แนวปฏิบัติการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของโรงพยาบาลค่ายจิรประวัติ พ.ศ. ๒๕๖๖

ประกาศโรงพยาบาลค่ายจิรประวัติ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจของโรงพยาบาลค่ายจิรประวัติที่ให้บริการทางการแพทย์และสาธารณสุขแก่กำลังกำลังพลทหาร ครอบครัวและประชานชน จึงจำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองกำลังพลทหาร ครอบครัว และประชาชนหรือประโยชน์ที่สำคัญของกองทัพบกนั้น

เพื่อให้การบริหารจัดการระบบความมั่นคงปลอดภัยด้านสารสนเทศ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปรับเปลี่ยนหน่วยงานภาครัฐเป็นรัฐบาลดิจิทัลอย่างมีประสิทธิภาพ มีความมั่นคง ปลอดภัย มีความเชื่อถือได้และให้บริการได้อย่างต่อเนื่องสามารถป้องกันภัยคุกคามไซเบอร์ ซึ่งอาจก่อให้เกิดความเสียหายแก่โรงพยาบาลค่ายจิรประวัติ จึงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ หน่วยงาน ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า "ประกาศโรงพยาบาลค่ายจิรประวัติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๖๖

ข้อ ๒ ในประกาศ

(๑) "ทภ.๓" หมายความว่า กองทัพภาคที่ ๓

(๒) "มทบ.๓๑" หมายความว่า มณฑลทหารบกที่ ๓๑

(๓) "ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" (Chief Information Officer: CIO) หมายความว่า เสนาธิการทหารบก

(๔) "ผู้อำนวยการโรงพยาบาล" หมายความว่า ผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ

(๕) "ผู้บริหารระบบ" หมายความว่า ผู้บริหารระบบสารสนเทศของโรงพยาบาลค่ายจิรประวัติ หรือประธานกรรมการทีมสารสนเทศ โรงพยาบาลค่ายจิรประวัติ

(๖) "คณะกรรมการ" หมายความว่า คณะกรรมการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลค่ายจิรประวัติ

(๗) "นโยบาย"...

(๗) "นโยบาย" หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติที่เกี่ยวข้อง ดังนี้

(๗.๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๗.๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๗.๓) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๗.๔) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

(๗.๕) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๘) "แนวปฏิบัติ" หมายความว่า ขั้นตอน วิธีการหรือข้อกำหนดให้ผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) รวมทั้งบุคคลภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โรงพยาบาลค่ายจิรประวัติ ได้ถือปฏิบัติตาม นโยบาย ข้อ ๒ (๗)

(๙) "ผู้บริหารหน่วยงาน" (System Owner) หมายความว่า โรงพยาบาลที่เป็นเจ้าของระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ

(๑๐) "ผู้ดูแลระบบ" (System Administrator) หมายความว่า บุคลากรศูนย์คอมพิวเตอร์และสารสนเทศ โรงพยาบาลค่ายจิรประวัติ ผู้ซึ่งได้รับมอบหมาย จากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ ให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ์ และการบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

(๑๑) "ผู้ใช้งาน " (User) หมายความว่า บุคลากร โรงพยาบาลค่ายจิรประวัติ ทุกระดับ ซึ่งเป็นข้าราชการ ลูกจ้างประจำ พนักงานราชการ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอก ที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศ โรงพยาบาลค่ายจิรประวัติ

(๑๒) "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลค่ายจิรประวัติ

(๑๓) "สินทรัพย์ " (asset) หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของ โรงพยาบาลค่ายจิรประวัติ ประกอบด้วย

(๑๓.๑) ฮาร์ดแวร์ (Hardware) หมายความว่า อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server)
- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) และคอมพิวเตอร์พกพา (Laptop)
- เครื่องพิมพ์ (Pinter/Scanner) และอุปกรณ์สำรองข้อมูลของ โรงพยาบาลค่ายจิรประวัติ
- อุปกรณ์โครงข่าย (Network) หรือ อุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

(๑๓.๒) ซอฟต์แวร์...

(๑๓.๒) ซอฟต์แวร์ (Software) หมายความว่า ชุดคำสั่งหรือโปรแกรม (Program) ที่เขียนขึ้นเพื่อให้คอมพิวเตอร์ทำงาน แบ่งออกเป็น ๒ ประเภท

(๑๓.๒.๑) ซอฟต์แวร์ระบบ (Infrastructure software) หมายถึงโปรแกรมที่ทำหน้าที่ประสานการทำงาน ติดต่อการทำงาน ระหว่างฮาร์ดแวร์กับซอฟต์แวร์ประยุกต์เพื่อให้ผู้ใช้สามารถใช้ซอฟต์แวร์ได้อย่างมีประสิทธิภาพและทำหน้าที่ในการจัดการระบบ ดูแลรักษาเครื่อง

(๑๓.๒.๒) ซอฟต์แวร์ประยุกต์ (Application software) โปรแกรมที่ใช้สำหรับทำงานต่างๆ ตามที่ต้องการ เช่น การทำงานเอกสาร งานกราฟิก งานนำเสนอหรือเป็น ซอฟต์แวร์สำหรับงานเฉพาะด้าน เช่น โปรแกรมงานทะเบียน โปรแกรมการให้บริการเว็บ

(๑๔) "ศูนย์ข้อมูลและสารสนเทศ" หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะ เพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Devices) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูลระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศและระบบป้องกันอัคคีภัย ซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์ ระบบข้อมูลและระบบสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย

(๑๔.๑) "ศูนย์ข้อมูล" หมายความว่า สถานที่ทางกายภาพที่เก็บเครื่องคอมพิวเตอร์และอุปกรณ์ฮาร์ดแวร์ อุปกรณ์โครงข่าย (Network) ที่เกี่ยวข้องกับการรักษาพยาบาลของโรงพยาบาลค่ายจิรประวัติ โดยที่มีโครงสร้างพื้นฐานคอมพิวเตอร์ที่ระบบสารสนเทศต้องการ

(๑๔.๒) "สถานพยาบาล" หมายความว่า หน่วยที่ให้การรักษาและให้การสนับสนุนการบริการทางการแพทย์ของโรงพยาบาลค่ายจิรประวัติ

(๑๕) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือ การมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

(๑๖) "ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้ง คุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (nonrepudiation) และความน่าเชื่อถือ (Reliability)

(๑๗) "เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๘) "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ โรงพยาบาล...

ข้อ ๓ โรงพยาบาลค่ายจิรประวัติ ได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

(๑) นโยบายได้มาเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบ

(๒) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติฯ ดังกล่าวให้ชัดเจน

(๓) ต้องทบทวนและปรับปรุงนโยบาย อย่างน้อย ปีละ ๑ ครั้ง

ข้อ ๕ โรงพยาบาลค่ายจิรประวัติ ได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศพร้อมทั้งได้ กำหนดให้ผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ เป็นผู้กำกับ ดูแล และติดตามผู้ใช้งาน (User) ให้ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจน ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้ระบบสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๓) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

(๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

(๗) การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

(๘) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management)

(๙) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management) โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๖ โรงพยาบาลค่ายจิรประวัติ ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้วยวิธีการ ใดวิธีการหนึ่งให้ผู้ใช้งาน (User) และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าใจ เข้าถึงและปฏิบัติตามด้วยหนังสือเวียนภายในองค์กร ระบบหนังสือเวียนอิเล็กทรอนิกส์ หรือเว็บไซต์โรงพยาบาลค่ายจิรประวัติ และติดประกาศนโยบายให้ทราบ

ข้อ ๗ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของโรงพยาบาลค่ายจิรประวัติ เกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือผ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติ ประธานกรรมการทีมสารสนเทศโรงพยาบาลค่ายจิรประวัติ ต้องรายงานต่อผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ สั่งการตรวจสอบผู้ละเลยที่ก่อให้เกิดความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลค่ายจิรประวัติ เพื่อรายงานต่อผู้บริหารระดับสูงสุด

ข้อ ๘ โรงพยาบาล...

ข้อ ๘ โรงพยาบาลค่ายจิรประวัติกำหนดให้ผู้อำนวยการเป็นผู้รับผิดชอบในการบริหารความเสี่ยง ควบคุมความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลค่ายจิรประวัติ

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๒๖ พฤษภาคม พ.ศ. ๒๕๖๖

พันเอก

(ปุญชทร ทิพยวงษ์)

ผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ

สารบัญ

หน้า

หมวดที่ ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

วัตถุประสงค์

เพื่อให้บุคลากรโรงพยาบาลค่ายจิรประวัติ และบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) พร้อมทั้งตระหนักถึง ความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากรโรงพยาบาลค่ายจิรประวัติ และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุน การรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตาม ภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ ผู้บริหารระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน

๑.๓ ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานตามที่ผู้บริหารระบบอนุมัติ

๑.๔ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๕ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากผู้บริหารระบบ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๑.๗ การเข้าถึงห้องศูนย์ข้อมูล (Data Center) ให้ดำเนินการ ดังนี้

๑.๗.๑ โรงพยาบาลค่ายจิรประวัติ ต้องกำหนดข้อปฏิบัติสำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ

๑.๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๑.๗.๔ ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๕ ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจาก ผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

๒.๑ สิทธิของผู้ใช้งาน (User) ระดับเจ้าหน้าที่ที่ได้รับมอบหมาย

๒.๑.๑ ระดับผู้บริหาร สิทธิการใช้งาน

- อนุมัติสิทธิการใช้งาน
- อ่านอย่างเดียว เช่น การเรียกดูผลการปฏิบัติงาน การออกรายงานสรุปผลรายงานต่างๆ

๒.๑.๒ ระดับผู้ดูแลระบบ สิทธิการใช้งาน

- สร้างข้อมูล เช่น กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ
- แก้ไขข้อมูล เช่น การบริหารจัดการข้อมูลภายในระบบสารสนเทศ
- ลบข้อมูล เช่น การลบสิทธิผู้เข้าใช้งาน ให้เป็นปัจจุบัน

๒.๑.๓ ระดับเจ้าหน้าที่ที่ได้รับมอบหมาย สิทธิการใช้งาน

- สร้างข้อมูล เช่น กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ
- แก้ไขข้อมูล เช่น การบริหารจัดการข้อมูลภายในระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศสำหรับการบริหารภายในหน่วยงาน เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลสุขภาพบุคลากร ข้อมูลงบประมาณรายรับสถานพยาบาล และข้อมูลการรักษาพยาบาล เป็นต้น

๓.๑.๒ ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไปและผู้ที่สนใจ เช่น ข้อมูลในเว็บไซต์ของโรงพยาบาลค่ายจิรประวัติ เป็นต้น

๓.๒ ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑ สำคัญมากที่สุด

๓.๒.๒ สำคัญมาก

๓.๒.๓ ปกติ

๓.๓ ลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ ดังนี้

๓.๓.๑ ลับที่สุด - ความลับที่มีความสำคัญที่สุด เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือ เป็นภยันตรายต่อความมั่นคงความปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติหรือพันธมิตร หรือการ ดำเนินงานของหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒ ลับมาก - ความลับที่มีความสำคัญมาก เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือ เป็นภยันตรายต่อความมั่นคงความปลอดภัยของประเทศชาติหรือพันธมิตร หรือความสงบเรียบร้อยภายในราชอาณาจักร หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้อย่างร้ายแรง

๓.๓.๓ ลับ - ความลับที่มีความสำคัญเกี่ยวกับ ข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อราชการ หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้

๓.๓.๔ ปกปิด - ความลับซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจองค์กรเท่านั้น

๓.๔ ช่องทางการเข้าถึงสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ ๒ ช่องทาง ดังนี้

๓.๔.๑ ระบบเครือข่ายภายใน (Intranet) คือ ระบบเครือข่ายภายในองค์กรเป็นบริการ การเชื่อมต่อคอมพิวเตอร์ภายในหน่วยงาน เช่น การแชร์ไฟล์ การแชร์ปริ้นเตอร์ ระบบบริการทางการแพทย์ เป็นต้น

๓.๔.๒ ระบบเครือข่ายภายนอก (Internet) คือ ระบบเครือข่ายที่สามารถเข้าได้จากภายนอกองค์กรสามารถเข้าใช้ได้ทุกพื้นที่ เช่น ระบบหรือเว็บไซต์ของหน่วยงานที่ให้บริการต่างๆ เป็นต้น

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Business Requirements For Access Control) ดังนี้

๔.๑ ผู้บริหารระบบอนุมัติสิทธิให้ผู้ใช้งาน ตามภารกิจเพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เฉพาะในส่วนที่ได้รับมอบหมาย ตามความจำเป็นในการใช้งาน

๔.๒ ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน ตามที่ผู้บริหารระบบกำหนด

หมวดที่ ๒
การบริหารจัดการเข้าถึงของผู้ใช้งาน

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้วและสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิ การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อไม่ได้ปฏิบัติงาน โรงพยาบาลค่ายจิรประวัติ

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ระบบสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สามารถนำข้อมูลไปตรวจสอบได้ ประกอบด้วยชื่อ นามสกุล ตำแหน่ง สังกัด และหมายเลขโทรศัพท์ ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และพระราชบัญญัติอื่น ๆ ที่เกี่ยวข้อง

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรภายใน

(๑) ให้บุคลากรกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศและส่งแบบฟอร์มให้กับผู้ดูแลระบบ

(๒) ผู้ดูแลระบบนำส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และ ระบบสารสนเทศให้กับผู้บริหารระบบ

(๓) ให้ผู้บริหารระบบพิจารณาและอนุมัติสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศพร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้บุคคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลในการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศเสนอให้ผู้บริหารระบบเพื่อขอใช้งานระบบสารสนเทศ

(๓) ให้ผู้บริหารระบบเสนอให้ผู้อำนวยการโรงพยาบาลพิจารณาและอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้ผู้บริหารระบบกำหนดลักษณะอื่นใดตามที่ผู้บริหารระบบที่มีการตกลงร่วมกัน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ประกอบไปด้วย ชุดของตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา

๑.๓.๓ การกำหนดบัญชีผู้ใช้งานครั้งแรกให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน ทราบโดยตรง

๑.๓.๔ เมื่อผู้ใช้งานมีการเปลี่ยนแปลงข้อมูลให้หน่วยงานทำการแจ้งผู้บริหารระบบ เพื่อปรับปรุงข้อมูลให้เป็นปัจจุบัน

๒. การยกเลิกสิทธิการใช้งานของบุคลากรหรือบุคคลภายนอกและผู้ดูแลระบบให้ดำเนินการ ดังนี้

๒.๑ ให้หน่วยงานแจ้งผู้บริหารระบบ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก โอนย้าย หรือสิ้นสุดการจ้าง

๒.๑.๑ กรณี บุคลากรหรือบุคคลภายนอก ให้ผู้ดูแลระบบดำเนินการปิดบัญชีผู้ใช้งาน (Username) และแจ้งกลับไปยังหน่วยงานของบุคคลดังกล่าวให้รับทราบ ภายใน ๑ เดือน

๒.๑.๒ กรณีผู้ดูแลระบบ ให้ดำเนินการแจ้งผู้บริหารสิทธิยกเลิกการใช้งานสิทธิของตนเองทุกระบบงาน ทั้งนี้ให้ดำเนินการแจ้งหน่วยงานต้นสังกัดของบุคคลดังกล่าวหรือผู้บริหารระบบรับทราบการยกเลิกสิทธิ การใช้งาน ภายใน ๗ วันทำการ เมื่อมีการลาออก โอนย้าย หรือสิ้นสุดการจ้าง

๒.๑.๓ ผู้ใช้งานต้องดำเนินการเปลี่ยนแปลงข้อมูลนับจากได้รับแจ้งภายใน ๗ วันทำการ ก่อนการลาออก โอนย้าย หรือสิ้นสุดการจ้าง

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้

๓.๑ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้ง ผู้บริหารระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๒ ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับ สิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้บริหารระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้

๔.๑ ในกรณีผู้ใช้งานลืมรหัสผ่าน (Password) ให้แจ้งหน่วยงานที่รับผิดชอบ โดยใช้วิธีการของระบบโปรแกรมนั้นๆ ตามที่ผู้บริหารระบบได้กำหนดไว้

๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ - ๖ เดือน ตามความเสี่ยงของ ระบบโปรแกรม และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่านเดิม

๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ ตามที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล และพระราชบัญญัติอื่นๆ ที่เกี่ยวข้อง

หมวดที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User)

๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และ ระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับของโรงพยาบาลค่ายจิรประวัติ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ตามหมวดที่ ๒ ข้อ ๑.๓ และต้องเปลี่ยนรหัสผ่านตาม ข้อ ๔.๒

๑.๒ ผู้ใช้งานต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

๑.๓ ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และ ระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๔ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็น ในการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๕ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของ บัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำาหนดแล้ว

๒. สิทธิ์การเข้าถึง

๒.๑ ผู้ดูแลระบบ มีสิทธิ์การเข้าถึง ทุกระบบ ทุกเมนูการใช้งานต่างๆ

๒.๒ เวชระเบียน มีสิทธิ์การเข้าถึง ทะเบียนผู้ป่วย (Registry), รายงาน (Report), ผู้ป่วยใน (IPD), งาน Primary Care (PCU)

๒.๓ ซักประวัติ มีสิทธิ์การเข้าถึง ทะเบียนผู้ป่วย (Registry), ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), จ่ายยา (Dispensing), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), ทะเบียนผู้ป่วยโรคเรื้อรัง (Chronic)

๒.๔ แพทย์ มีสิทธิ์การเข้าถึง ทะเบียนผู้ป่วย (Registry), ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), ฉุกเฉิน (ER), จ่ายยา (Dispensing), นัดหมาย (Appoint), ตรวจสุขภาพ (Checkup), ผ่าตัด (Operation), ส่งต่อผู้ป่วย (Refer), รายงาน (Report), ผู้ป่วยใน (IPD), ทะเบียนผู้ป่วยโรคเรื้อรัง (Chronic)

๒.๕ อุบัติเหตุฉุกเฉิน มีสิทธิ์การเข้าถึง ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), ฉุกเฉิน (ER), จ่ายยา (Dispensing), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), รายงาน (Report)

๒.๖ เภสัชกรรม มีสิทธิ์การเข้าถึง ทะเบียนผู้ป่วย (Registry), ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), ตรวจทางห้องปฏิบัติการ (LAB), การเงิน (Finance), จ่ายยา (Dispensing), รายงาน (Report), ผู้ป่วยใน (IPD), Super User (Super_User)

๒.๗ ตรวจทางห้องปฏิบัติการ มีสิทธิ์การเข้าถึง ตรวจทางห้องปฏิบัติการ (LAB), รายงาน (Report), คลังโลหิต (Bloodbank)

๒.๘ รังสีวินิจฉัย มีสิทธิ์การเข้าถึง รังสีวินิจฉัย (Xray), รายงาน (Report)

๒.๙ ทันตกรรม มีสิทธิ์การเข้าถึง ห้องตรวจแพทย์ (Doctor), ทันตกรรม (Dental), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), จ่ายยา (Dispensing), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), รายงาน (Report), งาน Primary Care (PCU)

๒.๑๐ กายภาพบำบัด มีสิทธิ์การเข้าถึง กายภาพบำบัด (Physic), ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), รายงาน (Report)

๒.๑๑ ผู้ป่วยใน มีสิทธิ์การเข้าถึง ผู้ป่วยใน (IPD), ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), จ่ายยา (Dispensing), ผ่าตัด (Operation), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), รายงาน (Report)

๒.๑๒ งาน PCU มีสิทธิ์การเข้าถึง งาน Primary Care (PCU), ทะเบียนผู้ป่วย (Registry), ซักประวัติ (Screen), ห้องตรวจแพทย์ (Doctor), รังสีวินิจฉัย (Xray), ตรวจทางห้องปฏิบัติการ (LAB), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), รายงาน (Report)

๒.๑๓ แพทย์ทางเลือก มีสิทธิ์การเข้าถึง ห้องตรวจแพทย์ (Doctor), ซักประวัติ (Screen), จ่ายยา (Dispensing), นัดหมาย (Appoint), ส่งต่อผู้ป่วย (Refer), รายงาน (Report), ผู้ป่วยใน (IPD)

๒.๑๔ การเงิน มีสิทธิ์การเข้าถึง การเงิน (Finance), จ่ายยา (Dispensing), รายงาน (Report)

๓. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๔.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล (Process Device) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของหน่วยงานเท่านั้น

๔.๒ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของหน่วยงาน และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน

๔.๓ ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใดๆ ที่เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์และระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัด

๔.๔ ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูล แบบพกพา หรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๔.๕ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านสารสนเทศ ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน

๔.๖ การทำลายอุปกรณ์บันทึกข้อมูลให้ดำเนินการ ดังนี้

ประเภท	**กรณีนำสื่อบันทึกกลับมาใช้ใหม่**	**กรณีบันทึกข้อมูลชั้นความลับและนำสื่อบันทึกกลับมาใช้**	**กรณีไม่นำสื่อบันทึกกลับมาใช้ใหม่**
CD/DVD	-	-	ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบปฏิบัติการ	ใช้การ Factory Data Reset	- ให้ใช้การ Factory Data Reset - ระบบปฏิบัติการอื่นๆ ใช้การลบและเขียนข้อมูล ทับจนเต็มพื้นที่จัดเก็บ	ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบถอดแยกได้	ใช้การ Format	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย
เทปบันทึกข้อมูล	- ใช้การ Format - เขียนทับข้อมูลเป็นจำนวนหลายๆ รอบ	ใช้การ Format แบบ Zero-filling	ใช้การทุบ หรือทำลายให้เสียหาย
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse	ห้ามนำกลับมาใช้ใหม่	ใช้เครื่องทำลายเอกสาร

หมวดที่ ๔
การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศของหน่วยงานได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำาหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่ง ระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๖. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศและการส่งข้อมูลสารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑ การใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ ผู้ใช้งานสามารถเข้าบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองที่ ได้รับอนุญาตจากหน่วยงาน เพื่อเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet)

๑.๑.๒ ควรควบคุมการใช้งานระบบเครือข่ายคอมพิวเตอร์ (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูง และที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ เช่น รายการบันเทิงต่าง ๆ ในเวลาราชการ เป็นต้น

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย เป็นต้น

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของหน่วยงาน เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และ ระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน

๑.๒ การใช้งานโดเมนเนม (Domain Name) ของหน่วยงานในระบบเครือข่ายให้ดำเนินการ ดังนี้

๑.๒.๑ ห้ามนำโดเมนเนม (Domain Name) นำไปใช้ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้โดเมนเนม (Domain Name) ของหน่วยงาน

๑.๒.๓ หลังจากการใช้งานโดเมนเนม (Domain Name) ของหน่วยงานต้องออกจากระบบ (Log Out) ทันที

๑.๓ การใช้งานเครือข่าย Local Area Network (LAN) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ดูแลระบบต้องทำการตั้งค่า (Configuration) เลขที่อยู่ไอพี (IP Address) เมื่อนำอุปกรณ์มาใช้ภายในหน่วยงาน

๑.๓.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่าย Local Area Network (LAN)

๑.๔ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๔.๑ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดจากผู้ผลิตทันที เมื่อนำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๑.๔.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็น ของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi)

๑.๔.๓ ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของหน่วยงานไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๔.๔ ผู้ใช้งานควรระมัดระวังในการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งานเครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัย

๑.๔.๕ ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สาย (WiFi) ของหน่วยงานและมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๕.๑ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้หน่วยงาน ควรนำเสนอเกี่ยวกับภารกิจงานของหน่วยงาน เช่น ผลการดำเนินงาน และข่าวสาร โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายจากหน่วยงาน และต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐ และพระราชบัญญัติอื่นๆที่เกี่ยวข้อง ทั้งนี้ให้รายงานต่อผู้บังคับบัญชา

๑.๕.๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของหน่วยงานผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากผู้บริหารหน่วยงาน

๑.๕.๓ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๕.๔ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากหน่วยงาน และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๕.๕ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)ผู้ใช้งานต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที ทั้งนี้ให้แจ้งผู้บังคับบัญชารับทราบ

๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

๒.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๑ ปี หรือตามความเหมาะสม

๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ แท็ปเลต โทรศัพท์มือถือ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน

๓. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้

๓.๑ หน่วยงานที่ดูแลด้านสารสนเทศต้องดูแล/ตรวจสอบพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) รวมทั้งการควบคุมการเข้าถึงพอร์ตทางกายภาพและเครือข่าย

๓.๒ หน่วยงานที่ดูแลด้านสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อย ๑ เดือน

๓.๓ หน่วยงานต้องดำเนินการจัดทำรายงานผังข้อมูลการเปิดใช้งานพอร์ตที่เปิดให้บริการทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๔.๑ หน่วยงานที่ดูแลด้านสารสนเทศควรมีระบบป้องกันการบุกรุกโจมตีทางเครือข่าย Firewall เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๔.๒ ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศ

๔.๓ ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากหน่วยงานที่ดูแลด้านสารสนเทศทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นใน การเชื่อมต่อสัญญาณให้รายงานหน่วยงานที่ดูแลด้านสารสนเทศทันที

๔.๔ การเชื่อมต่อเครือข่ายสารสนเทศกับหน่วยงานภายนอกหรือเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ ต้องได้รับอนุญาตจากผู้บริหารของหน่วยงาน

๕. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๕.๑ ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้ การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ - ส่งหรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๕.๒ ผู้ดูแลระบบต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งานเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

หมวดที่ ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกัน การเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการโดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่ได้กำหนดไว้

แนวปฏิบัติ

๑. การกำหนดขั้นตอนการปฏิบัติงาน ดังนี้

๑.๑ ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น Product Key หรือ License ของระบบปฏิบัติการ และการตั้งค่า (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น เว้นแต่ได้รับอนุญาต

๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ ตามหมวดที่ ๒

๑.๓ หลังจากผู้ดูแลระบบติดตั้งระบบปฏิบัติการเสร็จ ผู้ใช้งานต้องบริหารจัดการรหัสผ่านหรือเปลี่ยนรหัสผ่านที่เป็นค่าเริ่มต้นโดยทันที

๑.๔ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานเป็นเวลา ๑๕ นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๑.๕ ก่อนการเข้าใช้ระบบปฏิบัติการผู้ใช้งานจะต้องเข้าสู่ระบบ (Login) ทุกครั้ง

๑.๖ ห้ามให้ผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม บนระบบปฏิบัติของหน่วยงาน

๑.๗ ห้ามผู้ใช้งานของหน่วยงานเข้าควบคุมระบบปฏิบัติการคอมพิวเตอร์หรือระบบสารสนเทศจากภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระบบ

๑.๘ ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรมประเภท Formatter หรือโปรแกรมที่มีความเสี่ยง เป็นต้น

๑.๙ ซอฟต์แวร์ที่หน่วยงาน ใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๑.๑๐ ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑.๑๑ ห้ามใช้สินทรัพย์ทุกประเภทของโรงพยาบาลค่ายจิรประวัติ เพื่อประโยชน์ทางการค้า

๑.๑๒ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๑.๑๓ ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้ รับอนุญาตจากหัวหน้าหน่วยงาน หรือ ผู้บริหารหน่วยงาน

๒. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมสำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ ให้ดำเนินการ ดังนี้

๒.๑ การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบ เพื่อจำกัดและควบคุมการใช้งาน

๒.๒ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๒.๓ ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นใน การใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

หมวดที่ ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศของผู้ใช้งาน

๒. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน โดยต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุม สภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกหน่วยงาน

๓. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๔. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกหน่วยงาน โดยต้องกำหนดข้อปฏิบัติแผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกหน่วยงาน

แนวปฏิบัติ

๑. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้อง ได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓. ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๓๐ นาที ระบบจะยุติการใช้งานผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

๔. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๔.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๔.๒ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๔.๓ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๔.๔ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๕. ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทขั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๕.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๕.๒ ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

๕.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๕.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๕.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๕.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึก เช่น การกำหนดแบบฟอร์ม ข้อตกลงให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และพระราชบัญญัติอื่นๆ ที่เกี่ยวข้อง

๕.๗ ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอโดยกำหนดความ ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ

๕.๔ ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และข้อมูลดังกล่าว จะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน

๕.๙ ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์กร โดยถูกจัดเก็บไว้บนอุปกรณ์แบบพกพาหรือถูก ส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากผู้บริหารระบบงานและธุรกรรม และทำการเข้ารหัสข้อมูล และระบบเครือข่ายไร้สายก่อนเท่านั้น

๕.๑๐ การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่ผู้บริหารระบบงาน และธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว

๖. ระบบที่มีข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) มีผลกระทบและ มีความสำคัญสูง เช่น ระบบข้อมูลการตรวจสุขภาพที่เกี่ยวข้องกับการรักษาพยาบาลและข้อมูลทางการแพทย์ ระบบบุคลากรที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายในโรงพยาบาลค่ายจิรประวัติ เป็นต้น ให้ปฏิบัติดังนี้

๖.๑ ต้องมีการควบคุมสภาพแวดล้อมของระบบสำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวโดยเฉพาะ

๖.๒ มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไป ปฏิบัติงานในห้องควบคุมดังกล่าว

๖.๓ ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึงข้อมูล

๖.๔ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร

๗. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติดังต่อไปนี้

๗.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๗.๒ ระมัดระวังไม่ให้บุคคลอื่นคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๗.๓ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๗.๔ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๕ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวดที่ ๗
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

เพื่อจัดหาระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของโรงพยาบาลค่ายจิรประวัติ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้วเพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่อง แม้ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม และสามารถใช้งานสารสนเทศได้อย่างต่อเนื่องให้สอดคล้องกับพระราชบัญญัติการรักษามั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และพระราชบัญญัติอื่น ๆ ที่เกี่ยวข้อง

นโยบาย

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๔. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของโรงพยาบาลค่ายจิรประวัติเพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

๑. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

๑.๑ จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๑.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

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

๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ์การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บริหารระบบ

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๑.๓.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลสุขภาพ บุคลากร ข้อมูลงบประมาณรายรับสถานพยาบาล และข้อมูลการรักษาพยาบาล เป็นต้น

- ข้อมูลการรักษาพยาบาล เช่น ข้อมูลผู้ป่วย ข้อมูลยาและเวชภัณฑ์ ข้อมูลสถานพยาบาล เป็นต้น

๑.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๑.๓.๕ การกำหนดเวลาที่ได้เข้าถึง

๑.๓.๖ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๒. ข้อมูล ข่าวสารสารสนเทศทุกประเภทในฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน ผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบ ความถูกต้องของการใช้งานฐานข้อมูล ทั้งนี้ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และพระราชบัญญัติอื่นๆที่เกี่ยวข้อง

๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังต่อไปนี้

๕.๑ กำหนดนโยบาย ขั้นตอนปฏิบัติและมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๕.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกัน หรือแลกเปลี่ยนข้อมูล เช่น วิธีการส่ง การรับ เป็นต้น

๕.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๕.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธ

๕.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น

๕.๖ กำหนดสิทธิ์การเข้าถึงข้อมูล

๕.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๕.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

๒. ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๓. ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔. ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง

๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๔.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๔.๔ ตรวจสอบค่าการกำหนดค่า (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล

๔.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๔.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๔.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๔.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๔.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๔.๑๐ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

๔.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๕. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

๕.๑ มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๕.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้เป็นต้น

๕.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๕.๔. มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๕.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ซอฟต์แวร์เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๕.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๖. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๗. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๘. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

๙. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๘
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยด้านสารสนเทศ ทำให้มั่นใจว่านโยบาย และ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒.การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๑.๑ จัดลำดับความสำคัญของความเสี่ยง

๑.๒ ค้นหาวิธีการนำเนินการเพื่อลดความเสี่ยง

๑.๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

๑.๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๑.๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๑.๖ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๑.๖.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๑.๖.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๑.๖.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๑.๖.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลที่แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๑.๖.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้ และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนในหน่วยงาน เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

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

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Anti-virus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่ สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

<u>ประเภทที่ ๔</u> ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วม จัดเป็นภัย ร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) นำอุปกรณ์ Back up ข้อมูลทั้งหมด ไปเก็บไว้ในที่ปลอดภัย

(๓) นำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าและเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์สามารถใช้งานได้ปกติหรือไม่แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๙
การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศข้อมูล ซึ่งมี ผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวทางปฏิบัติ

๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้

๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลเป็นจำนวนมาก

๒.๓ จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๒.๔ จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๒.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจากบริเวณดังกล่าว

๒.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

๒.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

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

๔. การควบคุมการเข้าออก อาคารสถานที่

๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๒ การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษา ความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๔.๕ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๔.๖ จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๔.๗ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๘ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๔.๙ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๐ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๔.๑๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๔.๑๒ มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๔.๑๓ จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๔ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

๕.๑.๑ ระบบสำรองกระแสไฟฟ้า (UPS)

๕.๑.๒ เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

๕.๑.๓ ระบบระบายอากาศ

๕.๑.๔ ระบบปรับอากาศ และควบคุมความชื้น

๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๖.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการติดต่อสัญญาณผิดเส้น

๖.๕ จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๖.๗ พิจารณาใช้งานสายไฟเบอร์ออปติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ coaxial cable สำหรับระบบสารสนเทศที่สำคัญ

๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๑ ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๔.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๙.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง ดังนี้

๑๐.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๑๐
การใช้สื่อสังคมออนไลน์และการส่งข้อมูลของผู้ป่วยโดยใช้สื่อสังคมออนไลน์ เพื่อปรึกษาการดูแลรักษาผู้ป่วยของบุคลากร

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการปฏิบัติสำหรับบุคลากรของโรงพยาบาลค่ายจิรประวัติ ได้ใช้สื่อสังคมออนไลน์อย่างเหมาะสม สร้างสรรค์ และเกิดประโยชน์ ต่อผู้รับบริการมากที่สุด

๒. เพื่อเป็นการระมัดระวังในการ ใช้สื่อสังคมออนไลน์ในการส่งข้อมูลผู้ป่วยโดยการคำนึงถึงการรักษาความลับของผู้ป่วยขณะเดียวกันกับการสร้างความมั่นใจในการระบุตัวตนผู้ป่วยอย่างถูกต้องในการปรึกษาการดูแลรักษาผู้ป่วย

แนวทางปฏิบัติ

ส่วนที่ ๑ การใช้สื่อสังคมออนไลน์

สื่อสังคมออนไลน์ หมายถึง สื่อหรือช่องทางในการติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูล ระหว่างบุคคล โดยใช้เทคโนโลยีสารสนเทศ ที่เน้นการสร้างและเผยแพร่เนื้อหาระหว่างผู้ใช้งานด้วยกัน (Creation and Exchange of Use-Generated) หรือสนับสนุนการสื่อสารสองทาง หรือการนำเสนอและ เผยแพร่เนื้อหาในวงกว้างได้ด้วยตนเอง ซึ่งนิยมเรียกกันเป็นภาษาอังกฤษว่า Social media หรือ Social Network ซึ่งรวมถึงสื่อดังต่อไปนี้

- กระดานข่าว (Web board)
- เครือข่ายสังคมออนไลน์ เช่น Facebook, LINE, WhatsApp เป็นต้น
- สื่อสำหรับการเผยแพร่และแลกเปลี่ยนเนื้อหาที่เป็นภาพนิ่ง เสียง วีดิทัศน์ หรือ แฟ้มข้อมูล หรือให้บริการเนื้อที่เก็บข้อมูลบนอินเตอร์เน็ต เช่น YouTube, Instagram, Microsoft OneDrive เป็นต้น
บล็อก (blog) เช่น WordPress, blogger เป็นต้น
- เว็บไซต์สำหรับการสร้างและแก้ไขเนื้อหาร่วมกัน เช่น Wikipedia เป็นต้น
- เกมออนไลน์หรือโลกเสมือนที่มีผู้ใช้งานหลายคน
- สื่ออิเล็กทรอนิกส์หรือสื่อออนไลน์ในลักษณะเดียวกันหรือคล้ายคลึงกันที่เปิดให้ใช้งาน เพื่อเป็นช่องทางสื่อสารระหว่างบุคคล ระหว่างกลุ่มคน หรือกับสาธารณะ

การใช้สื่อสังคมออนไลน์มีแนวทางปฏิบัติสำหรับผู้ที่ใช้สื่อสังคมออนไลน์เพื่อให้แสดงตนในฐานะบุคลากรในสังกัดโรงพยาบาลค่ายจิรประวัติ ดังนี้

๑.พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่ในสื่อสังคมออนไลน์ ผู้เผยแพร่ต้อง รับผิดชอบความเสียหาย ทั้งทางด้านจริยธรรม ด้านสังคมและด้านกฎหมาย นอกจากนี้ ยังอาจมีผลกระทบต่อชื่อเสียงการทำงานและอนาคตของวิชาชีพ

๒. พึงใช้ความระมัดระวังอย่างยิ่งในการเผยแพร่ความคิดเห็น ที่อาจกระตุ้นหรือนำไปสู่การโต้แย้งที่รุนแรง เช่น เรื่องเกี่ยวกับการเมือง เชื้อชาติ ศาสนา พระมหากษัตริย์ พระบรมวงศานุวงศ์ รวมถึงการวิพากษ์องค์กรหรือสถาบันต่างๆ

๓. พึงระลึกว่า การละเมิดจรรยาบรรณอย่างร้ายแรงที่กำหนดไว้ในข้อบังคับ ว่าด้วยพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เช่น การเปิดเผย ความลับของบุคลากรหรือผู้รับบริการที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจ ที่ก่อให้เกิดความเสียหายแก่บุคลากรหรือผู้รับบริการ หรือการ

ทำให้เกิดความเสียหายอย่าง ร้ายแรงแก่ทรัพย์สิน เกียรติ และชื่อเสียงของโรงพยาบาล ถือเป็นความผิดทางวินัยอย่างร้ายแรง และผู้พี่ละเมิดสามารถถูกดำเนินการทางวินัยและทางกฎหายได้ด้วย โดยสามารถศึกษาจากประกาศพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ ของผู้ปฏิบัติงานสุขภาพ พ.ศ. ๒๕๕๙

๔. พึงระมัดระวังการเผยแพร่ข้อมูลข่าวสาร ภาพ หรือข้อความที่เป็นการละเมิดสิทธิส่วนบุคคล

๕. พึงแยกบัญชีผู้ใช้ (account) ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออก จากกันให้ชัดเจน

๖. พึงระมัดระวังในการใช้ถ้อยคำและภาษาในการสื่อสารให้มีความเหมาะสม หลีกเลี่ยงการใช้ภาษาที่ไม่สุภาพ ไม่สร้างสรรค์ ตลอดจนการใช้ภาษาที่อาจก่อให้เกิดความเข้าใจคลาดเคลื่อน เข้าข่ายดูหมิ่นหรือหมิ่นประมาทบุคคลอื่น

๗. หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของส่วนงานหรือโรงพยาบาล ต้องแจ้งให้หัวหน้างาน หรือทีมสารสนเทศ โรงพยาบาลค่ายจิรประวัติทราบ แล้วแต่กรณี และต้องแจ้งรายชื่อของผู้ดูแลระบบ หรือ เจ้าของ Account นั้นให้หัวหน้างานหรือทีมสารสนเทศ โรงพยาบาลค่ายจิรประวัติทราบ และผู้ดูแลมีหน้าที่ต้องมอบสิทธิ์ในการดูแล Page หรือ Account นั้นคืนแก่ส่วนงานหรือโรงพยาบาล เมื่อพ้นจาการหน้าที่ที่ต้องดูแล หรือพ้นสภาพจาการเป็นบุคลากรของ โรงพยาบาล

๘. การเผยแพร่ข้อมูล หรือแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นจาก โรงพยาบาล ส่วนงานหรือหน่วยงาน ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของโรงพยาบาล ส่วนงาน หรือ หน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของโรงพยาบาลส่วนงานหรือหน่วยงานอย่าง แท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้องแล้วแต่กรณี

๙. ผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความเห็นเนื่องจาก ถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของ ผู้ใต้บังคับบัญชาได้ ทั้งนี้ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจน เช่นเดียวกับ ข้อ ๗

๑๐. ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของโรงพยาบาล หรือข้อมูลที่ใช้ภายใน โรงพยาบาลค่ายจิรประวัติก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ

๑๑. บุคลากรที่ปฏิบัติงานวิชาชีพ หรือเป็นผู้ให้บริการสุขภาพหรือบริการอื่นใด พึงตระหนักถึง ความรับผิดชอบในการเผยแพร่ข้อมูลเกี่ยวกับผู้รับบริการ เนื่องจากผลของการเผยแพร่ ข้อมูล อาจมีผลกระทบต่อผู้รับบริการ หน่วยงาน และวิชาชีพของตนได้

๑๑.๑ ระมัดระวังอย่างยิ่งในการใช้ Social Media ในการปฏิสัมพันธ์กับผู้รับบริการ โดยเฉพาะไม่ควรใช้ Account ที่ใช้สำหรับเรื่องส่วนตัวเพื่อการนี้ เนื่องจากไม่มีวิธีที่ได้ผลสมบูรณ์ในการปกปิดความลับของผู้รับบริการบน Social Media

๑๑.๒ ปฏิบัติตามจริยธรรมของวิชาชีพอย่างเคร่งครัด

๑๑.๓ เคารพและระมัดระวังอย่างยิ่ง ไม่ให้มีการละเมิดความเป็นส่วนตัว(Privacy) และ ความลับ (Confidentiality) ของผู้รับบริการ

๑๑.๔ หากต้องการเผยแพร่ข้อมูลเพื่อการศึกษา เช่น รูปถ่าย หรือสื่ออื่นๆ ที่มาจาก ผู้รับบริการ ต้องขออนุญาตจากผู้รับบริการนั้นก่อนเสมอ และต้องลบข้อมูลที่อาจจะทำ ให้มีการทราบถึงตัวตนของ

ผู้รับบริการนั้นทั้งหมด เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้รับบริการ ทั้งนี้ให้รวมถึงการเผยแพร่ข้อมูลในกลุ่มปิดเฉพาะด้วย

๑๑.๕ หากพบการใช้สื่อ Social Media ที่เกี่ยวกับผู้รับบริการอย่างไม่เหมาะสม หรือพบว่า มีข้อความบน Social Media ที่อาจก่อให้เกิดความเสื่อมเสียชื่อเสียงของหน่วยงาน ให้แจ้งทีมบริหารความเสี่ยงและทีมสารสนเทศทันที

๑๒. พึงศึกษา การใช้ การตั้งค่าความเป็นส่วนตัว หรือ Privacy Setting ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบทของตน

๑๓. พึงระลึกถึงหลักทั่วไปของผู้ปฏิบัติงานด้านสุขภาพที่เกี่ยวข้องกับสื่อสังคมออนไลน์ประกาศคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของ ผู้ปฏิบัติงานสุขภาพ พ.ศ. ๒๕๕๙ ดังนี้

๑๓.๑ หลักเคารพกฎหมาย

๑๓.๒ หลักการเคารพในจริยธรรมแห่งวิชาชีพประกอบด้วย

๑๓.๒.๑ หลักการป้องกันอันตรายต่อผู้อื่น

๑๓.๒.๒ หลักการมุงประโยชน์ของผู้ป่วยเป็นสำคัญ

๑๓.๒.๓ หลักรักษาความเป็นวิชาชีพตลอดเวลา

๑๓.๒.๔ หลัก “คิดก่อนโพสต์”

๑๓.๒.๕ หลักการตรวจสอบเนื้อหาออนไลน์ของตนอยู่เสมอ

๑๓.๒.๖ หลักการ “เช็คก่อนแชร์”

๑๓.๓ หลักหารเคารพในกฎระเบียบและนโยบายองค์กร

๑๓.๔ หลักการเคารพศักดิ์ศรีความเป็นมนุษย์และการหลีกเลี่ยงการทำให้ผู้อื่นเสียหาย

๑๓.๕ หลักการรายงานพฤติกรรมที่ไม่เหมาะสมในการใช้สื่อสังคมออนไลน์ หลักเสรีภาพทางวิชาการ

ส่วนที่ ๒ การส่งข้อมูลของผู้ป่วย

ปัจจุบันมีการใช้สื่อสังคมออนไลน์มากขึ้นและมีโอกาสที่ข้อมูลการระบุตัวตนของผู้ป่วยจะรั่วไหลไปสู่สังคมในวงกว้างได้ ก่อให้เกิดความเสียหายแกผู้ป่วยโดยผู้ส่งไม่รู้ตัว เพื่อเป็นการระมัดระวังในการ ใช้สื่อสังคมออนไลน์ในการส่งข้อมูลผู้ป่วยโดยการคำนึงถึงการรักษาความลับของผู้ป่วยขณะเดียวกันกับการสร้างความมั่นใจในการระบุตัวตนผู้ป่วยอย่างลูกต้องในการปรึกษาการดูแลรักษาผู้ป่วย โรงพยาบาลค่ายจิรประวัติ จึงได้กำหนดแนวทางปฏิบัติการส่งข้อมูลของผู้ป่วยโดยใช้สื่อสังคม ออนไลน์ โดยยึดแนวทางปฏิบัติที่คณะกรรมการสุขภาพแห่งชาติ กำหนดเป็นหลัก ดังนี้

๑. ควรใช้สื่อสังคมออนไลน์ เช่น Line, Messenger ในลักษณะบุคคลต่อบุคคล ไม่ควรใช้สื่อสังคมออนไลน์แบบกลุ่ม เช่น Line Group เนื่องจากหากมีข้อมูลรั่วไหลจะยากต่อการตามรอยหาจุดรั่วไหล

๒. กรณีจำเป็นต้องใช้สื่อสังคมออนไลน์แบบกลุ่ม เช่น Line Group ควรรักษาความลับของผู้ป่วยโดยการปกปิดข้อมูลที่ทำให้ผู้อ่านสามารถระบุตัวผู้ป่วยได้แล้วใช้รหัส ID แทน หลังจากนั้นให้ส่งตัวถอดรหัส ID ไปเป็นชื่อตัวบุคคลผ่านช่องทางที่ ๒ เช่น Line, SMS, E-mail ของผู้ให้คำปรึกษา

๓. หลีกเลี่ยงการขอคำปรึกษาผู้ป่วยพร้อมกันมากกว่า ๑ ราย ในการปรึกษา ๑ ครั้ง เพื่อป้องกัน ข้อมูลบุคคลสลับกัน

๔. การปรึกษาโดยใช้ภาพถ่าย เช่น ภาพถ่าย X-ray, EKG, ผล LAB ควรใช้ภาพถ่ายที่มีความ ละเอียดของภาพสูงเพียงพอเพื่อให้เห็นรายละเอียดของภาพที่ขอปรึกษา เช่น รอยกระดูกหัก เป็นต้น เพื่อการ วินิจฉัยที่ถูกต้อง

๕. ผู้ให้คำปรึกษาจะต้องรักษาความลับของผู้ป่วย และทำลายข้อมูลที่ได้รับ เมื่อกระบวนการให้คำปรึกษาเสร็จสิ้น เพื่อป้องกันการรั่วไหลของข้อมูลในกรณีที่นำเครื่องไปซ่อมบำรุง

๖. ยึดตามหลักการปฏิบัติด้วยความระมัดระวังในการให้คำปรึกษาออนไลน์ ตามประกาศคณะกรรมการสุขภาพแห่งชาติ เรื่อง แนวทางปฏิบัติในการใช้งานสื่อสังคมออนไลน์ของผู้ปฏิบัติงานสุขภาพ พ.ศ. ๒๕๕๙

ภาคผนวก

ข้อปฏิบัติการเข้าใช้งานห้องศูนย์ข้อมูล (Data Center)

เพื่อให้การเข้าออกห้องศูนย์ข้อมูล (Data Center) เป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัย จึงได้มีการกำหนดข้อปฏิบัติดังนี้ ดังนี้

๑. บุคคลผู้มีสิทธิเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) ประกอบด้วย

๑.๑ ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) หมายถึง เจ้าหน้าที่ ๆ ได้รับมอบหมายจากผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ ให้รับผิดชอบ ดูแลห้องศูนย์ข้อมูล (Data Center)

๑.๒ เจ้าหน้าที่ผู้รับผิดชอบห้องศูนย์ข้อมูล (Data Center) จากบริษัท หมายถึง เจ้าหน้าที่ของบริษัทที่ได้รับการผู้รับจ้างในการบำรุงรักษาเครือข่าย ห้องศูนย์ข้อมูล (Data Center) โรงพยาบาลค่ายจิรประวัติ

๑.๓ บุคคลภายนอก หมายถึง ผู้ที่เข้ามาปฏิบัติงานตามภารกิจ โดยต้องการรับการอนุมัติจากผู้อำนวยการโรงพยาบาลค่ายจิรประวัติ

๒. การเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) มีขั้นตอนดังนี้

๒.๑ ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) เข้าใช้งานโดยการสแกนลายนิ้วมือ หรือ รหัส การใช้งานของอุปกรณ์เปิด – ปิด ประตู หน้าห้องศูนย์ข้อมูล (Data Center)

๒.๒ เจ้าหน้าที่ผู้รับผิดชอบห้องศูนย์ข้อมูล (Data Center) จากบริษัท เข้าใช้งานโดยการสแกนลายนิ้วมือ หรือรหัส การใช้งานของอุปกรณ์เปิด - ปิด ประตู หน้าห้องศูนย์ข้อมูล (Data Center) โดยได้รับการอนุมัติการนำเข้าลายนิ้วมือจากได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center)

๒.๓ บุคคลภายนอกจะต้องทำเป็นหนังสือขอเข้าพื้นที่เป็นลายลักษณ์อักษรเท่านั้น โดยให้หนังสือจะต้องระบุ วัน เวลา ที่ชัดเจน จำนวน หรือรายชื่อบุคลากร พร้อมด้วยเหตุผลความจำเป็นโดยมีผู้ได้รับมอบหมาย ให้ดูแลห้องศูนย์ข้อมูล (Data Center) เป็นผู้นำพาเข้าและควบคุมตลอดเวลา

๒.๔ บุคคลภายนอก ต้องลงทะเบียนเซ็นชื่อการเข้าในสมุดหน้าห้องทุกครั้ง และเมื่อเสร็จภารกิจต้องเซ็นชื่อออก ทุกครั้งเช่นกัน

๓. ระยะเวลาการเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) มีรายละเอียด ดังนี้

๓.๑ วันและเวลาราชการ ๘.๓๐ - ๑๖.๓๐ น.

๓.๒ กรณีที่มีเหตุฉุกเฉิน หรือนอกวันและเวลาราชการ ที่มีความจำเป็นต้องเข้าห้องศูนย์ข้อมูล (Data Center) ให้แจ้งได้รับมอบหมายให้ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) ทราบถึงเหตุผลและความจำเป็นในการเข้าไปใช้งาน

๔. ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center)

๕. ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๕. เมื่อเสร็จภารกิจให้ตรวจสอบความเรียบร้อยก่อนออกจากศูนย์ข้อมูล (Data Center) เช่น ไฟ ประตู

เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) โรงพยาบาลค่ายจิรประวัติ ได้แก่

๑.นาย ธงชัย คงเพชร	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙
๒.นาย ไพรัช พงศ์เมตต์	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙
๓.นาย อนุสรณ์ ปานกรด	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙
๔.น.ส. รดาณัฐ ศรีอรุณ	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙
๕.น.ส.วรรณนภา ฉายเพ็ชร์	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙

ผู้ควบคุม

๑. พ.ต.หญิงไพลิน สิทธิสมาน หัวหน้าทะเบียนการแพทย์และงานเวชระเบียน
เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙

เจ้าหน้าที่ผู้ได้รับมอบหมายให้สำรองของระบบสารสนเทศ โรงพยาบาลค่ายจิรประวัติ โดยสำรองข้อมูลระบบที่กลุ่มเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบ ได้แก่

๑.นาย ธงชัย คงเพชร	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙
๒.นาย ไพรัช พงศ์เมตต์	เจ้าหน้าที่ศูนย์คอมพิวเตอร์	เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙

ผู้ควบคุม

๑. พ.ต.หญิงไพลิน สิทธิสมาน หัวหน้าทะเบียนการแพทย์และงานเวชระเบียน
เบอร์ ๐๕๖-๒๕๕๑๒๑ ต่อ ๓๑๓๕๙

หมายเหตุ เจ้าหน้าที่ผู้ได้รับมอบหมายให้สำรองของระบบสารสนเทศ กอง/กลุ่ม ให้สำรองข้อมูลของหน่วยงานของตนเอง