับผิดชอบ

๓.๘.๕ เครื่องที่ลงทะเบียนแล้วจะย้ายไปใช้ต่างของหน่วยงานไม่ได้ เว้นแต่จะดำเนินการยกเลิกความเป็นเจ้าของ

๓.๘.๖ ในการเคลื่อนย้ายเครื่องคอมพิวเตอร์ หรืออุปกรณ์เครือข่ายที่มีการลงทะเบียนแล้วไปใช้ในห้องประชุม ให้แจ้งความจำนงที่ผู้ดูแลระบบดำเนินการ

๔. ผู้ใช้งานภายนอก หรือผู้ใช้งานภายในนาเครื่องส่วนตัวมาใช้เครือข่ายสำนักงาน สามารถเข้าใช้งานอินเทอร์เน็ตได้เท่านั้น และสามารถใช้งานได้ชั่วคราว (ครั้งละไม่เกิน ๑ วัน) โดยต้องปฏิบัติดังนี้

๔.๑ ต้องทำการลงทะเบียนขอเข้าใช้งานระบบเครือข่ายทุกครั้งที่ต้องการใช้ระบบเครือข่าย

๔.๒ หน่วยงานเจ้าของเรื่องหรือผู้ที่ได้รับมอบหมายจากหน่วยงานเจ้าของเรื่องที่จะเข้ามาติดต่อต้องทำการตรวจสอบ และอนุมัติการใช้งานสำหรับผู้ใช้งานภายนอกผ่านระบบ แล้วแจ้งให้ผู้ดูแลระบบ ทราบการขอใช้

๔.๓ ผู้ดูแลระบบของโรงพยาบาลส่งเสริมสุขภาพตำบลคลองหลวงแพ่ง จะทำการตรวจสอบข้อมูลการขอใช้งานระบบเครือข่ายจากข้อมูลที่ผู้ขอใช้ทำการกรอกมาเบื้องต้น หากข้อมูลถูกต้องครบถ้วนผู้ดูแลระบบจะทำการอนุมัติการใช้งานระบบเครือข่าย Internet หากข้อมูลไม่ถูกต้องครบถ้วนจะแจ้งกลับไปให้ผู้เป็นเจ้าของเรื่องทราบว่าไม่อนุญาตให้ใช้งานระบบเครือข่าย Internet ได้ ในกรณีนี้ให้ปรับปรุงข้อมูลให้ถูกต้อง

๔.๔ การขอใช้ช่องทางการบริการ (Service port) ของเครื่องแม่ข่าย ต้องได้รับอนุญาตจากโรงพยาบาลทุ่งเสลี่ยม

๕ การใช้งานอินเทอร์เน็ตจากระบบเครือข่ายสำนักงาน ต้องทำการพิสูจน์ตัวตน(Authentication) ผู้ใช้งานภายในและภายนอก ให้ใช้ชื่อผู้ใช้และ รหัสผ่าน ตามที่ผู้ดูแลระบบกำหนด

การบริหารจัดการการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑.๑ กำหนดให้มีรหัสผู้ใช้/รหัสผ่าน (Username/Password) ในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการ

๑.๒ กำหนดจำนวนครั้งที่สามารถพิมพ์รหัสผิดได้ หากเกินกว่าที่กำหนดระบบต้องทำการLock ไม่ให้ใช้งานเป็นระยะเวลาหนึ่ง

๑.๓ ผู้ดูแลระบบควรกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามทีระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๑.๔ ผู้ดูแลระบบควรตั้งระบบการล็อกหน้าจอเมื่อไม่มีการใช้งาน เมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๑.๕ ผู้ดูแลระบบต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒. การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ (Control of operational software)

๒.๑ มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของสำนักงาน เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อ ระบบงานนั้น

๒.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อ ระบบงานของสำนักงาน

๒.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๒.๔ กำหนดให้มีการจัดเก็บ Source Code และ Library สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๒.๕ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒.๖ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒.๗ ทำการปรับปรุง Library สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกันทั้งหมด ก่อนที่ทำการติดตั้ง

๒.๘ กำหนดให้ผู้ที่เกี่ยวข้องจัดทำแผนถอยหลังกลับ (Rollback strategy) ก่อนที่จะดำเนินการติดตั้งระบบงานบนเครื่องให้บริการ

๓. ให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(Technical review of applications after operating system changes)

๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่สำนักงาน ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๔. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๔.๑ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๔.๒ สำนักงานเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๔.๓ ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๔.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๕. ความเป็นเจ้าของและความรับผิดชอบ

๕.๑ หน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์ Server ต้องกำหนดผู้มีหน้าที่รับผิดชอบเพื่อดูแลเครื่องคอมพิวเตอร์ Server โดยทำการ update service pack หรือ patch ต่างๆ ให้ทันสมัยอยู่เสมอเพื่อปิดรูรั่วของตัวระบบปฏิบัติการ และตัวโปรแกรม และต้องมีเอกสารในการปรับเปลี่ยนค่าปรับแต่งบนเครื่องคอมพิวเตอร์ Server และต้องมีภาระรายละเอียดของเครื่องคอมพิวเตอร์ Server ในระบบการจัดการเครือข่าย (Enterprise Management System)

๕.๒ กำหนด ชื่อ/รหัส ระดับสิทธิ์การใช้ให้ผู้ใช้งานแต่ละคน

๖. การติดตั้ง

๖.๑ ห้ามเปิด Services และ Application ใด ๆ ที่ไม่เกี่ยวข้องกับงานของเครื่องคอมพิวเตอร์ Server นั้น ๆ โดยเด็ดขาด

๖.๒ เมื่อมีการปรับแต่งหรือแก้ไขค่า ต้องมีการแจ้งผู้ดูแลรับผิดชอบเครื่องคอมพิวเตอร์ Server นั้น ๆ

๗. การเฝ้าดูและตรวจสอบ

๗.๑ ต้องดำเนินการเก็บ Log และ Audit Trails ของเหตุการณ์ละเมิดความมั่นคงปลอดภัยดังต่อไปนี้

๗.๑.๑ Log ทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยต้องเก็บไว้อย่างน้อยเป็นเวลา ๙๐ วัน

๗.๑๒ ต้องมีระบบจัดเก็บ Log ที่มีอยู่เกินกว่า ๙๐ วัน ให้มีความปลอดภัยและพร้อมให้เรียกใช้งานได้เมื่อพนักงานเจ้าหน้าที่ต้องการ ต้องสามารถนำออกมามอบให้กับพนักงานเจ้าหน้าที่ได้ ๗.๒ ผู้ดูแลระบบ ต้องตรวจสอบ Log และเหตุการณ์ละเมิดความมั่นคงปลอดภัย และรายงานให้กับผู้บังคับบัญชาทราบ ดังนี้

๗.๒.๑ การโจมตีในรูปแบบ Port-Scan

๗.๒.๒ การเข้าสู่ระบบของผู้ใช้งานที่ไม่มีสิทธิในการใช้งานระบบนั้น

๗.๒.๓ เหตุการณ์ผิดปกติของเครื่องคอมพิวเตอร์ Server ที่เกิดขึ้น

๗.๓ ต้องดำเนินการบำรุงรักษา (Maintenance) เป็นประจำ

๗.๔ ต้องมีการประเมินความเสี่ยงทุก ๖ เดือน พร้อมจัดทำรายงานผลการประเมินความเสี่ยงเสนอผู้บังคับบัญชา

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

แนวทางปฏิบัติ

๑ การปฏิบัติทั่วไป

๑.๑ เครื่องคอมพิวเตอร์ที่สำนักงาน อนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของสำนักงานดังนั้นผู้ใช้งาน จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานได้ซื้อ ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย

๑.๓ ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ ของสำนักงาน และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือ แก๊ซ หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๔ ไม่อนุญาตให้ ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมมัลแวร์ในเครื่อง คอมพิวเตอร์ส่วนบุคคลของสำนักงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจาก ผู้ดูแลระบบของหน่วยงานใน โรงพยาบาลทุ่งเสลี่ยม

๑.๕ การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องได้รับการพิจารณาจากผู้ดูแลระบบ

๑.๖ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๑.๗ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

๑.๘ ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ ๑๕ นาทีเพื่อให้ ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน เพื่อป้องกันบุคคลอื่น มาใช้งานที่เครื่องคอมพิวเตอร์

๑.๙ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของสำนักงาน ยกเว้นจะได้รับการพิจารณาอนุมัติจากผู้ดูแลระบบ ก่อนการใช้งาน

๑.๑๐ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ส่วนบุคคลต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยผู้ดูแลระบบของหน่วยงาน

๑.๑๑ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยผู้ดูแลระบบของ หน่วยงาน เท่านั้น

๑.๑๒ การเคลื่อนย้ายเครื่องคอมพิวเตอร์จากจุดเชื่อมต่อเครือข่ายเดิมไปยังจุดเชื่อมต่อเครือข่ายใหม่ภายใน หน่วยงานในสำนักงาน จะต้องแจ้งผู้ดูแลระบบของหน่วยงานเท่านั้น

๑.๑๓ กรณีส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบโดยผู้รับจ้าง เมื่อตรวจสอบเสร็จแล้วต้องให้ผู้ดูแลระบบ ของหน่วยงาน เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงาน

๑.๑๔ ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงานทุกเครื่อง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบของหน่วยงาน

๑.๑๕ เครื่องคอมพิวเตอร์ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสโดย โปรแกรมป้องกันไวรัสของสำนักงาน จากผู้ดูแลระบบ

๑.๑๖ ผู้ใช้งานไม่ควรสร้าง short-cut หรือปุ่มกดง่าย บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ สำนักงาน

๑.๑๗ ผู้ใช้งานมีหน้าที่และความรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยต้อง ปฏิบัติ ดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ disk drive

๑.๑๘ ห้ามเจ้าหน้าที่ทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงานทุก เครื่อง และต้องดูแลมิให้เครื่องที่ถือครอบครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่องคอมพิวเตอร์ส่วนบุคคลถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้และเมื่อรู้ว่าเครื่องมีการแก้ไขการตั้งค่าเวลาต้องแจ้งให้ ผู้ดูแลระบบ ทราบทันที

๑.๑๙ ต้องทำการล้างข้อมูลในเครื่องคอมพิวเตอร์ทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์ให้กับเจ้าของ เครื่องรายใหม่ พร้อมทั้งต้องทำการปลด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์(ระบบปฏิบัติการ) และต้อง ทำการแจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์ทุกครั้ง

๒. แนวทางปฏิบัติในการเข้าใช้เครื่องคอมพิวเตอร์(ระบบปฏิบัติการ) และ รหัสผ่าน

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

๒.๒ ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตาม “การบริหารจัดการสิทธิการใช้งานระบบและ รหัสผ่าน”

๒.๓ ผู้ใช้งาน ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้(User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่อง คอมพิวเตอร์ร่วมกัน

๓. การป้องกันจากโปรแกรมซุคคำสั่งไม่พึงประสงค์ (Malware)

๓.๑ ผู้ใช้งาน ควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๓.๒ ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๓.๓ ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีซุคคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูล คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือซุคคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือ ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๔. การสำรองข้อมูลและการกู้คืน

๔.๑ ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลภายนอก

๔.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของ ข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

การใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ (mobile computing)

แนวปฏิบัติ

๑. การใช้งานทั่วไป

๑.๑ เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่สำนักงานอนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ของสำนักงาน ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๓ ผู้ใช้งานควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑.๔ การตั้งชื่อเครื่องคอมพิวเตอร์(Computer name) จะต้องกำหนดโดยผู้ดูแลระบบของหน่วยงานเท่านั้น

๑.๕ กรณีส่งเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ตรวจซ่อมโดยผู้รับจ้าง เมื่อตรวจซ่อมเสร็จแล้วต้องให้ผู้ดูแลระบบของหน่วยงาน เป็นผู้ติดตั้งโปรแกรมที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศของสำนักงาน

๑.๖ ระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ต้องมีการ Update service pack และ hot fix ที่เป็น version ล่าสุดเสมอ โดยผู้ดูแลระบบของหน่วยงานเท่านั้น

๑.๗ ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม โปรแกรมยูทิลิตี้ในเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงาน เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบของหน่วยงาน

๑.๘ ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกอย่าง เว้นแต่ ได้รับความเห็นชอบจากผู้ดูแลระบบของหน่วยงาน และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้มีสภาพเดิม

๑.๙ เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส โดยโปรแกรมป้องกันไวรัสของสำนักงาน จากผู้ดูแลระบบ

๑.๑๐ การนำเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกเครื่องออกไปใช้งานนอกสำนักงาน เมื่อนำกลับมาที่สำนักงาน ต้องทำการเชื่อมต่อระบบเครือข่ายภายในสำนักงาน เพื่อทำการอัปเดต (Update) ข้อมูลไวรัสล่าสุด

๑.๑๑ ห้ามเจ้าผู้ใช้งานทุกคนทำการปรับแต่งการตั้งค่าเวลาของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ของสำนักงานทุกเครื่อง และต้องดูแลมิให้เครื่องที่ถือครองถูกแก้ไขการตั้งค่าเวลา ในกรณีที่ค่าเวลาของเครื่อง

คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ถูกแก้ไข เจ้าของเครื่องจะปฏิเสธความรับผิดชอบไม่ได้ และเมื่อรู้ว่าเครื่องมีการแก้ไข การตั้งค่าเวลาต้องแจ้งให้ผู้ดูแลระบบ ทราบทันที

๑.๑๒ การเชื่อมต่อเพื่อใช้ระบบงานจากภายนอกให้ปฏิบัติตามนโยบายการควบคุมการเข้าถึงหรือการใช้งาน ระบบเทคโนโลยีสารสนเทศ (Access Control)

๑.๑๓ ต้องทำการลบข้อมูลทุกครั้งที่มีการเปลี่ยนเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ให้กับเจ้าของเครื่อง รายใหม่ พร้อมทั้งต้องทำการปัด Password สำหรับการเข้าใช้เครื่องคอมพิวเตอร์(ระบบปฏิบัติการ) และต้องทำการ แจ้งการเปลี่ยนแปลงแก่ผู้ดูแลการใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ทุกครั้ง

๒. ความปลอดภัยทางด้านกายภาพ

๒.๑ ผู้ใช้งาน มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย โดยการล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒.๒ ผู้ใช้งาน ไม่ควรเก็บหรือใช้งานเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระแทบ

๒.๓ ไม่ควรใส่เครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๒.๔ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ควรใส่กระเป๋าสำหรับเครื่องเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระแทบกระเทือน

๒.๕ หลีกเลี่ยงการของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่แตกเสียหายได้ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๖ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบา มือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอที่มีรอยขีดข่วนได้

๒.๗ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๒.๘ ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

๒.๙ ไม่ใช่หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ใกล้สิ่งที่เป็นของเหลว

๒.๑๐ ไม่ใช่หรือวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

๒.๑๑ ไม่ควรวางเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้

๒.๑๒ ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน

๓. การเข้าใช้เครื่องคอมพิวเตอร์(ระบบปฏิบัติการ) และ รหัสผ่าน

๓.๑ ผู้ใช้งาน ต้องกำหนดชื่อผู้ใช้(User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์และสื่อสารเคลื่อนที่

๓.๒ ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ในเอกสาร “ข้อกำหนดการจัดการชื่อผู้ใช้และรหัสผ่านของระบบสารสนเทศของ สำนักงาน”

๓.๓ ผู้ใช้งาน ต้องใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ ๑๕ นาทีให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๓.๔ ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๕ ผู้ใช้งาน ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้(User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๔. การสำรองข้อมูลและการกู้คืน

๔.๑ ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกเครื่องมีหน้าที่ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ ได้แก่ CD, DVD หรือ ฮาร์ดดิสก์แบบติดตั้งภายนอก

๔.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของ ข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๕. การป้องกันจากโปรแกรมขูดคำสั่งไม่พึงประสงค์(Malware)

๕.๑ ผู้ใช้งาน ควรตรวจสอบหาไวรัสจากสื่อต่างๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๕.๒ ผู้ใช้งานควรตรวจสอบ File ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือ File ที่ download มาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๕.๓ ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีขูดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือขูดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การใช้งานอินเทอร์เน็ต (Use of the Internet)

แนวทางปฏิบัติ

๑. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่Proxy, Firewall และ IPS/IDS

๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๓. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของสำนักงาน เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม

๔. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสำนักงาน โดยผ่านความเห็นชอบจากผู้บริหารของหน่วยงาน
๕. ผู้ใช้งานต้องไม่กระทำการเปิดเผยข้อมูลสำคัญเกี่ยวกับงานของสำนักงาน ที่ไม่เข้าหลักเกณฑ์การเปิดเผยประกาศอย่างเป็นทางการ ผ่านทางอินเทอร์เน็ตความลับ
๖. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้งาน
๗. การใช้งานเว็บบอร์ด (Web Board) ของสำนักงาน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน
๘. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ
๙. ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๕๐ อย่างเคร่งครัด

การใช้งานจดหมายอิเล็กทรอนิกส์(Use of Electronic Mail)

แนวทางปฏิบัติ

๑. ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน หรือระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐเท่านั้น ในการติดต่อราชการ หรือรับ-ส่งข้อมูลของทางราชการผ่านทางจดหมายอิเล็กทรอนิกส์
๒. ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานและระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งานรวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เมื่อมีการลาออก เป็นต้น
๓. การรับ-ส่งข้อมูลของทางราชการที่เป็นความลับ ห้ามรับ-ส่งผ่านทางระบบจดหมายอิเล็กทรอนิกส์
๔. ผู้ใช้งานรายใหม่จะต้องทำการเปลี่ยนรหัสผ่าน (Password) โดยทันทีเมื่อได้รับรหัสผ่าน (default password) ในการผ่านเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรก โดยต้องกำหนดรหัสผ่านให้มีคุณภาพดีตามที่ระบุไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
๕. รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องแสดงออกมาในรูปของสัญลักษณ์เท่านั้น ได้แก่ “X” หรือ . ในการพิมพ์แต่ละครั้ง
๖. ห้ามผู้ใช้งานตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
๗. ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด โดยเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน
๘. ผู้ใช้งาน ต้องไม่ใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อสำนักงาน หรือละเมิดสิทธิ์สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ สำนักงาน
๙. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ทำการออกจากระบบ (Log out) ทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๐. ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file

๑๑. ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก ในเครื่องที่อยู่ในระบบเครือข่ายของ สำนักงาน

๑๒. ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๓. ผู้ใช้งานต้องไม่ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ประเภทดังต่อไปนี้

๑๔.๑ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ

๑๔.๒ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

๑๔.๓ ข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

๑๔.๔ ข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกอนาจาร

๑๕. ผู้ใช้งานต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๑๖. ผู้ใช้งาน ต้องไม่ใช่ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของสำนักงาน ทำให้เกิดความแตกแยกระหว่างสำนักงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

แนวทางปฏิบัติ

๑ ห้ามใช้ระบบเครือข่ายไร้สายภายในอาคารของสำนักงาน ในระหว่างที่สำนักงาน ยังไม่มีการติดตั้งระบบบริหารจัดการและระบบรักษาความปลอดภัยสำหรับระบบเครือข่ายไร้สายโดยเฉพาะ

๒. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายชั่วคราวของสำนักงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุมัติจาก ผู้อำนวยการโรงพยาบาลทุ่งเสลี่ยมความจำเป็นในการใช้งาน

๓. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบริเวณเครือข่ายไร้สาย

๔. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๕. ผู้ดูแลระบบต้องควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๖. ผู้ดูแลระบบต้องควรเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะต้องเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ไม่สามารถเดาหรือเจาะรหัสได้โดยง่าย

๗. ผู้ดูแลระบบต้องกำหนดค่าใช้ Wep (wired equivalent privacy) หรือ WPA (Wi-Fi protected access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ(access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๘. ผู้ดูแลระบบต้องควรเลือกใช้วิธีการควบคุม MAC Address (media access control address) และชื่อผู้ใช้ (username) รหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้(username) รหัสผ่าน (password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๙. ผู้ดูแลระบบต้องควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๑๐. ผู้ดูแลระบบต้องควรทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๑๑. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการโรงพยาบาลส่งเสริมสุขภาพคลองหลวงแห่งทราบโดยทันที

การสำรองและกู้คืนข้อมูล (Backup and Recovery)

แนวทางปฏิบัติ

๑. การสำรองข้อมูลและกู้คืนข้อมูลในสถานการณ์ปกติเมื่อมีระบบงานใหม่หรือข้อมูลใหม่หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่กำหนดให้ใช้แนวทางปฏิบัติในการจัดทำนโยบายการสำรอง และกู้คืนข้อมูล ดังต่อไปนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดหาระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง

- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาขนาดข้อมูลที่สำรองสำเร็จ/ไม่สำเร็จ เป็นต้น

- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ระบบปฏิบัติการ ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล

- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑.๓ กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๑.๔ กำหนดชนิดของระบบงานนั้น ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อย ต้องประกอบด้วย ข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆที่เกี่ยวข้อง เป็นต้น

๑.๕ กำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบ

๑.๖ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

๑.๗ การเก็บสื่อบันทึกข้อมูลสำรองต้องถูกเก็บไว้บริเวณพื้นที่ภายนอกอาคารของสำนักงานเดือนละ ๒ ครั้ง

๑.๘ ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลในการสำรองข้อมูลทุกครั้ง

๑.๙ ต้องทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

๑.๑๐ จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะที่กำหนด

๑.๑๑ การสำรองข้อมูล และการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการตรวจสอบความถูกต้องเป็นระยะ ๆ

๑.๑๒ ต้องมีการตรวจสอบรายงานบันทึกการเก็บสื่อข้อมูลที่สถานที่เก็บข้อมูลสำรองเป็นประจำทุกปี

๑.๑๓ สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนสื่อตามอายุการใช้งานของสื่อตามประเภทของสื่อแต่ละชนิด

๒. ต้องจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้งผู้ที่ได้รับมอบหมายปฏิบัติหน้าที่ความรับผิดชอบด้วยความรวดเร็ว ถูกต้องตามระเบียบทางราชการ

ทั้งนี้ ตั้งแต่ 17 กุมภาพันธ์ 2563 เป็นต้นไป

(นายบริรักษ์ ลิภนะกุล)

นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)

รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลทุ่งเสลี่ยม