แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลหนองม่วง

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้สำนักงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลหนองม่วง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยด้านสารสนเทศและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ทั้งภายในและภายนอกอาศัยอำนาจตามข้อบังคับคณะกรรมการบริหารงานโรงพยาบาลหนองม่วง เห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ(Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ ไว้ดังนี้

๒. วัตถุประสงค์

๒.๑ จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ที่มีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบยอมรับ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔ เพื่อดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายขององค์กร

๓.๒ มุ่งกำหนดแนวทางปฏิบัติแนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔ เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของสำนักงานเองและ

ของสำนักงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการเรียนรู้อย่างต่อเนื่อง

๓.๕ ติดตาม ตรวจสอบการดำเนินงานและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. องค์ประกอบของนโยบาย

๔.๑ คำนิยาม

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

๔.๓ แนวปฏิบัติในการควบคุมการเข้าถึงของสารสนเทศของหน่วยงาน ครอบคลุมทุกระดับ

๔.๔ แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๔.๕ แนวปฏิบัติในการสำรองข้อมูลและกู้คืนระบบ

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

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและสำนักงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม ประกอบด้วย

๑. สำนักงาน หมายถึง โรงพยาบาลหนองม่วง

๒. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน

๓. ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) หมายถึง ผู้บังคับบัญชาสูงสุดของสำนักงาน (ผู้อำนวยการโรงพยาบาลหนองม่วง) ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย กำหนดทิศทางรวมทั้งมอบหมายงานให้ผู้ปฏิบัติที่เกี่ยวข้อง กำหนดความ

รับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ใช้งานไม่ได้ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

๔. การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของสำนักงาน

๕. มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๖. ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๗. แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๘. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสำนักงาน โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role)ซึ่งสำนักงานกำหนดไว้ดังนี้

ก. ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของสำนักงาน เช่นผู้อำนวยการ รองผู้อำนวยการ ผู้อำนวยการกลุ่มแผนงาน เป็นต้น

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

ค. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่และลูกจ้าง พนักงานจ้างประจำกิจกรรมโครงการต่าง ๆ ของสำนักงาน

๙. สำนักงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่สำนักงานอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสำนักงาน

๑๐. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๑๑. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

๑๒. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๓. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร

๑๔. ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในสำนักงานเข้าด้วยกัน

๑๕. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึงระบบงานของสำนักงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศ ที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหารการพัฒนาและควบคุมการติดต่อสื่อสาร

๑๖. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่สำนักงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาเพื่อปฏิบัติงานในสำนักงาน
- พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
- พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

๑๗. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๑๘. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

๑๙. สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๐. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๒๑. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ(confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๒๒. เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒๓. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๒๔. จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษราพถ่ายภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๒๕. รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๖. ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

กระบวนการตรวจสอบภายใน

๑. วัตถุประสงค์

เพื่อจัดตั้งคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทำการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง ร่วมกำหนดนโยบาย มาตรฐานหรือบรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง ตลอดจนการกำหนดขั้นตอนการรายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์เพื่อการควบคุมและตรวจสอบภายในสำนักงาน

๒. แนวทางปฏิบัติกระบวนการตรวจสอบภายใน

๒.๑ จัดตั้งคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีหน้าที่กำหนดแนวนโยบายและแนวปฏิบัติด้านการรักษาความปลอดภัยด้านสารสนเทศของสำนักงาน และทบทวนปรับปรุงการรักษาความปลอดภัยของสารสนเทศของสำนักงาน

๒.๒ กำหนดแผนการตรวจสอบและประเมิน โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศของหน่วยงานอย่างน้อย จำนวน ๑ ครั้งต่อปีทั้งนี้ขึ้นอยู่กับการจัดทำงบประมาณประจำปี

แนวทางปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของหน่วยงาน

๑. การควบคุมการเข้า-ออกห้องปฏิบัติการระบบเครือข่าย

เจ้าหน้าที่ผู้ดูแลห้องปฏิบัติการการระบบเครือข่าย มีแนวทางการปฏิบัติ ดังนี้

๑. เป็นผู้ถือกุญแจห้องปฏิบัติการระบบเครือข่ายเพียงผู้เดียวและเก็บกุญแจสำรองไว้ที่ห้องเวชระเบียนมีที่เก็บมิดชิด ใช้ได้เฉพาะในกรณีฉุกเฉินหรือได้รับอนุญาต

๒. เจ้าหน้าที่ผู้ดูแลห้องปฏิบัติการการระบบเครือข่าย ต้องเป็นผู้เปิดและปิด ประตูห้องปฏิบัติการการระบบเครือข่าย เมื่อมีเจ้าหน้าที่ในโรงพยาบาลหรือเจ้าหน้าที่จากหน่วยงานภายนอก เข้ามาปฏิบัติงานภายในห้องห้องปฏิบัติการการระบบเครือข่าย

๓. ห้ามนำอุปกรณ์ เทคโนโลยีสารสนเทศจากภายนอกเข้าห้องปฏิบัติการการระบบเครือข่ายก่อนได้รับอนุญาตจากเจ้าหน้าที่ผู้ดูแล

๔. จดบันทึกการเข้า-ออกห้องปฏิบัติการการระบบเครือข่ายและเหตุผลการเข้าไปในห้องปฏิบัติการการระบบเครือข่าย

๒. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. วิธีการบริหารจัดการการเข้าถึงของผู้ใช้งาน มีแนวทางการปฏิบัติ ดังนี้

ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสำนักงานกำหนดให้มีขั้น ตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น ต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงานต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น

ขั้นตอนการลงทะเบียนเจ้าหน้าที่ใหม่ขององค์กร

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

๒) ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิ์จากเจ้าของระบบสำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิ์จากผู้บริหารอย่างชัดเจน

๓) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๔) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบและมี

ความสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร

๕) ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้ เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทพการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๖) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๗) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๘) การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๘.๑ เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการลงแบบ ฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เช่น คำขอใช้อินเตอร์เน็ต ระบบอีเมล์หรือระบบงานต่าง ๆ

๘.๒ ยื่นคำขอกับผู้อำนวยการศูนย์สารสนเทศ หรือเจ้าหน้าที่ศูนย์สารสนเทศผู้ที่ได้รับมอบหมาย

๙) การให้สิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๙.๑ ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิ์อนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๙.๒ ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

๙.๓ ผู้ดูแลระบบให้สิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม

๑๐) การแจ้งยกเลิกสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๑๐.๑ หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการศูนย์สารสนเทศ๑๐.๒ ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๒. วิธีการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน มีแนวทางการปฏิบัติดังนี้

๑. ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

๒. มีการกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน

๓. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๑) ต้องได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้น ๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

(๒) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

(๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(๔) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน

หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น.

๓. วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย มีวิธีการปฏิบัติ ดังนี้

๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๒. ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕”

๓. ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

๔. ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๕. กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

๖. ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

๗. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๘. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๔. วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ มีวิธีการปฏิบัติ ดังนี้

๑. การจัดแบ่งประเภทของข้อมูล ประกอบด้วย

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลคำรับรอง ข้อมูลงบประมาณการเงินและบัญชี และข้อมูลระบบบริหารราชการ (Back Office)
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลผู้รับบริการทางสังคม

๒. การจัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภทข้างต้น ดังนี้
- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๓. การจัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภทข้างต้น ดังนี้
- ลับที่สุด
- ลับมาก
- ลับ

๔. การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภทข้างต้น ดังนี้
- สามารถเข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ
- สามารถเข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น
- สามารถเข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
- สามารถเข้าถึงได้โดยทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

๕. การกำหนดเวลาการเข้าถึง ดังนี้
- การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)
- การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ – ๑๖.๓๐ น.)
- การเข้าถึงในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุด นขัตฤกษ์)
- การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

๖. การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ดังนี้
- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)
- โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)
- หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)
- ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบอินเตอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
- ระบบจดหมายอิเล็กทรอนิกส์(เข้าถึงได้ทุกช่วงเวลา)
- เว็บไซต์(เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนด)

๓. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๑. ผู้ติดต่อจากหน่วยงานภายนอกต้องติดบัตรผู้ติดต่อตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในโรงพยาบาลหนองม่วง
๒. ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงานในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ ตามที่ระบุไว้ในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ให้ถูกต้องชัดเจน
๓. ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อ กับผู้ดูแลระบบ ซึ่งผู้ดูแลระบบต้องตรวจสอบการคืนบัตรและตรวจสอบการลงบันทึกตามเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ทุกครั้ง
๔. ผู้ดูแลระบบ ควรตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ เป็นประจำทุกเดือน

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอกหรือ Outsource วิธีการปฏิบัติ ดังนี้

๑. ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
๒. ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล
๓. ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร
๔. ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว
๕. ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน
๖. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟวอลตามที่องค์กรต้องการ
๗. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๘. องค์กรไม่อนุญาตให้ ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์กร

๙. องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๐. องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๔. การควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (PC)

แนวทางปฏิบัติการใช้งานทั่วไป

๑. เครื่องคอมพิวเตอร์ที่โรงพยาบาลหนองม่วง อนุญาตให้ใช้งาน เป็นสินทรัพย์ของโรงพยาบาลหนองม่วง เพื่อใช้ในงานของโรงพยาบาลหนองม่วง

๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของโรงพยาบาลหนองม่วงต้องเป็นโปรแกรมที่โรงพยาบาลหนองม่วง ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓. ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้ง แก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของโรงพยาบาลหนองม่วง

๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของโรงพยาบาลหนองม่วง เท่านั้น

๕. ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๖. ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์

๗. ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๘. ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกิน ๓๐ นาทีเพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

๙. ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของโรงพยาบาลหนองม่วง ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของโรงพยาบาลหนองม่วง ก่อนการใช้งาน

การใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย”

การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑. ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Flash Drive Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับคอมพิวเตอร์

๒. ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๓. ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การสำรองข้อมูลและกู้คืน

๑. ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น Flash Drive CDเป็นต้น

๒. ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๓. ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่มีผลกระทบต่อการดำเนินการของโรงพยาบาลหนองม่วง

๕. การใช้เครื่องคอมพิวเตอร์แบบพกพา(Notebook)

แนวทางปฏิบัติการใช้งานทั่วไป

๑. เครื่องคอมพิวเตอร์แบบพกพาที่โรงพยาบาลหนองม่วง อนุญาตให้ใช้งาน เป็นสินทรัพย์ของโรงพยาบาลหนองม่วงเพื่อใช้ในงานของโรงพยาบาลหนองม่วง
๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของโรงพยาบาลหนองม่วงต้องเป็นโปรแกรมที่โรงพยาบาลหนองม่วง ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
๓. ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
๔. ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
๕. ในกรณีการเคลื่อนย้ายคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน
๖. หลีกเลี่ยงการสัมผัสหน้าจอ คอมพิวเตอร์แบบพกพา เพื่อป้องกันรอยขีดข่วนหรือทำให้จอ เสียหาย
๗. ไม่ว่างของทับบนหน้าจอและแป้นพิมพ์
๘. ใช้ความระมัดระวังในการทำความสะอาดหน้าจอและตัวเครื่อง

ความปลอดภัยด้านกายภาพ

๑. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่นไม่ว่างเครื่องทิ้งไว้ในที่สาธารณะ
๒. ไม่เก็บคอมพิวเตอร์แล้วพกพาในที่มีสภาพอากาศร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังการตกกระทบ

การควบคุมการเข้าถึงระบบปฏิบัติการ

๑. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
๒. ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย”
๓. ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกิน ๓๐ นาทีเพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

การสำรองข้อมูลและกู้คืน

๔. ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น Flash Drive CDเป็นต้น
๕. ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖. ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่มีผลกระทบต่อการดำเนินการของโรงพยาบาลหนองม่วง

๖. การควบคุมการใช้งานอินเตอร์เน็ต (Internet)

ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของสำนักงาน มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๑. การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเตอร์เน็ตของสำนักงาน โดยยื่นคำขอกับเจ้าหน้าที่กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศโดยผู้ใช้งานต้องเป็นบุคลากรสังกัดสำนักงาน สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๒. ไม่ใช้ระบบอินเทอร์เน็ตของสำนักงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับสำนักงาน

๓. ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๔. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๕. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๖. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นต้องดาวน์โหลดไฟล์ขนาดใหญ่ให้ปฏิบัตินอกเวลาทำงาน

๗. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับบุคลากรของสำนักงานอื่น ๆ

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (WLAN)

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของสำนักงาน มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติดังนี้

๑. การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒. ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในสำนักงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๓. ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

๔. กรณีที่ผู้บังคับบัญชาอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๔.๑ ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวางAccess Point หน้า Firewall และหากมีความจำเป็นจริง ๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

๔.๒ ให้ผู้ใช้กรอกรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น ให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๔.๓ ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่น า Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๔.๔ ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configurationให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๔.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ(Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือสำนักงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของสำนักงาน

๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศทราบทันที

แนวปฏิบัติในการจัดทำระบบสำรองข้อมูลและกู้คืนระบบ

๑. การสำรองข้อมูลและระบบคอมพิวเตอร์

ผู้ดูแลระบบหรือบุคลากรที่เกี่ยวข้อง จะต้องระบุแนวปฏิบัติสาหรับการจัดทาระบบสำรองข้อมูลที่ชัดเจน เพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

๑. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบระบบสารสนเทศ และระบบสำรองข้อมูลของสำนักงาน

๒. ผู้ดูแลระบบ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสารองข้อมูลและสารสนเทศของสำนักงาน

๓. ทำการพิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ตามลำดับความสำคัญ

๔. ระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญต่อภารกิจของสำนักงาน

๕. มีการกำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

๖. จัดทำแผนการสำรองที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

๗. ดำเนินการตามกระบวนการสำรองข้อมูล สำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

๘. มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

๙. การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

๑๐. มีขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๑๑. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๑๒. ให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๑๓. ในกรณีที่พบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานต่อผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ

๑๔. ให้ผู้ดูแลระบบ กำหนดชนิดและช่วงเวลาการสารองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑๕. ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดยเคร่งครัด

๒. การปฏิบัติเกี่ยวกับการสำรองข้อมูล มีวิธีการปฏิบัติ ดังนี้

๑. ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการ โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ ดังนี้

(๑) Web servers : สำรองข้อมูลเผยแพร่บนเว็บไซต์ ๑ ครั้งต่อเดือน

(๒) Database servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ๑ ครั้งต่อเดือน

(๓) Firewall server : สำรองข้อมูล Rule ของ Firewall ๑ ครั้งต่อเดือน

(๔) Server อื่น ๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่น ๆ เช่น ระบบงานต่าง ๆ ๑ ครั้งต่อเดือน

๒. ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้อง สมบูรณ์หรือไม่

๓. การทดสอบและการกู้คืนระบบ

ต้องกำหนดแผนการทดสอบกู้คืนข้อมูล ตามชนิดของการสำรองข้อมูลที่กำหนดไว้แล้ว เพื่อให้ระบบสารสนเทศมีสภาพพร้อมใช้งานอยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

๑. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องกู้คืนระบบ ผู้ดูแลระบบจะต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึก และสรุปผลการปฏิบัติงานต่อผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้อานวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศทราบ

๒. การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

๓. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๔. กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

๑. บทบาทและความรับผิดชอบ

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใด ๆ ต่อ โรงพยาบาลหนองม่วง หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลหนองม่วง และป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น และการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยได้กำหนดบทบาทและความรับผิดชอบให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ดังนี้

๑. ผู้อำนวยการสำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ(องค์การมหาชน) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลหนองม่วง
๒. ผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลหนองม่วง โดยกำหนดมาตรการและกำกับดูแลการใช้งานและผลักดันให้เจ้าหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลหนองม่วง
๓. ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลหนองม่วง
๔. ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง ตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลหนองม่วง

๒. หน้าที่ความรับผิดชอบของผู้ดูแลระบบ

๑. จัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน
๒. บริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลักของโรงพยาบาลหนองม่วง เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย
๓. เก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น
๔. กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง ตามที่ได้รับมอบหมาย โดยกำหนดสิทธิให้ผู้ใช้งานสามารถใช้งานได้ตามภารกิจของผู้ใช้งาน และสามารถเข้าใช้ได้แต่เพียงงานที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๕. บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลหนองม่วง ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทาดังกล่าวในทันทีและในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อโรงพยาบาลหนองม่วงให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

๖. ติดตั้งและเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลหนองม่วง ที่ได้รับมอบหมาย และทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยเดือนละครั้ง

๗. บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานของโรงพยาบาลหนองม่วง สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง ให้มีความปลอดภัย

๘. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของ โรงพยาบาลหนองม่วง เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้องตามพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงไอซีทีเรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

๙. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๑๐. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๑. คืนทรัพย์สินของ โรงพยาบาลหนองม่วง ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้บริหารของ โรงพยาบาลหนองม่วง หรือผู้ที่ได้รับมอบหมาย เพื่อการตรวจสอบการคืนทรัพย์สิน

๓. หน้าที่ความรับผิดชอบของผู้ใช้งาน

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวทางปฏิบัติ ดังนี้

๑. การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลหนองม่วง ควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

(๑) เก็บรหัสผ่านไว้เป็นความลับ

(๒) หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

(๓) เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

(๔) กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอสำหรับ

(๔.๑) ง่ายสำหรับจดจำ

(๔.๒) ไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่ายหรือสามารถหาได้จากข้อมูลเกี่ยวกับตน เช่น ชื่อ หมายเลขโทรศัพท์และวันเกิด เป็นต้น

(๔.๓) ไม่สร้างจุดอ่อนโดยการใช้ค าที่อยู่ในพจนานุกรม

(๔.๔) ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่ควรเป็นตัวเลขทั้งหมด หรือไม่ควรเป็นตัวอักษรทั้งหมด

(๕) เปลี่ยนรหัสผ่านอย่างสม่ าเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิ์พิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

(๖) กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

(๗) ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

(๘) ไม่ใช้รหัสผ่านร่วมกับผู้อื่น

(๙) ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

(๑๐) ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว ควรแนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้นสำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

คุณสมบัติของรหัสผ่านที่ดี

(๑) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๒) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น“abcdef” “aaaaaa” “๑๒๓๔๕” “๑๒๓๔๕”

(๓) ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(๔) ไม่ควรกำหนดรหัสผ่านเป็นค าศัพท์ที่อยู่ในพจนานุกรม

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

(๗) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

(๑) ผู้ใช้งานควรออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลหนองม่วง โดยทันทีเมื่อเสร็จสิ้นงานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน๊ตบุ๊ค

(๒) ผู้ใช้งานควรล็อค (Lock) อุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(๓) ผู้ใช้งานควรป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของตน โดยต้องใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(๔) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงานร่วมกัน

(๕) ผู้ใช้งานและผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อค (Lock) หน้าจอ หลังจากที่ไม่ได้ใช้งาน มาช่วงระยะเวลาหนึ่ง เช่น ๑๐ นาที หลังจากที่มีการล็อค (Lock) หน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(๖) ปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือไม่มีการใช้งานนานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายที่ให้บริการซึ่งต้องใช้งานตลอด ๒๔ ชั่วโมง

(๗) ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้เจ้าหน้าที่เข้าใจในมาตรการป้องกันที่ได้กำหนดไว้นั้น

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์

การควบคุมทรัพย์สินสารสนเทศ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลและแฟ้มข้อมูล เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงระบบสารสนเทศและข้อมูลสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ มีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องป้องกันทรัพย์สินของ โรงพยาบาลหนองม่วง และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศ ที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่างๆ ประกอบด้วย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า
- ออกพื้นที่
- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

- วัฒนธรรมองค์กร

(๓) ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของ โรงพยาบาลหนองม่วง ก่อนเข้าใช้งาน โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสม

(๔) ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของ โรงพยาบาลหนองม่วง
- จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูล ไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ เช่น เก็บไว้ในตู้ที่ล็อคกุญแจได้ เป็นต้น
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือส่งข้อมูลสำคัญ เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอลเครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารสำคัญหรือลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกคอมพิวเตอร์ หรือสารสนเทศ ออกจาก โรงพยาบาลหนองม่วง ต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

(๕) ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

(๖) ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของ โรงพยาบาลหนองม่วง เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย

(๗) ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

(๘) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ

๔. การเข้าถึงและควบคุมการใช้งานระบบคอมพิวเตอร์หรือสารสนเทศ

ต้องจัดทำนโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงอย่างน้อยปีละ ๑ ครั้ง โดยการจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางการปฏิบัติงาน และทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ ซึ่งมีแนวทางปฏิบัติ ดังนี้

(๑) การควบคุมการเข้าถึงเครือข่าย (Network access control)

- ต้องจัดทำนโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้งานได้ บริการใดไม่สามารถใช้งานได้

- ต้องมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักงาน (User authentication for external connections) ก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงาน ได้
- ต้องมีการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) ให้สามารถระบุและพิสูจน์ตัวตน เพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว
- ต้องมีการแบ่งแยกเครือข่าย (Segregation in networks) ตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
- ต้องมีการควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) โดยต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายในการควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางการปฏิบัติงานได้ระบุไว้
- ต้องมีการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) เพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง

(๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

- ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน
- ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงานร่วมกัน
- ผู้ใช้บริการต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานภายใน ๑๐ นาทีหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน
- ผู้ใช้บริการต้องทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- ควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยง

(๓) การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and information access control)

- ต้องมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอพพลิเคชั่น(Information access restriction) โดยการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน
- ต้องมีการแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)ไว้ในบริเวณที่แยกต่างหากออกมา สำหรับระบบนี้โดยเฉพาะ

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการ รักษาความลับทางราชการ พ.ศ. ๒๕๔๔ มีแนวปฏิบัติ ดังนี้

- ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน
- กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล
- การจัดเก็บ username และ password ของระบบสารสนเทศลงในฐานข้อมูลใด ๆ จะต้องทำการเข้ารหัสด้วย MD๕ ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง
- ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ web application ที่มีชั้นหรือระดับความลับ/สำคัญมาก เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์
- กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมกับสำนักงานสำหรับช่องทางดังต่อไปนี้
    - ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต
    - เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย- สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)
- กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสาหรับการเข้ารหัสข้อมูลดังนี้
    - วิธีการป้องกันกุญแจที่ใช้สาหรับการเข้ารหัสข้อมูล
    - วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย
    - บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูลประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจเกิดการสูญหาย
- ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูลดังนี้
    ก) ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
    ข) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่สำนักงานกำหนด
    ค) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการกำหนดรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน
- ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของสำนักงานเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้
- ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่
- ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น