ประกาศโรงพยาบาลกุยบุรี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลกุยบุรี

เพื่อให้การดำเนินการใด ๆ ต่อระบบสารสนเทศโรงพยาบาลกุยบุรี เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่งคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถดำเนินงานต่อไปได้จากภัยคุกคามด้านเครือข่ายต่าง ๆ ซึ่งอาจส่งผลทำให้เกิดความเสียหายต่อระบบสารสนเทศโรงพยาบาลกุยบุรี และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง โรงพยาบาลกุยบุรีจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาลกุยบุรี ทำให้ดำเนินงานได้อย่างปลอดภัย และต่อเนื่อง

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในโรงพยาบาลกุยบุรีได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลกุยบุรี ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยมีการทบทวนนโยบายปีละ ๑ ครั้ง

อาศัยอำนาจตามในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โรงพยาบาลกุยบุรีจึงกำหนดนโยบายและแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลกุยบุรี ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศโรงพยาบาลกุยบุรี” เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโรงพยาบาลกุยบุรี

ข้อ ๒ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ให้ ใช้ประกาศนี้แทน

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลกุยบุรี กำหนดประเด็นสำคัญดังต่อไปนี้

๓.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๓.๑.๑ ส่วนผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๓.๑.๒ นโยบายได้รับการจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถ เข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของโรงพยาบาลกุยบุรี

๓.๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๓.๑.๔ กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๓.๑.๕ กำหนดให้ทบทวนและปรับปรุงนโยบายปีละ ๑ ครั้ง

๓.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบายประกอบด้วย ๓ ส่วน คือ

ข้อที่ ๔ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลกุยบุรีเกิดความเสียหาย หรือได้รับอันตรายจากภัยคุกคามทางด้านต่าง ๆ ผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย ละเว้น หรือฝ่าฝืน การปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของโรงพยาบาลกุยบุรีเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อที่ ๕ ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แบบท้ายประกาศนี้

ข้อที่ ๖ ประกาศนี้ให้บังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ พฤ ๒๕๖๔

(นายวิทยา โปธาสินธุ์)
ทันตแพทย์เชี่ยวชาญ ด้านทันตสาธารณสุข
รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลกุยบุรี

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ โรงพยาบาลกุยบุรี

สารบัญ

ส่วนที่ ๑
คำนิยามและคำจำกัดความ

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

๑. **องค์กร** หมายถึง โรงพยาบาลกุยบุรี

๒. **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารงานของโรงพยาบาลกุยบุรี

๓. **กลุ่มเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานบริหาร จัดการ และดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร เสนอแนะนโยบาย ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายของโรงพยาบาลกุยบุรี

๔. **หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลกุยบุรี ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการ ควบคุมดูแลการใช้งานระบบสารสนเทศ

๕. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของโรงพยาบาลกุยบุรี

๖. **มาตรฐาน** (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๗. **วิธีการปฏิบัติ** (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๘. **แนวทางปฏิบัติ** (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๙. **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของโรงพยาบาลกุยบุรี

๑๐. **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารระดับสูงของโรงพยาบาลกุยบุรี

๑๑. **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรม เครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลเครือข่ายคอมพิวเตอร์

๑๒. **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุขลูกจ้างประจำ ลูกจ้างชั่วคราว และพนักงานเจ้าหน้าที่บริการ

๑๓. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่โรงพยาบาลกุยบุรี อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๔. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๑๕. **สารสนเทศ** (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๖. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๗. **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของโรงพยาบาลกุยบุรี ได้ เช่น ระบบ LAN, ระบบ Internet เป็นต้น

๑๘. **ระบบ LAN และระบบ Intranet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑๙. **ระบบ Internet** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๒๐. **ระบบสารสนเทศ** (Information System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

๒๑. **พื้นที่ใช้งานระบบสารสนเทศ** (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น

๒๑.๑ ห้องปฏิบัติงาน พื้นที่ทำงานทั่วไป (General Working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพา (Notebook) ที่ประจำโต๊ะทำงาน

๒๑.๒ พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) ๒๑.๓ พื้นที่ติดตั้งอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)

๒๑.๔ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

๒๑.๕ พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

๒๒. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๓. **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของ หน่วยงาน เช่นอุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๔. **จดหมายอิเล็กทรอนิกส์** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดย ผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสาร ไปยังผู้รับคนเดียวหรือหลายคนก็ได้มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๒๕. **รหัสผ่าน** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๒๖. **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๒
นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลกุยบุรี

หมวดที่ ๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

๑.๑ ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

วัตถุประสงค์ เพื่อกำหนดทิศทางและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ โดยให้สอดคล้องตามภารกิจขององค์กร และไม่ขัดต่อข้อกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องของโรงพยาบาลกุยบุรี

<u>นโยบาย</u>

๑.๑.๑ เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy of Information Security)

๑) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล โดยนโยบายฯ ดังกล่าวจะต้องได้รับการอนุมัติจากผู้อำนวยการโรงพยาบาลกุยบุรีเพื่อการนำไปใช้

๒) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศต้องกำหนดขอบเขตพื้นที่รักษาความมั่นคงปลอดภัยตามโครงสร้างสายการบังคับบัญชา อันได้แก่ ระดับผู้บริหาร ระดับผู้ดูแลระบบ และระดับเจ้าหน้าที่

๓) นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศต้องกำหนดหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความปลอดภัยอย่างชัดเจน

๔) การกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริการจัดการความมั่นคงปลอดภัย โดยมอบหมายให้กลุ่มเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยในการเข้าถึงและจัดการคอมพิวเตอร์ ระบบเครือข่าย และสารสนเทศ ทั้งหมดของโรงพยาบาล

๑.๑.๒ การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security)

๑) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ ต้องทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อโรงพยาบาลกุยบุรี และต้องมีการติดตาม ทบทวน ประเมินนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างน้อย ๑ ครั้งต่อปี เพื่อให้นโยบายนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศมีประสิทธิภาพอยู่เสมอ

หมวดที่ ๒ โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)

๒.๑ โครงสร้างความมั่นคงปลอดภัยสารสนเทศภายในองค์กร (Internal organization)

วัตถุประสงค์ เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์กร

<u>นโยบาย</u>

๒.๑.๑ การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ(Information security roles and responsibilities)

๑) ผู้อำนวยการโรงพยาบาลกุยบุรีต้องแต่งตั้งกลุ่มหรือคณะกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยระบุอำนาจละหน้าที่ของคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมและชัดเจน ต้องมีการทบทวน แก้ไข หรือแต่งตั้งคณะกรรมการ ทุก ๑ ปี นับจากวันประกาศครั้งก่อน หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อโรงพยาบาลกุยบุรี เพื่อให้มีความสอดคล้องกับกฎหมาย รวมถึงมาตรฐานอื่น ๆ ที่เกี่ยวข้อง

๒.๑.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

๑) ผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (CSO) ต้องกำหนดอำนาจ หน้าที่ของคณะกรรมการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และรับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลกุยบุรี

๒) ผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (CSO) ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลกุยบุรี

๓) ผู้ใช้งาน เจ้าหน้าที่ และหน่วยงานภายนอกต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวทางปฏิบัติของโรงพยาบาลกุยบุรีในการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลกุยบุรี

๒.๑.๓ การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities)

๑) ผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (CSO) ต้องจัดตั้งเจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการประสานงาน

๒) ผู้อำนวยการโรงพยาบาลกุยบุรี ต้องจัดทำรายชื่อและดำเนินการมอบอำนาจให้เจ้าหน้าที่เพื่อติดต่อประสานงานกับหน่วยงานอื่น ๆ

๒.๑.๔ ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)

๑) ผู้บริหารระดับสูงทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (CSO) ต้องมีการตรวจสอบการบริหารจัดการ ระบุความมั่นคงปลอดภัยสารสนเทศสำหรับโครงการที่เกี่ยวข้องกับสารสนเทศ

๒.๒ อุปกรณ์คอมพิวเตอร์แบบพกพา Digital device รวมถึงการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและนำไปใช้ปฏิบัติงานภายนอกองค์กร และสินทรัพย์สารสนเทศจากการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา รวมทั้งการปฏิบัติงานนอกหน่วยงานจากระยะไกล

<u>นโยบาย</u>

๒.๒.๑ นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile and Digital Device Policy)

๑) ต้องกำหนดวิธีการป้องกันข้อมูลและสินทรัพย์สารสนเทศที่อยู่ในอุปกรณ์คอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารอื่น ๆ โดยให้เป็นไปตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

๒.๒.๒ การปฏิบัติงานจากระยะไกลภายนอกโรงพยาบาล (Teleworking)

๑) อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานโดยต้องใช้งานผ่านช่องทางที่ศูนย์คอมพิวเตอร์จัดเตรียมไว้ให้ และต้องมีการตรวจสอบตัวตนก่อนการเข้าถึง โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๒) ต้องไม่นำข้อมูลที่เป็นความลับขององค์กรเก็บหรือบันทึกไว้ในอุปกรณ์ส่วนตัว หากมีความจำเป็นเมื่อใช้งานเสร็จผู้ใช้งานควบดำเนินการลบข้อมูลที่สำคัญนั้นทิ้งโดยทันทีหลังเลิกใช้งาน

หมวดที่ ๓ ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

๓.๑ การสรรหาบุคลากรก่อนการจ้างงาน (Prior to employment)

วัตถุประสงค์ เพื่อคัดสรรพนักงานที่ตรงกับความต้องการ และเพื่อให้พนักงานเข้าใจในหน้าที่และความรับผิดชอบ

<u>นโยบาย</u>

๓.๑.๑ ข้อกำหนดการตรวจสอบและอ้างอิงบริษัท (Screening)

๑) กำหนดนโยบายความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล โดยให้เป็นไปตามแนวปฏิบัติความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล

๒) กำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลกุยบุรี

๓.๑.๒ ข้อกำหนดการตรวจสอบของบุคลากรหรือทีมงานที่จะเข้ามาปฏิบัติงานในโรงพยาบาลกุยบุรี (Term and Conditions of employment)

๑) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน จะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลกุยบุรี โดยให้เป็นไปตามแนวปฏิบัติความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล

๓.๒. ระหว่างการจ้างงาน (During employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

<u>นโยบาย</u>

๓.๒.๑ หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

๑) ต้องให้ผู้ใช้งาน และหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบ นโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

๓.๒.๒ การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)

๑) เจ้าหน้าที่ใหม่ต้องได้รับการอบรมเกี่ยวกับเรื่องนโยบายการรักษาความมั่นคงปลอดภัย โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศพนักงาน โดยให้เป็นไปตามแนวปฏิบัติความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล

๓.๓. การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ เพื่อให้ยกเลิกหรือเปลี่ยนแปลงสิทธิกับเจ้าหน้าที่ หรือเจ้าหน้าที่จากหน่วยงานภายนอกที่ถูกยกเลิกหรือเปลี่ยนแปลงการจ้างงาน เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

<u>นโยบาย</u>

๓.๓.๑ การสิ้นสุดหรือการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)

๑) เพื่อให้การบริหารจัดการบัญชีผู้ใช้เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด เจ้าหน้าที่บุคคลที่ดูแลทรัพยากรบุคคลของโรงพยาบาลกุยบุรี ต้องแจ้งให้ศูนย์คอมพิวเตอร์ทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงาน และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

๒) ทรัพย์สินโรงพยาบาลกุยบุรีที่สำคัญหรือเป็นความลับของโรงพยาบาลกุยบุรี ห้ามนำออกนอกโรงพยาบาลกุยบุรีโดยเด็ดขาด หรือสำรองข้อมูลไว้ที่อื่นนอกโรงพยาบาลกุยบุรี

หมวดที่ ๔ การบริหารจัดการทรัพย์สิน (Asset Management)

๔.๑ หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์ เพื่อให้ระบุสินทรัพย์ของโรงพยาบาลและกำหนดหน้าที่ความรับผิดชอบในการป้องกันสินทรัพย์อย่างเหมาะสม

นโยบาย

๔.๑.๑ บัญชีทรัพย์สิน (Inventory of assets)

๑) หน่วยงานต้องจัดทำและเก็บทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์ อุปกรณ์ต่อพ่วงคอมพิวเตอร์เครือข่ายและชุดโปรแกรมสำเร็จรูป) อันประกอบด้วย ชื่ออุปกรณ์ หมายเลขครุภัณฑ์ ปีที่ได้รับ สถานที่ใช้งาน และผู้รับผิดชอบอย่างชัดเจน เพื่อเป็นข้อมูลสำหรับการนำไปวิเคราะห์และประเมินความเสี่ยง รวมถึงการบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

๒) ต้องมีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินตามระยะเวลาที่กำหนดเช่น มีการตรวจสอบปรับปรุงทะเบียนบัญชีทรัพย์สินทุก ๆ ๑ ปี หรือเมื่อมีการเปลี่ยนแปลงของอุปกรณ์

๔.๑.๒ ผู้ถือครองทรัพย์สิน (Ownership of assets)

๑) หน่วยงานต้องระบุชื่อผู้รับผิดชอบต่อทรัพย์สินอย่างชัดเจนและมีการทบทวนปรับปรุงรายชื่อผู้รับผิดชอบต่อทรัพย์สินทุกครั้งที่มีการเปลี่ยนแปลง

๔.๑.๓ การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

๑) ต้องมีการจัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับ ภารกิจและบุคลากร โดยมีการทบทวนปีละ ๑ ครั้ง

๒) ต้องจัดทำคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ อุปกรณ์ต่อพ่วงคอมพิวเตอร์ เครือข่ายและชุดโปรแกรมสำเร็จรูป รวมถึงกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์

๔.๑.๔ การคืนทรัพย์สิน (Return of assets)

๑) มีการกำหนดนโยบายให้ผู้ใช้ต้องคืนทรัพย์สินของโรงพยาบาลกุยบุรีทั้งหมดที่โรงพยาบาลกุยบุรีถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา สิ้นสุดข้อตกลงการจ้าง หรือทุกครั้งที่มีการเปลี่ยนแปลง

๒) พนักงานที่สิ้นสุดสัญญาจ้างงาน หรือสิ้นสุดโครงการต้องคืนทรัพย์สินสารสนเทศต่าง ๆ ที่รับผิดชอบทั้งหมดเช่น กุญแจ บัตรประจำตัว คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เป็นต้น

๔.๒ การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์ เพื่อให้สินทรัพย์สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

นโยบาย

๔.๒.๑ ชั้นความลับของสารสนเทศ (Classification of information)

๑) ต้องทำการจัดหมวดหมู่สินทรัพย์ กำหนดระดับความสำคัญ และกำหนดชั้นความลับเพื่อป้องกัน สารสนเทศให้มีความปลอดภัย โดยปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ. ๒๕๔๔

๒) มีการกำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกกิจการ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้งานอุปกรณ์

๔.๒.๒ การบ่งชี้สารสนเทศ (Labeling of information)

๑) ต้องจัดทำป้ายชื่อสินทรัพย์อย่างชัดเจน

หมวดที่ ๕ การควบคุมการเข้าถึง (Access Control)

๕.๑ ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)
วัตถุประสงค์ เพื่อจำกัดการเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต
<u>นโยบาย</u>

๕.๑.๑ นโยบายควบคุมการเข้าถึง (Access Control Policy)

๑) การกำหนดผู้รับผิดชอบภายในโรงพยาบาลกุยบุรีและร่วมกันพิจารณาออกข้อกำหนดในการเข้าถึงระบบ และมีการประกาศใช้อย่างเป็นทางการ เช่น กำหนดสิทธิในการเข้าใช้งานในอุปกรณ์คอมพิวเตอร์, กำหนดสิทธิในการเข้าใช้งานระบบ

๕.๑.๒ การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services)

๑) การกำหนดให้มีการพิจารณาสิทธิในการเข้าถึงข้อมูลของผู้ใช้โดยกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ, มีการทบทวนสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่เดิม

๕.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
วัตถุประสงค์ เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้
<u>นโยบาย</u>

๕.๒.๑ การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration)

๑) การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งานระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพต้องยกเลิกออกจากระบบทันที

๕.๒.๒ การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning)

๑) ผู้ดูแลระบบต้องมีกระบวนการกำหนดสิทธิ์ให้ครอบคลุมผู้ใช้งานให้ครบทุกประเภทและทุกการบริการของระบบสารสนเทศ

๕.๒.๓ การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

๑) ผู้ดูแลระบบต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบ

๕.๒.๔ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

๑) ผู้ดูแลระบบต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้อย่างน้อยปีละ ๑ ครั้ง

๕.๒.๕ การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal of adjustment of access rights)

๑) เมื่อเจ้าหน้าที่ เปลี่ยนแปลง ปรับเปลี่ยน โยกย้าย การทำงานหรือสัญญาสิ้นสุดการจ้าง ผู้ดูแลระบบต้องทำการถอดถอนหรือปรับปรุงสิทธิให้ถูกต้อง

๕.๓ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

วัตถุประสงค์ เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

<u>นโยบาย</u>

๕.๓.๑ การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information)

๑) ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศองค์กร การกำหนดการเปลี่ยนแปลง การยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

๒) รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย

๓) ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด

๔) รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้

๕.๔ การควบคุมการเข้าถึงระบบ (System and application access Control)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบสารสนเทศและข้อมูลบนระบบสารสนเทศโดยไม่ได้รับอนุญาต

<u>นโยบาย</u>

๕.๔.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

๑) ต้องควบคุมการใช้งานสารสนเทศในระบบสารสนเทศกำหนดสิทธิในการใช้งาน ได้แก่ เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้งานที่สามารถใช้งานได้ ตรวจสอบว่า สารสนเทศที่อนุญาตให้ใช้งานนั้น มีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็น และกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๕.๔.๒ ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure tog-on procedures)

๑) การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัยตาม แนวทางปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๕.๔.๓ การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)

๑) ต้องกำหนดให้ควบคุมการใช้โปรแกรมอรรถประโยชน์สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้

๕.๔.๔ การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to program source code)

๑) มีการกำหนดระดับความปลอดภัยของเข้าใช้ซอร์สโค้ดของโปรแกรมเป็นลำดับขั้นความปลอดภัยเพื่อป้องกันเกี่ยวกับข้อมูลสูญหายหรือ มีซอร์สโค้ดที่ไม่ได้รับการอัพเดตรายการแก้ไขเข้าไปอย่างถูกต้อง

หมวดที่ ๖ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

๖.๑ พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

<u>นโยบาย</u>

๖.๑.๑ ขอบเขตพื้นที่หรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

๑) ต้องแบ่งพื้นที่อย่างชัดเจน และกำหนดระดับการควบคุมเพื่อป้องกันการเข้าถึงสินทรัพย์สารสนเทศที่มีความสำคัญ

๒) ต้องจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ

๖.๑.๒ การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

๑) ต้องควบคุมให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่

๒) ต้องกำหนดสิทธิ และช่วงเวลาในการผ่านเข้าออกพื้นที่

๓) ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัว หรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๖.๑.๓ การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงานและอุปกรณ์ (securing office, room and facilities)

๑) ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก

๒) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๕) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๖.๑.๔ การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (protecting against external and environment threats)

๑) ต้องมีวิธีป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น เช่น

- มีระบบเตือนภัยฉุกเฉิน กรณีไฟไหม น้ำท่วม
- มีอุปกรณ์ดับเพลิงตามมาตรฐาน
- มีระบบปรับอากาศและความคุมความชื้น
- จัดทำแผน คู่มือ การซักซ้อม และการสรุปผล การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม
- แผนการใช้งานด้านระบบคอมพิวเตอร์สำรองเมื่อมีเหตุการณ์ ด้านภัยพิบัติของสภาพแวดล้อมขึ้น

๖.๑.๕ การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working is secure areas)
ขั้นตอนปฏิบัติสำหรับการปฏิบัติการในพื้นที่

๑) ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น “ห้ามเข้าก่อนได้รับอนุญาต

๒) กรณีที่ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกสำนักงานต้องมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ บันทึกการทำงาน (log files) ของบุคคลภายนอก และกำหนดให้บุคคลภายนอกรายงานการปฏิบัติงาน เป็นต้น

๖.๑.๖ พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)

๑) ต้องแยกจุดที่รับส่งสิ่งของ ออกจากพื้นที่ที่มีอุปกรณ์ประมวลผลสารสนเทศ และดำเนินการแกะหีบห่อหรือตรวจสอบให้เสร็จสิ้น ก่อนนำเข้าสู่พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

๖.๒ อุปกรณ์ (Equipment)

วัตถุประสงค์ เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อสินทรัพย์และป้องกันการหยุดชะงักต่อการดำเนินงานของโรงพยาบาลกุยบุรี

<u>นโยบาย</u>

๖.๒.๑ การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)

๑) การจัดตั้ง หรือการจัดวางอุปกรณ์สินทรัพย์สารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวางในที่เข้าถึงได้ยาก

๖.๒.๒ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๑) อุปกรณ์ที่มีความสำคัญสูง ควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า

- ความเสี่ยงสูง ต้องมีระบบสำรองไฟฟ้าทั้ง UPS และเครื่องกำเนิดไฟฟ้า
- ความเสี่ยงปานกลาง ต้องมีระบบสำรองไฟฟ้าUPS
- ความเสี่ยงต่ำมีระบบสำรองไฟฟ้าหรือไม่ก็ได้

๖.๒.๓ ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

๑) การเดินสายสัญญาณต้องคำนึงถึงผลกระทบต่อความเสี่ยงที่อาจเกิดขึ้นเพื่อป้องกันสัญญาณรบกวน เช่น

- ความเสี่ยงสูง การเดินสายต้องใช้สายป้องกันการรบกวนสัญญาณและการเข้าถึงสายสัญญาณ
- ความเสี่ยงปานกลาง การเดินสายต้องป้องกันการเข้าถึงสายสัญญาณ
- ความเสี่ยงต่ำใช้สายสัญญาณธรรมดา
- ต้องมีแผนการตรวจสอบระบบการเดินสายไฟ สายเคเบิ้ล สายสื่อสาร ฯลฯ

๒) ต้องมีการทำป้ายสายสัญญาณชัดเจน และเมื่อมีการเปลี่ยนแปลงต้องมีการปรับปรุงป้ายสายสัญญาณให้ถูกต้อง

๖.๒.๔ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑) ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือมากกว่าตามระดับความสำคัญ เช่น

- ระบบที่มีความเสี่ยงสูงต้องบำรุงรักษาทุก ๑ เดือน
- ระบบที่มีความเสี่ยงปานกลางต้องบำรุงรักษาทุก ๓ เดือน
- ระบบที่มีความเสี่ยงต่ำต้องบำรุงรักษาทุก ๑๒ เดือน

๖.๒.๕ การนำทรัพย์สินของโรงพยาบาลกุยบุรีออกนอกสำนักงาน (Removal of assets)

๑) ห้ามนำสินทรัพย์สารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีระบบการควบคุมดูแลทรัพย์สิน การลงทะเบียนทรัพย์สิน/ครุภัณฑ์ แบบฟอร์มการยืม-คืนทรัพย์สิน

๖.๒.๖ ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกส่วนงาน (Security of equipment and assets off-premises)

๑) ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยตามความเสี่ยง เช่น

- กำหนดรหัสการเข้าถึงการใช้งานอุปกรณ์คอมพิวเตอร์
- กำหนดผู้รับผิดชอบและดูแลอุปกรณ์
- กำหนดผู้รับผิดชอบและดูแลอุปกรณ์ห้องแม่ข่าย
- มีระบบป้องกันความปลอดภัย เช่น antivirus การกำหนดสิทธิ์ใช้งาน

๖.๒.๗ ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

๑) ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายให้สิ้นซาก

๖.๒.๘ อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended use equipment)

๑) ต้องป้องกันให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สินทรัพย์สารสนเทศที่ไม่มีผู้ดูแล

๖.๒.๙ นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

๑) เจ้าหน้าที่ต้องควบคุมเอกสาร ข้อมูล หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บหรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

หมวดที่ ๗ การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

๗.๑ ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบการพัฒนา ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

<u>นโยบาย</u>

๗.๑.๑ การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification

๑) ระบบสารสนเทศใหม่ ต้องมีการรักษาความปลอดภัยที่สอดคล้องและสามารถเชื่อมโยงกับระบบเดิมได้

๒) ระบบสารสนเทศเก่า จะต้องมีการป้องกันการเข้าใช้ server โดยอนุญาตให้เฉพาะบุคคลที่มีหน้าที่การทำงานโดยใช้การ login ด้วย user name และ password ของบุคคลนั้น และการยืนยันการเข้าใช้ว่าเป็นบุคคลไม่ใช่ program การ update ต่าง ๆ ต้องเป็นแบบ manual เท่านั้น

๗.๑.๒ ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

๑) สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกันจากการเปลี่ยนแปลงข้อมูลบนเครือข่ายสาธารณะโดยการกำหนด username และ password ของผู้เข้าถึงข้อมูล

๒) ข้อมูลต้องระบุได้ว่าบุคคลใดเป็นผู้สร้างข้อมูลและมีการสำเนา/สำรองข้อมูลทุกครั้งเพื่อสามารถย้อนดูข้อมูลเก่า ณ เวลานั้นได้

๓) การเปิดเผยข้อมูลบนเครือข่ายสาธารณะ ต้องได้รับการอนุญาตของผู้ดูแลระบบเท่านั้น

๔) ไม่อนุญาตให้แก้ไขข้อมูลใดๆ ที่ถูกสร้างขึ้น

๗.๑.๓ การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application Services transactions)

๑) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

๒) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ให้มีการตั้งระบบตอบกลับการส่งข้อมูลพร้อมทั้งมีการเข้ารหัสข้อมูลและมีการยืนยันตัวบุคคล

๗.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

<u>นโยบาย</u>

๗.๒.๑ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

๑) ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง เช่น ต้องมีการอนุมัติโดยผู้มีอำนาจ

๒) มีการแต่งตั้งผู้ดูแลควบคุมระบบซอฟต์แวร์

๗.๒.๒ ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

๑) ผู้พัฒนาระบบสารสนเทศต้องจัดทำแนวปฏิบัติการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

๗.๒.๓ การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

๑) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๗.๒.๔ การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

๑) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้ เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

๗.๒.๕ สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

๑) หากมีความจำเป็นต้องให้หน่วยงานภายนอกเข้ามาพัฒนาระบบภายในหน่วยงาน ต้องกำหนดสภาพแวดล้อมที่มีความมั่นคงปลอดภัย

๒) มีการแบ่งสิทธิตามหน้าที่การทำงานอย่างชัดเจน เช่น ผู้พัฒนาระบบ ผู้ดูแลฐานข้อมูล

๓) หน่วยงานภายนอกต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

๗.๒.๖ การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

๑) ต้องมีการประชุมติดตาม และบันทึกการประชุมกิจกรรมการพัฒนาระบบอย่างสม่ำเสมอ

๒) หากพบการละเมิดความมั่นคงปลอดภัยต้องแจ้งให้ผู้บังคับบัญชาทราบ

๗.๒.๗ การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

๑) การทดสอบด้านความมั่นคงปลอดภัยต้องทำการทดสอบการใช้งานในช่วงของการพัฒนา หากไม่ผ่านการทดสอบต้องแก้ไขให้แล้วเสร็จก่อนการส่งมอบ

๗.๒.๘ การทดสอบเพื่อรับรองระบบ (System acceptance testing)

๑) จัดบุคลากรในการทดลองและประเมินผลการใช้งานของระบบการทำงานของฟังก์ชั่นทุกฟังก์ชั่นการทำงาน ต้องทำงานถูกต้อง และสามารถทำงานได้

๗.๓ ข้อมูลสำหรับการทดสอบ (Test data)

วัตถุประสงค์ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

<u>นโยบาย</u>

๗.๓.๑ การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)

๑) ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบ ในการรักษาข้อมูลและเจ้าของข้อมูลนั้นๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่า ได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวันเวลา และหน่วยงานที่ทดสอบ

หมวดที่ ๘ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๘.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

นโยบาย

๘.๑.๑ หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

๑) มีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

๒) มีการกำหนดผู้รับผิดชอบและหน้าที่รับผิดชอบอย่างชัดเจน

๓) มีมาตรการในการควบคุมกำกับดูแลผู้รับผิดชอบ เพื่อให้การปฏิบัติเป็นไปในทางเดียวกัน

๘.๑.๒ การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)

๑) มีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

๒) จัดทำการรายงานผ่านช่องทางที่สามารถแจ้งเตือนแก่ผู้ดูแลระบบทราบให้รวดเร็วมากที่สุด

๓) เมื่อมีสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศเกิดขึ้น ให้ผู้ดูแลทำรายงานเสนอต่อผู้บังคับบัญชาในทันที

๘.๑.๓ การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses)

๑) มีการกำหนดเกณฑ์เหตุการณ์อยู่ในระดับต่ำผู้ดูแลระบบสารสนเทศของโรงพยาบาล สามารถแก้ไขเหตุการณ์ที่เกิดขึ้นเองได้ เช่น การติดไวรัส เป็นต้น

๒) มีการกำหนดเกณฑ์เหตุการณ์อยู่ในระดับกลางผู้ดูแลระบบสารสนเทศของโรงพยาบาล แจ้งให้ผู้อำนวยการทราบถึงเหตุการณ์ที่เกิดขึ้น หากเหตุการณ์ที่เกิดขึ้น หน่วยงานที่เกิดเหตุประเมินความเสี่ยงแล้วให้ทำการแจ้งเป็นลายลักษณ์อักษร แจ้งไปยังศูนย์คอมพิวเตอร์ของโรงพยาบาลกุยบุรี เพื่อให้ศูนย์คอมพิวเตอร์เข้ามาแก้ไขเหตุการณ์ที่เกิดขึ้น

๓) มีการกำหนดเกณฑ์เหตุการณ์อยู่ในระดับสูงผู้ดูแลระบบสารสนเทศของโรงพยาบาล ต้องทำการแจ้งไปยังศูนย์คอมพิวเตอร์โรงพยาบาลกุยบุรี อย่างเร่งด่วนหากเหตุการณ์ที่เกิดขึ้นเป็นเหตุการณ์ร้ายแรงและเร่งด่วน เพื่อหาแนวทางในการแก้ไขปัญหา จากนั้นทำการสรุปปัญหาที่เกิดขึ้นกับระบบสารสนเทศให้ผู้อำนวยการทราบ

๘.๑.๔ การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

๘.๑.๔.๑ หัวหน้าศูนย์คอมพิวเตอร์ ต้องกำหนดนโยบายให้กับบุคลากรและผู้ดูแลระบบในหน่วยงานนั้น ๆ ปฏิบัติตามนโยบายที่วางไว้

๑) ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติและการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ จะถูกทำการวิเคราะห์ และหาสาเหตุของการบุกรุก ในระบบสารสนเทศของโรงพยาบาลกุยบุรี เพื่อเป็นเครื่องมือสืบสวนหาบุคคลที่โจมตี บุกรุกหรือใช้ระบบในทางที่ผิด

๘.๑.๔.๒ ผู้ดูแลระบบ ต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ เหตุการณ์ผิดปกติ และการแจ้งเตือนต่าง ๆ ที่อุปกรณ์ตรวจพบ

๑) ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุกหรือโจมตีโรงพยาบาลกุยบุรี เป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟวอล์ เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตราย ที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ hacker รวมทั้ง ไวรัสประเภทต่าง ๆ

๘.๑.๔.๓ ผู้ดูแลระบบ ผู้ดูแลระบบต้องมีการบริหารจัดการการบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับโรงพยาบาลกุยบุรี

๑) ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับโรงพยาบาลกุยบุรี และจัดทำวิธีปฏิบัติที่ถูกต้องให้กับโรงพยาบาลกุยบุรี เพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ

๘.๑.๕ การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

๑) เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

๒) มีการจัดทำขั้นตอนการปฏิบัติอย่างชัดเจนในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศ

๓) กรณีเกิดปัญหาให้รายงานเหตุการณ์ต่อผู้บังคับบัญชาทุกครั้ง

๘.๑.๖ การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

๑) มีการแจ้งเวียนเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น ให้เจ้าหน้าที่ภายในหน่วยงานทราบ

๘.๑.๗ การเก็บรวบรวมหลักฐาน (Collection of evidence)

๑) มีการเก็บหลักฐานด้านสารสนเทศในสถานที่ปลอดภัย มีข้อกำหนดควบคุมการนำมาใช้เพื่อไม่ให้เกิดการสูญหายและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

ส่วนที่ ๓
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลกุยบุรี

แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดหลักเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจ

๓. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ (๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ หรือเจ้าของข้อมูล หรือเจ้าของระบบตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ (๒) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลกุยบุรี จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้ากลุ่มงานของหน่วยงาน และหัวหน้าศูนย์คอมพิวเตอร์พิจารณา

ข้อ (๓) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

๑.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๑.๒ กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลกุยบุรี จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้ากลุ่มงานของหน่วยงาน และหัวหน้าศูนย์คอมพิวเตอร์พิจารณา

(๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๒.๑ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๒.๒ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายร้ายแรงที่สุด
- ข้อมูลลับมาก หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายร้ายแรง
- ข้อมูลลับ หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๓ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหารโรงพยาบาลกุยบุรี
- ระดับชั้นสำหรับผู้ดูแลระบบของโรงพยาบาลกุยบุรี
- ระดับชั้นสำหรับเจ้าหน้าที่ของโรงพยาบาลกุยบุรี
- ระดับชั้นสำหรับบุคคลทั่วไปมาใช้บริการของโรงพยาบาลกุยบุรี

ข้อ (๔) ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของโรงพยาบาลกุยบุรี และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ (๕) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ (๖) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกการผ่านเข้า - ออกสถานที่ตั้งระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ (๗) กำหนดระยะเวลาเข้าถึงระบบสารสนเทศ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ (๘) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

(๔) ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้ เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ (๙) ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ (๑๐) ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

(๒) จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน ทำการ หรือเมื่อเปลี่ยนแปลงตำแหน่งต้องดำเนินการภายใน ๗ วัน ทำการ

ข้อ (๑๑) การบริหารจัดการรหัสผ่าน

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้และรหัสผ่านต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๔) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน

(๕) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นกำหนดระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับ ว่าสามารถเข้าถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ (๑๒) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๑) ควบคุมการเข้าถึงแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) กำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๖) เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน

ข้อ (๑๓) ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศของโรงพยาบาลกุยบุรี พิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างโรงพยาบาลกุยบุรีกับหน่วยงานที่มาขอเชื่อมโยง

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ (๑๔) การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๑) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้งาน และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ไม่เกิน ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ (๑๕) การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษา ความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสำกล

ข้อ (๑๖) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้เป็นความรับผิดชอบ ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ (๑๗) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของโรงพยาบาลกุยบุรี และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากใส่รหัสผิดเกิน ๓ ครั้งก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนก่อนการใช้งานทุกครั้ง

(๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๓๐ นาที

ข้อ (๑๘) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลกุยบุรี หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ (๑๙) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของโรงพยาบาลกุยบุรี ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้อำนวยการโรงพยาบาลกุยบุรี

ข้อ (๒๐) ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลกุยบุรี และข้อมูลของผู้มารับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิดการเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ (๒๑) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ (๒๒) ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร โรงพยาบาลกุยบุรีจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่โรงพยาบาลกุยบุรีต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาล ซึ่งโรงพยาบาลกุยบุรีอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ (๒๓) ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายความว่า วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน แต่ละเครื่อง - ต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้มข้อมูล (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เว้นแต่จะได้รับอนุญาต จากผู้อำนวยการโรงพยาบาลกุยบุรี

ข้อ (๒๔) ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างปฏิบัติงาน

ข้อ (๒๕) ห้ามใช้สินทรัพย์ของโรงพยาบาลกุยบุรี ที่จัดเตรียมให้เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของโรงพยาบาลกุยบุรี

ข้อ (๒๖) ห้ามใช้สินทรัพย์ของโรงพยาบาลกุยบุรี เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้การโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของโรงพยาบาลกุยบุรี

ข้อ (๒๗) ห้ามใช้สินทรัพย์ของโรงพยาบาลกุยบุรี เพื่อประโยชน์ทางการค้า ที่มิใช้ภารกิจโรงพยาบาลกุยบุรี

ข้อ (๒๘) ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของโรงพยาบาลกุยบุรีโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ (๒๙) ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของโรงพยาบาลกุยบุรี ต้องหยุดชะงัก

ข้อ (๓๐) ห้ามใช้ระบบสารสนเทศของโรงพยาบาลกุยบุรี เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ (๓๑) ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ (๓๒) ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของโรงพยาบาลกุยบุรี โดยไม่ได้รับอนุญาตจากผู้อำนวยการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ (๓๓) มาตรการควบคุมการเข้า-ออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๑) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร "ขออนุญาตเข้า-ออกอาคารของโรงพยาบาลกุยบุรี (บุคคลภายนอก)" ให้ถูกต้องชัดเจน

ข้อ (๓๔) ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของโรงพยาบาลกุยบุรี ต้องได้รับอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์และต้องปฏิบัติตามแนวปฏิบัตินี้โดยเคร่งครัด

ข้อ (๓๕) การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลต่อผลกระทบต่อการทำงานของระบบและผู้ใช้งานอื่น

ข้อ (๓๖) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณ (Switch) อุปกรณ์เชื่อมต่อระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ (๓๗) ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๑) ต้องจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของโรงพยาบาลกุยบุรี ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายทั้งหมดต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาลกุยบุรีในลักษณะที่ผิดปกติ

(๖) การเข้าสู่ระบบเครือข่ายภายในโรงพยาบาลกุยบุรี โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของโรงพยาบาลกุยบุรี

(๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๙) การระบุอุปกรณ์บนเครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ตั้ง
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

- กรณีอุปกรณ์มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้ หรือไม่สามารถเชื่อมต่อได้

- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

ข้อ (๓๘) ผู้ดูแลระบบ ต้องบริหาร ควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software

ข้อ (๓๙) การติดตั้งหรือปรับปรุงซอฟต์แวร์ระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบก่อนดำเนินการ

ข้อ (๔๐) กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ (๔๑) การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ ๒๕๖๐

ข้อ (๔๒) กำหนดมาตรฐานควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจากผู้ใช้งานภายนอกโรงพยาบาลกุยบุรี เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติดังต่อไปนี้

(๑) บุคลากรจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของโรงพยาบาลกุยบุรี จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศโรงพยาบาลกุยบุรี

(๒) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าระบบอย่างรัดกุม

(๓) วิธีการใด ๆ ที่สามารถเข้าถึงข้อมูลและระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศโรงพยาบาลกุยบุรี

(๔) การเข้าถึงระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินการกับโรงพยาบาลกุยบุรี อย่างเพียงพอ

(๕) การเข้าถึงระบบเครือข่ายภายในและระบบสารสนเทศในโรงพยาบาลกุยบุรี จากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ (๔๓) กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๑) Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามความจำเป็นในการใช้งาน เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(๒) Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ (๔๔) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งให้บุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ (๔๕) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกโรงพยาบาลกุยบุรี ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ (๔๖) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของโรงพยาบาลกุยบุรี ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย

การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ (๔๗) IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ (๔๘) การใช้งานเครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจากัดการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ (๔๙) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของโรงพยาบาลกุยบุรี (โดยปฏิบัติติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน โดยปฏิบัติติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในโรงพยาบาลกุยบุรี เป็นต้น

ข้อ (๕๐) กำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งาน

(๑) ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(๒) หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

(๓) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

(๔) ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งานทุกครั้ง

(๕) ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของโรงพยาบาลกุยบุรีร่วมกัน

(๖) ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่ได้อยู่ที่หน้าจอเป็นเวลานาน

(๗) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศของโรงพยาบาลกุยบุรี

(๘) ซอฟต์แวร์ที่โรงพยาบาลกุยบุรี ใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้ได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

(๙) ซอฟต์แวร์ที่โรงพยาบาลกุยบุรี จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

(๑๐) ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของโรงพยาบาลกุยบุรี เพื่อประโยชน์ทางการค้า

(๑๑) ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

(๑๒) ห้ามผู้ใช้งานของโรงพยาบาลกุยบุรี ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาต

ข้อ (๕๑) การระบุยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ (๕๒) การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๑) การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

(๒) โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตได้

ข้อ (๕๓) การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out) ให้ดำเนินการ ดังนี้

(๑) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด และกำหนดให้ใช้งานได้ตามช่วงเวลาการทำงานที่หน่วยงานกำหนดเท่านั้น

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกโรงพยาบาลกุยบุรี) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ข้อ (๕๔) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) เช่น การลาออก หรือการเปลี่ยนตำแหน่งภายในโรงพยาบาลกุยบุรี เป็นต้น

ข้อ (๕๕) ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๓๐ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการลงบันทึกเข้าใช้งานก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ (๕๖) ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ (๕๗) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอก โรงพยาบาลกุยบุรี เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ (๕๘) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ

(๒) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

ข้อ (๕๙) การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๗ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual Property and Preventing Malware)

ข้อ (๖๐) โรงพยาบาลกุยบุรีได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่โรงพยาบาลกุยบุรีอนุญาตให้ใช้งานหรือที่โรงพยาบาลกุยบุรี มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้ได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐาน ละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ (๖๑) ซอฟต์แวร์ที่โรงพยาบาลกุยบุรี ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ (๖๒) คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่โรงพยาบาลกุยบุรี ได้ประกาศให้ใช้เท่านั้น

ข้อ (๖๓) บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ (๖๔) ผู้ใช้งานต้องการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ (๖๕) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ (๖๖) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบทราบทันที

ข้อ (๖๗) ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของโรงพยาบาลกุยบุรี หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้อำนวยการ

ข้อ (๖๘) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของโรงพยาบาลกุยบุรี สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการ ดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครอง ทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับ หนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ (License) การใช้ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณี อันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ (๖๙) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอกโรงพยาบาลกุยบุรี ต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

ส่วนที่ ๘ การควบคุมการเข้าระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ (๖๙) ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ (๗๐) ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สายมาใช้งาน

ข้อ (๗๑) ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณแบบไร้สาย

ข้อ (๗๒) ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งานและรหัสผ่าน ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งานและรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ (๗๓) ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายนอกโรงพยาบาลกุยบุรี

ข้อ (๗๔) ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในโรงพยาบาลกุยบุรี ผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกจากระบบเครือข่ายไร้สาย

ข้อ (๗๕) ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ (๗๖) ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศทราบทันที

ข้อ (๗๗) ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต และฐานข้อมูลภายในต่าง ๆ ของโรงพยาบาลกุยบุรี

ข้อ (๗๘) ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของโรงพยาบาลกุยบุรี จะต้องได้รับพิจารณาอนุญาตจากหัวหน้าศูนย์คอมพิวเตอร์อย่างเป็นลายลักษณ์อักษร

ข้อ (๙๗) ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้ง มีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ ๙ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ (๙๘) ศูนย์คอมพิวเตอร์โรงพยาบาลกุยบุรีมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ (๙๙) การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ (๑๐๐) การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้พอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหัวหน้ากลุ่มงานสารสนเทศก่อน

ส่วนที่ ๑๐ การควบคุมการใช้อินเตอร์เน็ต (Internet)

ข้อ (๑๐๑) ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่โรงพยาบาลกุยบุรี จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านทางช่องทางอื่น เช่น Dial-Up, Modem, etc. ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้อำนวยการเป็นลายลักษณ์อักษร

ข้อ (๑๐๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ (๑๐๓) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ (๑๐๔) ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของโรงพยาบาลกุยบุรี เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับโรงพยาบาลกุยบุรี

ข้อ (๑๐๕) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของโรงพยาบาล ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต

ข้อ (๑๐๖) ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเตอร์เน็ต การอัพเดทโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ (๑๐๗) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของโรงพยาบาลกุยบุรี

ข้อ (๑๐๘) ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาลกุยบุรี หรือการทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ (๑๐๙) ผู้ใช้งานไม่นำเข้าคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

ข้อ (๑๑๐) หลังจากใช้งานระบบอินเตอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ (๑๑๑) หลังจากใช้งานระบบอินเตอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ (๑๑๒) ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ส่วนที่ ๑๑ การใช้งานคอมพิวเตอร์ส่วนบุคคล

ข้อ (๑๑๓) แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่โรงพยาบาลกุยบุรี อนุญาตให้ใช้งาน เป็นสินทรัพย์ของโรงพยาบาลกุยบุรี เพื่อใช้ในงานของโรงพยาบาลกุยบุรี

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของโรงพยาบาลกุยบุรี ต้องเป็นโปรแกรมที่โรงพยาบาลกุยบุรี ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของโรงพยาบาลกุยบุรี

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของโรงพยาบาลกุยบุรี หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับโรงพยาบาลกุยบุรี เท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือ เมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

(๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของโรงพยาบาลกุยบุรี ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของโรงพยาบาลกุยบุรี ก่อนการใช้งาน

ข้อ (๑๑๔) การใช้รหัสผ่าน ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ (๑๑๕) การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ (๑๑๖) การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของโรงพยาบาลกุยบุรี

ส่วนที่ ๑๒ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ (๑๑๗) แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่โรงพยาบาลกุยบุรี อนุญาตให้ใช้งานเป็นสินทรัพย์ของโรงพยาบาลกุยบุรี เพื่อใช้ในงานของโรงพยาบาลกุยบุรี

(๒) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๓) ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๔) ในกรณีที่ต้องการเคลื่อนย้ายคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

(๕) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๖) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๗) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

(๘) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๙) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ (๑๑๘) ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ (๑๑๙) การควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์พกพา

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ ความรับผิดชอบของผู้ใช้งาน”

(๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ โดยตั้งเวลาประมาณ ๓๐ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ (๑๒๐) การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ (๑๒๑) การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ด้วยวิธีการและสื่อบันทึกต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสารองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสารองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสารองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของโรงพยาบาลกุยบุรี

ส่วนที่ ๑๓ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS)

ข้อ (๑๒๒) IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในโรงพยาบาลกุยบุรี ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ (๑๒๓) IDS/IPS Policy ต้องครอบคลุมทุกโฮสต์ ในเครือข่ายของโรงพยาบาลกุยบุรี และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเตอร์เน็ตทุกเส้นทาง

ข้อ (๑๒๔) ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเตอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบระบบจาก IDS/IPS

ข้อ (๑๒๕) ระบบทั้งหมดใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ (๑๒๖) โฮสต์ และเครือข่ายทั้งหมดที่มีการส่งผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ (๑๒๗) ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

ข้อ (๑๒๘) ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ (๑๒๙) IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ ข้อ (๑๖๒) เครื่องแม่ข่ายที่มีการติดตั้ง Host-Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ (๑๓๐) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศทราบทันทีที่ตรวจพบ

ข้อ (๑๓๑) พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศทราบ

ข้อ (๑๓๒) การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ (๑๓๓) ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ลบซอฟต์แวร์ที่มุ่งร้ายที่ตรวจพบ

ข้อ (๑๓๔) ศูนย์คอมพิวเตอร์ มีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ (๑๓๕) ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของโรงพยาบาลกุยบุรี การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้งานเครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของโรงพยาบาลกุยบุรี จะต้องถูกดาเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๔ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ (๑๓๖) การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ และชื่อผู้ใช้งาน

(๔) กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address

(๕) ปรับปรุง / กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ

(๖) ติดตั้งโปรแกรม Antivirus / ปรับปรง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

ข้อ (๑๓๗) การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

(๑) กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

(๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

ข้อ (๑๓๘) การปรับปรุงระบบการรักษาความปลอดภัย / Anti-Virus (System Security & Antivirus Update)

(๑) ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ

(๒) Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง / กำหนดค่าระบบความปลอดภัย

(๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์ เป็นประจำ

ข้อ (๑๓๙) ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบงานที่โรงพยาบาลกุยบุรีใช้

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามระบบฐานข้อมูลนั้นกำหนด

(๓) สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัย หรือป้องกันการเกิดปัญหาอยู่เสมอ

ข้อ (๑๗๓) ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่าง ๆ /กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการหรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบงานตามความต้องการหรือการพัฒนา

(๒) กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด

(๔) แจ้งผู้ใช้งาน หรือเจ้าของระบบงาน ให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อ รหัสผ่าน และสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้าง/ปรับปรุง

แนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

(๑) เพื่อให้ระบบสารสนเทศของโรงพยาบาลกุยบุรี สามารถให้บริการได้อย่างต่อเนื่อง

(๒) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

(๓) เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

(๑) จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๒) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๒.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๒.๒) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๒.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของโรงพยาบาลกุยบุรี จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

(๓) ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๓.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการวิจัย การพัฒนา และการให้บริการเทคโนโลยีที่เกี่ยวข้อง เช่น สถิติผู้ใช้บริการ สถิติผลงานวิจัย ข้อมูลงานวิจัย เป็นต้น

(๓.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- **ข้อมูลลับที่สุด** หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- **ข้อมูลลับมาก** หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- **ข้อมูลลับ** หมายความว่า หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- **ข้อมูลทั่วไป** หมายความว่า ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๓.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(๓.๕) การกำหนดเวลาที่ได้เข้าถึง

(๓.๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒ ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๔ ผู้ดูแลระบบของศูนย์คอมพิวเตอร์เป็นผู้มีสิทธิ์และอำนาจในการพิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างหน่วยงาน หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากหน่วยงานภายนอกให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างโรงพยาบาลกุยบุรี กับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

(๓) กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

(๔) กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

(๕) กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

(๖) กำหนดสิทธิ์การเข้าถึงข้อมูล

(๗) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖ พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลาดับความจำเป็นมากไปน้อย

ข้อ ๗ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๘ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของโรงพยาบาลกุยบุรี พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

(๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

(๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

(๔) ตรวจสอบค่าคอนฟิกกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรอง ต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับโรงพยาบาล

(๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๑๐) ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

(๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๐ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๑ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

ข้อ ๑๓ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

ข้อ ๑๔ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของโรงพยาบาลกุยบุรี อย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

(๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

(๒) เพื่อการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

(๓) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของโรงพยาบาล (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้โรงพยาบาลกุยบุรี ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

ข้อ ๑ จัดลำดับความสำคัญของความเสี่ยง

ข้อ ๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

ข้อ ๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

ข้อ ๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

ข้อ ๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลแสดงการเข้าถึง นั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของโรงพยาบาลกุยบุรี (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของโรงพยาบาลกุยบุรี ขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑) จัดหลักสูตรอบรมหรือประชาสัมพันธ์สำหรับเจ้าหน้าที่ของโรงพยาบาลกุยบุรี ให้มีความรู้ความเข้าใจด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนภายในโรงพยาบาลกุยบุรี เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเตอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Anti-Virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า ถือเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) Backup ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ โดยปิดเบรกเกอร์ที่เกี่ยวข้อง เพื่อป้องกันอุปกรณ์เสียหาย และป้องกันภัยจากไฟฟ้า

(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องปฏิบัติการเครือข่ายคอมพิวเตอร์สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถใช้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

แนวปฏิบัติในการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลกุยบุรี

แนวปฏิบัติ

ข้อ ๑ อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายความว่า ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า - ออก ของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้าออก อาคารสถานที่

(๑) กำหนดสิทธิ์ผู้ใช้งาน มีสิทธิ์ผ่านเข้า - ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของศูนย์คอมพิวเตอร์โรงพยาบาลกุยบุรี ของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่ จะต้องได้รับอนุญาตจากผู้รับผิดชอบ

(๓) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๔) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๕) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๖) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๗) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๘) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า - ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๙) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลกุยบุรี ที่เพียงพอต่อความต้องการใช้งานโดยมีระบบ ดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้น อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของโรงพยาบาลกุยบุรี ในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในโรงพยาบาลกุยบุรี

(๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘ การนำทรัพย์สินของโรงพยาบาลกุยบุรี ออกนอกโรงพยาบาลกุยบุรี (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกโรงพยาบาลกุยบุรี

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกจากโรงพยาบาลกุยบุรี

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกโรงพยาบาลกุยบุรี

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของโรงพยาบาลกุยบุรีออกไปใช้งานนอกโรงพยาบาลกุยบุรี เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกโรงพยาบาลกุยบุรี (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของโรงพยาบาลกุยบุรีออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของโรงพยาบาลกุยบุรีไว้ในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

แนวปฏิบัติในการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

ข้อ ๑ ระบบป้องกันผู้บุกรุก

(๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒ ระบบไฟร์วอลล์

(๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

(๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งผู้อำนวยการ เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓ ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต หรือมัลแวร์ ประกอบด้วย ไวรัส หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์

(๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในโรงพยาบาลกุยบุรี ไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของโรงพยาบาลกุยบุรี

(๓) หากตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์ หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

(๑) เพื่อสร้างความรู้ความเข้าใจ ในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของโรงพยาบาลกุยบุรี

(๒) เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

(๓) เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑ จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของโรงพยาบาลกุยบุรี

ข้อ ๓ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ ๗ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของโรงพยาบาลกุยบุรี

ข้อ ๘ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของโรงพยาบาลกุยบุรี และข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของ ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับ มอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

(๑) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ หรือ เทียบเท่าหัวหน้าส่วนงาน

(๑) รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓ ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้อำนวยการ เช่น นักวิชาการคอมพิวเตอร์ เจ้าพนักงานเครื่องคอมพิวเตอร์

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๓) รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

(๔) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๖) รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต

(๗) ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวปฏิบัติสำหรับการจัดซื้อจัดจ้างระบบสารสนเทศของโรงพยาบาลกุยบุรี

วัตถุประสงค์

เพื่อให้โรงพยาบาลกุยบุรี มีแนวทางสำหรับการควบคุมการพัฒนา การจัดหา และการติดตั้งระบบงานเพื่อเตรียมพร้อมการนำสู่การใช้งาน รวมทั้งบริหารจัดการกรณีมีการเปลี่ยนแปลงระบบงานและ ทบทวนการทำงานของระบบงานให้มีความพร้อมใช้งานอยู่เสมอ โดยแนวปฏิบัตินี้จะมีผลบังคับใช้กับผู้รับผิดชอบสารสนเทศและผู้ที่เกี่ยวข้องของโรงพยาบาลกุยบุรี

แนวปฏิบัติ

ข้อ ๑ ผู้รับผิดชอบสารสนเทศต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบที่ได้มีความมั่นคงปลอดภัยเพียงพอ ดังนี้

(๑) ระบุข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวควรครอบคลุมประเด็นสำคัญต่าง ๆ ตามแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

(๒) พัฒนาหรือจัดหาระบบงานให้สอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัยในข้อที่แล้ว

(๓) พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลหรือผู้พัฒนาระบบเพื่อทำการบันทึก เปลี่ยนแปลง แก้ไข หรือถอดถอนสิทธิของผู้ใช้งานได้

(๔) กำหนดให้มีการจัดทำแผนการทดสอบระบบ นำเสนอแผนดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้มีอำนาจดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการทดสอบให้ผู้มีอำนาจได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงหรือแก้ไขต่าง ๆ ตามความจำเป็น

(๕) ไม่อนุญาตการนำข้อมูลสำคัญของหน่วยงาน เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลใช้ภายในเท่านั้นไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ให้ตัดข้อมูลส่วนที่เป็นความลับ หรือข้อมูลส่วนบุคคลทิ้งไป

ข้อ ๒ ภายหลังจากที่ระบบงานพัฒนาเสร็จแล้วและพร้อมติดตั้ง ให้ดำเนินการควบคุมการติดตั้งระบบลงไปยังเครื่องแม่ข่ายให้บริการระบบงาน ดังนี้ (แนวปฏิบัติสำหรับการติดตั้งระบบ)

(๑) กำหนดแผนการติดตั้งสำหรับระบบ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้าในระยะเวลาที่นานเพียงพอ เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่น ๆ

(๒) กำหนดให้เฉพาะผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายที่มีความชำนาญเท่านั้น ที่จะเป็นผู้ดาเนินการติดตั้ง

(๓) ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูล ซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่น ๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จ จะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

(๔) ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลบนระบบงานที่จะทำการติดตั้งให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

(๕) กำหนดพื้นที่หรือบริเวณที่จะทำการติดตั้งระบบที่มีความมั่นคงปลอดภัยทางกายภาพเพียงพอ

(๖) คำนวณและตรวจสอบปริมาณความต้องการใช้กระแสไฟฟ้าและเครื่องสำรองไฟฟ้าให้เพียงพอกับความต้องการของระบบ

(๗) ปฏิบัติตามคู่มือหรือเอกสารที่เกี่ยวข้องกับการติดตั้งซอฟต์แวร์บนระบบ เช่น คู่มือการติดตั้งเว็บเซิร์ฟเวอร์ คู่มือการติดตั้งระบบบริหารจัดการฐานข้อมูล เป็นต้น ๑

(๘) ดำเนินการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ต่าง ๆ ในระบบ (เช่น ซอฟต์แวร์ระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล) ที่ขออนุมัติการติดตั้งเพื่อปรับปรุงหรือแก้ไขให้ระบบมีความสมบูรณ์และมั่นคงปลอดภัย

(๙) ตรวจสอบและปิดพอร์ตต่าง ๆ บนระบบที่ไม่มีความจำเป็นในการใช้งาน

(๑๐) กำหนดให้มีการตั้งสัญญาณนาฬิกาของระบบต่าง ๆ ของหน่วยงาน ให้ถูกต้องและตรงตามเวลามาตรฐานสำกลอยู่เสมอ

(๑๑) การใช้งานโปรแกรมยูทิลิตี้นั้น ผู้ใช้งานจะต้องขออนุมัติก่อนการติดตั้งและใช้งานโปรแกรมดังกล่าว รวมทั้งจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้นั้นและจะต้องติดตั้งโปรแกรมที่ไม่ละเมิดลิขสิทธิ์ของผู้ผลิตโปรแกรมนั้น

(๑๒) สำหรับซอฟต์แวร์ในระบบที่จะทำการติดตั้งประเภทฟรีแวร์หรือแชร์แวร์ตรวจสอบก่อนที่จะทำการติดตั้งว่าสามารถใช้งานได้ด้วยเงื่อนไขอะไรบ้าง และจะต้องไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

(๑๓) ตรวจสอบและติดตั้งระบบป้องกันไวรัสสำหรับระบบที่ทำการติดตั้ง

(๑๔) ตรวจสอบและลบบัญชีผู้ใช้งานในระบบที่ไม่ได้มีการใช้งาน ซึ่งรวมถึงบัญชีผู้ใช้งานต่าง ๆ ที่มีมากับซอฟต์แวร์ที่ได้รับเหล่านั้น

(๑๕) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความปลอดภัยและจำกัดการเข้าถึงโดยผู้ที่เกี่ยวข้องเท่านั้น

(๑๖) กำหนดวิธีเรียกเวอร์ชั่นของซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงาน เมื่อมีการเปลี่ยนแปลงซอร์สโค้ดหรือไลบรารี่ จะต้องเปลี่ยนแปลงเวอร์ชั่นให้ถูกต้องตามวิธีการที่กำหนดไว้

(๑๗) จำกัดการเชื่อมต่อทางเครือข่ายเพื่ออนุญาตให้เฉพาะกลุ่มผู้ใช้งานที่เกี่ยวข้องเท่านั้น จึงจะสามารถเชื่อมต่อและล็อกอินเข้าสู่ระบบที่ทำการติดตั้งนั้นได้

ข้อ ๓ ในการขอเปลี่ยนแปลงระบบงานภายหลังจากที่ได้มีการติดตั้งและใช้ระบบงานไปแล้ว กำหนดให้มีการขออนุมัติการเปลี่ยนแปลงระบบงาน ดังนี้ (แนวปฏิบัติสำหรับการเปลี่ยนแปลงระบบงานตามความต้องการของผู้ใช้งาน)

(๑) กำหนดให้มีการทำบันทึกข้อความเพื่อขออนุมัติเปลี่ยนแปลงระบบงาน เช่น ขอเพิ่มรายงานในระบบ เพิ่มฟังก์ชั่นการทำงาน เป็นต้น โดยผ่านผู้บังคับบัญชาในสายงานเพื่อพิจารณาอนุมัติ

(๒) พิจารณาปริมาณการเปลี่ยนแปลง ผลกระทบของการเปลี่ยนแปลง ความเร่งด่วน ความเหมาะสม และค่าใช้จ่ายในการดำเนินการ

(๓) อนุมัติตามที่ร้องขอหากเห็นสมควร

(๔) จัดประชุมกับผู้ร้องขอเพื่อรวบรวมความต้องการด้านระบบงานโดยละเอียด และสรุปความต้องการทั้งหมด

(๕) เริ่มต้นพัฒนาระบบงานตามความต้องการที่ได้รับ

ข้อ ๔ กำหนดให้มีการทบทวนการทำงานของระบบงานในระหว่างหรือภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการของระบบงานดังนี้ (แนวปฏิบัติสำหรับการทบทวนการทำงานของระบบงานภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน)

(๑) ปฏิบัติตามแนวปฏิบัติสำหรับการเปลี่ยนแปลงระบบ เพื่อขออนุมัติเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน

(๒) กำหนดแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงานซึ่งรวมถึงแผนการทดสอบ

(๓) ประสานงานแจ้งให้ผู้ใช้งานและผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับแผนดำเนินการเปลี่ยนแปลงฯ เพื่อให้บุคคลเหล่านั้นเข้าร่วมการทดสอบระบบงานเพื่อดูว่าระบบและข้อมูลสามารถใช้งานได้อย่างถูกต้องและสมบูรณ์หรือไม่

(๔) เปลี่ยนแปลงระบบตามแผนดำเนินการเปลี่ยนแปลงฯ

(๕) ทดสอบระบบร่วมกับผู้ใช้งานตามแผนการทดสอบที่กำหนดไว้ จนกระทั่งมั่นใจว่าระบบงานสามารถทำงานได้อย่างถูกต้องและสมบูรณ์ตามที่ควรจะเป็น

(๖) ดำเนินการติดตั้งบนระบบจริงโดยปฏิบัติตามแนวปฏิบัติสำหรับการติดตั้งระบบที่ได้กำหนดไว้

แนวปฏิบัติความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล

วัตถุประสงค์

๑) เพื่อคัดสรรพนักงานที่ตรงกับความต้องการ และเพื่อให้พนักงานเข้าใจในหน้าที่และความรับผิดชอบ

๒) เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

๓) เพื่อให้ยกเลิกหรือเปลี่ยนแปลงสิทธิกับเจ้าหน้าที่ หรือเจ้าหน้าที่จากหน่วยงานภายนอกที่ถูกยกเลิกหรือเปลี่ยนแปลงการจ้างงาน เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ ข้อกำหนดการตรวจสอบและอ้างอิงบริษัท

๑) ทุนจดทะเบียนต้องไม่น้อยกว่าร้อยละ ๒๐ ของวงเงินจ้าง ให้เป็นไปตามระเบียบสำนักนายกฯ ว่าด้วยพัสดุ

๒) ประวัติ/รายละเอียด/ประเภท ต้องเป็นบริษัทที่ดำเนินกิจการตรงกับประเภทของงานซื้อ/จ้าง

๓) ไม่อยู่ในระหว่างการพิจารณาคดีให้เป็นผู้ทิ้งงาน หรือเป็นผู้ทิ้งงาน หรือเป็นผู้กระทำผิดทาง ละเมิด

๔) ส่งหลักฐาน การทดสอบตนของบริษัท ที่ถูกต้องตามกฎหมาย เกี่ยวกับเอกสารที่คัดสำเนาจากส่วนราชการ ไม่ปลอมแปลงเอกสาร

๕) ประวัติการทำงาน หรือ ผลงานทางบริษัท ในสายงานที่ตรงกับการว่าจ้างตามที่กำหนด

๖) ให้แสดงผลงานที่เคยเป็นที่ประจักษ์ของบริษัท หรือหากไม่มีให้แสดงผลงานของบุคคลกรที่เป็นผู้รับผิดชอบของงานจ้าง โดยบุคลากรนั้นต้องทำงานจนเสร็จสิ้นงานจ้าง

๗) หลักประกันความเสียหายตามระเบียบสำนักนายกฯ ว่าด้วยพัสดุ

๘) ต้องไม่เป็นบริษัทขายช่วง หรือซื้อช่วง การจ้าง/ซื้อ

ข้อ ๒ ข้อกำหนดการตรวจสอบของบุคลากรหรือทีมงานที่จะเข้ามาปฏิบัติงานในโรงพยาบาลกุยบุรี

๑) ระดับวุฒิการศึกษาอย่างน้อย ปริญญาตรี ในสำขาที่ตรงกับงานที่จ้างและประวัติการศึกษา

๒) ใบรับรองหรือประกาศนียบัตร ของทีมงาน/บุคคล

๓) ประวัติการทำงาน และประสบการณ์การทำงาน

๔) ข้อมูลหลักฐานแสดงตัวตนของทีมงาน/บุคคล เช่นบัตรประชาชนหรือเอกสารระบุตัวบุคคล

๕) ต้องมีผลงานเป็นที่ประจักษ์ ตรงกับประเภทงานจ้าง

ข้อ ๓ การจ้างงานด้านการพัฒนาระบบสารสนเทศ

๑) มีแผนงานในการดำเนินงานและนำเสนอต่อคณะกรรมการ

๒) มีการแต่งตั้งคณะกรรมการเปิดซอง/ตรวจรับ/คณะกรรมการTOR

๓) มีรายงานผลการศึกษาระบบเดิมและความต้องการผู้ใช้งาน

๔) มีการนำเสนอผลการวิเคราะห์ระบบและการออกแบบ

๕) ในการพัฒนาระบบ ต้องจัดทำให้สามารถเชื่อมโยงข้อมูลได้อย่างสมบูรณ์

๖) ระหว่างการพัฒนาระบบ ต้องมานำเสนอความก้าวหน้าเป็นระยะตามที่กรมกำหนด

๗) เมื่อพัฒนาระบบเสร็จสิ้น ต้องมีระบบการทดสอบหรือทดลองใช้งานจากผู้ใช้

๘) เมื่อขั้นตอนทดสอบระบบเสร็จสิ้นก่อนจะติดตั้งระบบขึ้นใช้งานจริงต้องมีการวิเคราะห์การ ทำงานของระบบ

๙) หลังการติดตั้งระบบที่พัฒนาขึ้นใช้งานจริง ต้องมีการรายงานประเมินผลการใช้งาน

๑๐) กรณีสิ้นสุดการจ้างต้องเปลี่ยนสิทธิการเข้าถึงระบบหรือคืนทรัพย์สินตามที่กรมกำหนด

ข้อ ๔ การจ้างงานด้านระบบเครือข่ายและอุปกรณ์

๑) มีการแต่งตั้งคณะกรรมการเปิดซอง/ตรวจรับ/คณะกรรมการTOR

๒) มีรายงานการศึกษาวิเคราะห์และออกแบบพร้อมนำเสนอแผนงานไดอะแกรมการออกแบบ ระบบเครือข่ายต่อคณะกรรมการตรวจรับ

๓) นำเสนอผลการวิเคราะห์และแผนสำรอง กรณีที่อาจมีผลกระทบกับระบบเครือข่ายปัจจุบันที่ดำเนินงานต่อเนื่องเพื่อไม่ให้การดำเนินงานของกรมหยุดชะงัก

๔) หากระหว่างการดำเนินการติดตั้งหรือปรับปรุงระบบส่งผลกระทบความเสียหายต่อ โรงพยาบาล บริษัทหรือผู้รับจ้างต้องรับผิดชอบเป็นเงินประกันตามความเสียหายทั้งหมด หรือตาม ข้อตกลงทางคณะกรรมการตรวจรับ

๕) ข้อมูลหรือทรัพย์สินด้านการพัฒนาหรือปรับปรุงระบบเครือข่าย ที่ถูกกำหนดเป็นความลับ ห้ามนำออกนอกโรงพยาบาลกุยบุรีหรือห้ามสำรองข้อมูลเอกสารอื่นใด

ข้อ ๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยแก่บุคลากรของโรงพยาบาลกุยบุรี

๑) ประกาศแจ้งนโยบายความมั่นคงปลอดภัย

๒) รวบรวมปัญหาเกี่ยวกับการใช้เครื่องมืออุปกรณ์และระบบที่เป็นช่องโหว่ส่งผลกระทบต่อระบบ ความมั่นคงปลอดภัยของโรงพยาบาลกุยบุรี

๓) ประชาสัมพันธ์ให้เกิดความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยต่อโรงพยาบาลกุยบุรี

๔) จัดอบรมให้ความรู้การใช้งานระบบเทคโนโลยีสารสนเทศที่ถูกต้องและให้เกิดความตระหนัก ต่อระบบความมั่นคงปลอดภัย

๕) จัดทำมาตรการและบทลงโทษกรณีผู้ทำผิดนโยบายความมั่นคงปลอดภัยของโรงพยาบาลกุยบุรี โดยควรได้รับการรับรองสนับสนุนจากผู้บริหารโรงพยาบาลกุยบุรี

๖) ประเมินผลการถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยที่ประกาศใช้

ข้อ ๖ การกำหนดสำหรับบุคลากรทั่วไปภายในโรงพยาบาลกุยบุรี

๑) ห้ามนำโปรแกรม (Software) ที่ไม่เกี่ยวข้องกับการใช้งานตามมาตรฐานที่กรมกำหนดมาใช้ในโรงพยาบาลกุยบุรี

๒) หากมีความประสงค์หรือความจำเป็นต้องใช้งานโปรแกรม (Software) ที่ไม่อยู่ในรายการ มาตรฐานที่โรงพยาบาลกุยบุรีกำหนด ให้ขออนุญาตเป็นลายลักษณ์อักษรและขอขึ้นทะเบียนจากผู้มีหน้าที่ รับผิดชอบรับทราบก่อนทุกครั้ง ป้องกันการละเมิดลิขสิทธิ์และความเสียหายของโรงพยาบาลกุยบุรีอันเกิดจาก การละเมิดลิขสิทธิ์การใช้ซอร์ฟแวร์อย่างไม่ถูกต้อง

๓) จัดทำคู่มือการใช้งานและการบำรุงรักษาเบื้องต้นให้กับบุคลากรทั่วไปทราบในการปฏิบัติงานที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์

๔) การนำอุปกรณ์สำรองข้อมูลทุกประเภท เข้ามาใช้กับเครื่องคอมพิวเตอร์หรืออุปกรณ์ของโรงพยาบาลกุยบุรี ต้องมีการตรวจสอบความปลอดภัยของตัวอุปกรณ์ก่อนใช้งานทุกครั้ง

๕) เครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้ในโรงพยาบาลกุยบุรีควรมีการเข้ารหัส ทั้งในส่วนระบบที่เป็น Workgroup และ Active Directory การเชื่อมต่อระบบของโรงพยาบาลกุยบุรี

๖) หากเครื่องคอมพิวเตอร์มีปัญหาที่ไม่สามารถแก้ไขได้เองต้องแจ้งแผนกที่เกี่ยวข้องกับการ บำรุงรักษาและปรับปรุงระบบคอมพิวเตอร์เท่านั้น

๗) บุคลากรต้องรับผิดชอบดูแลเครื่องคอมพิวเตอร์ที่ใช้งานของตนเองหากเกิดความเสียหายหรือสูญหายต้องรับผิดชอบตามมติ

๘) บุคลากรผู้ใช้งานไม่ควรเข้าเว็บไซต์ที่ก่อให้เกิดอันตรายหรือไม่เกี่ยวข้องกับการปฏิบัติงานหรือดาวน์โหลดข้อมูลอันก่อให้เกิดความเสียหายต่อระบบ

ข้อ ๗ ผู้ดูแลระบบการรักษาความมั่นคงปลอดภัยหรือเครือข่าย

๑) โรงพยาบาลกุยบุรีต้องกำหนดโครงสร้างบทบาทหน้าที่ความรับผิดชอบของบุคลากร ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัย

๒) ต้องมีการกำหนดยุทธศาสตร์ด้านการดำเนินงานและปฏิบัติงานระบบคอมพิวเตอร์ ให้สอดคล้องกับความมั่นคงปลอดภัยของโรงพยาบาลกุยบุรี

๓) ต้องมีการวางแผนการดำเนินงานด้านความมั่นคงปลอดภัยอย่างเป็นระบบโดยการตรวจสอบ และควบคุมจากคณะกรรมการรักษาความมั่นคงปลอดภัย

๔) ต้องมีระบบการมอบหมายงานตามขอบเขตอำนาจหน้าที่ที่เหมาะสมต่อผู้ปฏิบัติงานด้านความมั่นคงปลอดภัย

๕) ต้องมีระบบการประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยและมีระบบแก้ไขปัญหาด้านความมั่นคงปลอดภัย