กรมสุขภาพจิต
ศูนย์สุขภาพจิตที่ ๖

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
ศูนย์สุขภาพจิตที่ ๖

สารบัญ

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สุขภาพจิตที่ ๖

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของศูนย์สุขภาพจิตที่ ๖

ตามประกาศศูนย์สุขภาพจิตที่ ๖ เรื่องนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของศูนย์สุขภาพจิตที่ ๖ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์สุขภาพจิตที่ ๖ เพื่อให้ระบบเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ ๖ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อศูนย์สุขภาพจิตที่ ๖ นั้น

ศูนย์สุขภาพจิตที่ ๖ จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศศูนย์สุขภาพจิตที่ ๖ เรื่อง แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์สุขภาพจิตที่ ๖ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ คำนิยาม

“หน่วยงาน” หมายถึง ศูนย์สุขภาพจิตที่ ๖

“ผู้บริหาร” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน

“เจ้าของระบบ” (System Owner) หมายความว่า โรงพยาบาล/สถาบัน/สานัก/กอง/ศูนย์/กลุ่ม ที่เป็นผู้รับผิดชอบหลักในการพัฒนาระบบคอมพิวเตอร์และระบบสารสนเทศ โดยมีวัตถุประสงค์เพื่อสนับสนุนภารกิจการปฏิบัติงานของหน่วยงานให้เกิดประสิทธิภาพต่อศูนย์สุขภาพจิตที่ ๖ ในภาพรวม หรือตามที่ผู้อานวยการมอบหมาย และมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน (User)

“นโยบาย” หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องกับภารกิจของศูนย์สุขภาพจิตที่ ๖ เพื่อเป็นทิศทางให้ผู้ดูแลระบบ (Administrator) ผู้ใช้งาน (User) และบุคคลภายนอกได้ถือปฏิบัติ

“แนวปฏิบัติ” หมายถึง แนวทางหรือข้อกำหนดให้ผู้ใช้งาน (User) และบุคคลภายนอกได้ถือปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

“ผู้ดูแลระบบ” หมายถึง บุคลากร ศูนย์สุขภาพจิตที่ ๖ ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการหน่วยงานให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศของระบบเทคโนโลยีสารสนเทศ

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของ

ระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“ผู้ใช้งาน” หมายถึง บุคลากรศูนย์สุขภาพจิตที่ ๖ ทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมาและบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่ายและโปรแกรมประยุกต์หรือแอปพลิเคชันของ และ/หรือเกี่ยวข้องกับการใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศ

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

“สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟท์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศหรือสิ่งอื่นใดก็ตามที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ ๖ ประกอบด้วย

๑. ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์คุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งต่อไปนี้

- เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทั้งแบบเครื่องแม่ข่ายปกติ (Rack Server) และเครื่องแม่ข่าย
- เครื่องคอมพิวเตอร์ลูกข่าย (Client) อันได้แก่ เครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Laptop) อุปกรณ์สื่อสารแบบพกพา (Tablet/Smart phone) รวมถึงอุปกรณ์สนับสนุน เครื่องพิมพ์ (printer/Scanner) และอุปกรณ์สำรองข้อมูลของศูนย์สุขภาพจิตที่ ๖
- อุปกรณ์โครงข่าย (Network) หรืออุปกรณ์รักษาความมั่นคงปลอดภัย (Firewall) หรืออุปกรณ์สำหรับเชื่อมต่อระบบสื่อสาร (Router, Switch, Access Point) หรืออุปกรณ์จัดเก็บบันทึกการใช้งาน (Log File)

๒. โปรแกรมประยุกต์หรือแอปพลิเคชัน (Program or Application) หมายถึง ระบบคุณลักษณะใกล้เคียงอย่างใดอย่างหนึ่งในต่อไปนี้ ระบบ, System Software, Database Software, Software Tool และ Application Software ที่ใช้งานร่วมกับอุปกรณ์ในหัวข้อ Hardware

“ระบบคอมพิวเตอร์” หมายถึง ระบบคอมพิวเตอร์ลูกข่ายแบบเสมือน (Virtualization System) ที่ติดตั้งบนอุปกรณ์ในการประมวลผลข้อมูล (Process Device) โดยเข้าถึงด้วยเทคโนโลยีแบบคลาวด์คอมพิวติ้ง (Cloud Computing) และระบบปฏิบัติการ (Operating System) ที่ติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) พร้อมด้วยโปรแกรมประยุกต์ (Application Software)

“ระบบสารสนเทศ” หมายถึง ระบบงานคอมพิวเตอร์ เช่น เว็บไซต์ ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) และระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น หรืออุปกรณ์เทคโนโลยีสารสนเทศที่ได้รับการพัฒนาหรือติดตั้ง หรือการนำมาประยุกต์ใช้ เพื่อสนับสนุนการปฏิบัติงาน

“ข้อมูลสารสนเทศ” หมายถึง ข้อมูล (Data) หรือสารสนเทศ (Information) ที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ เช่น แฟ้มข้อมูล (File) ฐานข้อมูล (Database) และเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (E-Document)

“พื้นที่ปฏิบัติงานทั่วไป” (General Working Area) หมายความว่า พื้นที่สำหรับการปฏิบัติงานภายในศูนย์สุขภาพจิตที่ ๖ ซึ่งได้รับการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์ลูกข่ายเสมือน เครื่องคอมพิวเตอร์พกพาอุปกรณ์ต่อพ่วง และเครือข่ายแบบไร้สาย (Wireless LAN)

“ห้องศูนย์ข้อมูล” (Data Center) หมายความว่า พื้นที่ที่มีความสำคัญที่กั้นแยกเฉพาะเพื่อติดตั้งอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ระบบเครือข่ายคอมพิวเตอร์ ระบบจัดเก็บข้อมูล

ระบบรักษาความมั่นคงปลอดภัย ระบบไฟฟ้า ระบบปรับอากาศ และระบบป้องกันอัคคีภัยซึ่งทำงานตลอด ๒๔ ชั่วโมงต่อวัน เพื่อให้บริการระบบคอมพิวเตอร์และระบบสารสนเทศแก่ผู้ใช้งาน (User)

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ รวมทั้งคุณสมบัติอื่น ๆ ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืน นโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบคอมพิวเตอร์และระบบสารสนเทศถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ ศูนย์สุขภาพจิตที่ ๖ ได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรพร้อมทั้งได้กำหนดให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบ กำกับดูแล ติดตามให้ผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจนดังนี้

๔.๑ การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๔.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๔.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๔.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๔.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๔.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๔.๗ การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

๔.๘ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management) โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ ๕ ศูนย์สุขภาพจิตที่ ๖ ได้ประกาศนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางเว็บไซต์หลักศูนย์สุขภาพจิตที่ ๖ และหนังสือเวียนภายในระบบสารบรรณอิเล็กทรอนิกส์ให้ผู้ใช้งาน เจ้าหน้าที่ และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามได้อย่างถูกต้อง

ข้อ ๖ ศูนย์สุขภาพจิตที่ ๖ ต้องบริหารระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติการรักษา

ความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง แต่ต้องสอดคล้องกับ “ประกาศศูนย์สุขภาพจิตที่ ๖ เรื่องแนวนโยบายและการปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ศูนย์สุขภาพจิตที่ ๖”

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ ๑
การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

วัตถุประสงค์

๑. เพื่อกำหนดการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัยด้านสารสนเทศ
๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิและการมอบอำนาจของหน่วยงานของรัฐ
๓. เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
๔. เพื่อให้การตรวจสอบและติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

นโยบาย

บุคลากรศูนย์สุขภาพจิตที่ ๖ และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น
๒. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน
๓. ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น
๔. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึง อย่างสม่ำเสมอ ดังนี้
    ๔.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้
        ๔.๑.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น
            - อ่านอย่างเดียว
            - สร้างข้อมูล
            - ป้อนข้อมูล

- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

๔.๑.๒ กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

๔.๑.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตาม ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๔.๒.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วย ข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

๔.๒.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๔.๒.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ข้อมูลลับ หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
- ข้อมูลใช้งานภายในองค์กร หมายถึง ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกองค์กร
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัย ข้อมูลที่เผยแพร่สู่สาธารณะ ผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณาอนุมัติ หากข้อมูลสูญหายหรือถูกเปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร

๔.๒.๔ จัดแบ่งระดับชั้นการเข้าถึง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๔.๒.๕ รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้
- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมี รูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)
- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ มีรูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

๕. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๖. เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าวต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากศูนย์สุขภาพจิตที่ ๖ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายบุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๗. การเข้าถึงห้องศูนย์ข้อมูล (Data Center) เพื่อปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ให้ดำเนินการ ดังนี้

๗.๑ ศูนย์สุขภาพจิตที่ ๖ ต้องกำหนดหลักเกณฑ์สำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center)

๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใด ๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากศูนย์สุขภาพจิตที่ ๖ ก่อนเริ่มดำเนินการทุกครั้ง

๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากศูนย์สุขภาพจิตที่ ๖

๗.๔ ผู้ใช้งาน (User) หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา และต้องไม่นำอาหาร หรือเครื่องดื่มเข้าไปในห้องศูนย์ข้อมูล (Data Center) และห้ามสูบบุหรี่ในห้องศูนย์ข้อมูล (Data Center)

๘. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๙. ผู้ดูแลระบบต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ตารางการแบ่งระดับชั้นของข้อมูล (Information Classification)

ระดับชั้นความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
ประเภทข้อมูล	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด สิทธิส่วนบุคคลละเมิดสิทธิส่วนบุคคลทำให้เสียชื่อเสียงและทรัพย์สินอย่างร้ายแรง หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อองค์กรในระดับสูงมาก	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง สิทธิส่วนบุคคลละเมิดสิทธิส่วนบุคคลทำให้เสียชื่อเสียงและทรัพย์สิน	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ สิทธิส่วนบุคคลละเมิดสิทธิส่วนบุคคล แต่ไม่ทำให้เสียชื่อเสียงและทรัพย์สิน	• ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกองค์กร • หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อองค์กรในระดับต่ำหรืออาจจะไม่มีผลกระทบใด ๆ	• ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัย ข้อมูลที่เผยแพร่สู่สาธารณะ ผ่านช่องทางที่เหมาะสม ซึ่งองค์กรพิจารณาอนุมัติ หากข้อมูลสูญหาย หรือถูกเปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร

ตารางการแบ่งระดับชั้นของข้อมูล (Information Classification) (ต่อ)

ระดับชั้นความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
ตัวอย่างเอกสาร	คำสั่งพิเศษที่ห้ามเปิดเผยข้อมูล	ข้อมูลใด ๆ ที่เจ้าหน้าที่พิจารณาแล้วกำหนดให้เป็นชั้นความลับมาก	ข้อมูลความลับทางราชการ ผลประเมินความเสี่ยง, แผนการซ้อม BCP, รายงานการซ้อม BCP Infrastructure Diagram, Key License, Asset Inventory List, สัญญาว่าจ้าง NDA, บันทึกต่าง ๆ ที่มีข้อมูลส่วนตัวของพนักงาน เป็นต้น	ข้อมูลคำรับรอง ข้อมูลบุคลากร, คู่มือการปฏิบัติงาน, IT Policy, Procedure, แบบฟอร์ม เป็นต้น	หลักเกณฑ์ต้องสื่อสารให้ได้ข้อมูล นโยบายระบบความมั่นคงปลอดภัย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคลที่เจ้าของข้อมูลให้เผยแพร่ได้ถ้ามี รายงานวิชาการ หลักฐานทางวิทยาศาสตร์ งานวิจัยที่มีการตีพิมพ์, ข้อมูลงบประมาณการเงินบัญชี Supplier, ประกาศต่าง ๆ ที่ต้องการสื่อสาร, ข้อมูลใน Web Site เป็นต้น

ตารางการแบ่งระดับชั้นของข้อมูล (Information Classification) (ต่อ)

ระดับชั้นความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
การเคลื่อนย้ายเอกสารภายนอกองค์กร	แสดงเครื่องหมายอักษรตัวโต สีแดงหรือสีที่เห็นได้ชัด ที่กระดาษด้านบนและล่างของทุกหน้า รวมด้านนอกหน้าปกหน้าและหลัง เอกสารที่เป็นม้วนหรือพับให้แสดงที่ม้วนหรือพับอยู่ แถวบันทึกที่อยู่ในกล่องหรือภาชนะ ต้องแสดงชั้นความลับที่สุดที่กล่องหรือภาชนะบรรจุซองหรือภาชนะทึบแสง ๒ ชั้น ระบุชื่อตำแหน่งผู้รับ, หน่วยงานที่ส่ง,ระบุเครื่องหมายแสดงชั้นความลับด้านหลังและด้านหลังของซองหรือภาชนะและปิดผนึกด้วยเทปกาว หรือวัสดุที่สามารถป้องกันการลักลอบเปิดอ่านได้	แสดงเครื่องหมายอักษรตัวโต สีแดงหรือสีที่เห็นได้ชัดที่กระดาษด้านบนและล่างของทุกหน้า รวมด้านนอกหน้าปกหน้าและหลังเอกสารที่เป็นม้วนหรือพับให้แสดงที่ม้วนหรือพับอยู่ แถวบันทึกที่อยู่ในกล่องหรือภาชนะต้องแสดงชั้นความลับมาก ที่กล่องหรือภาชนะบรรจุซองหรือภาชนะทึบแสง ๒ ชั้น ระบุชื่อตำแหน่งผู้รับ, หน่วยงานที่ส่ง, ระบุเครื่องหมายแสดงชั้นความลับด้านหลังและด้านหลังของซองหรือภาชนะและปิดผนึกด้วยเทปกาว หรือวัสดุที่สามารถป้องกันการลักลอบเปิดอ่านได้	แสดงเครื่องหมายอักษรตัวโต สีแดงหรือสีที่เห็นได้ชัดที่กระดาษด้านบนและล่างของทุกหน้า รวมด้านนอกหน้าปกหน้าและหลัง เอกสารที่เป็นม้วนหรือพับให้แสดงที่ม้วนหรือพับอยู่ แถวบันทึกที่อยู่ในกล่องหรือภาชนะต้องแสดงชั้นความลับ ที่กล่องหรือภาชนะบรรจุซองหรือภาชนะทึบแสง ๒ ชั้น ระบุชื่อตำแหน่งผู้รับ, หน่วยงานที่ส่ง, ระบุเครื่องหมายแสดงชั้นความลับด้านหลังและด้านหลังของซองหรือภาชนะและปิดผนึกด้วยเทปกาว หรือวัสดุที่สามารถป้องกันการลักลอบเปิดอ่านได้	สอดซองปิดผนึก และระบุชื่อ-ที่อยู่ของผู้รับ และระบุใช้งานภายในองค์กรเท่านั้น	ไม่มีข้อจำกัด

ตารางการแบ่งระดับชั้นของข้อมูล (Information Classification) (ต่อ)

ระดับชั้นความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
วิธีการดูแลรักษาข้อมูล	จัดเก็บในแผนกที่เกี่ยวข้องเท่านั้น และมีการเข้ารหัสข้อมูลทั้งหมดในระหว่างที่จัดเก็บ	จัดเก็บในแผนกที่เกี่ยวข้องเท่านั้น และมีการเข้ารหัสข้อมูลทั้งหมดในระหว่างที่จัดเก็บ	จัดเก็บในแผนกที่เกี่ยวข้องเท่านั้น และมีการเข้ารหัสข้อมูลทั้งหมดในระหว่างที่จัดเก็บ	เก็บใน Folder ของแต่แผนก	แผนกที่ทำการจัดเก็บ
การส่งต่อข้อมูล	มีการกำหนดรหัสเข้าไฟล์ข้อมูล	มีการกำหนดรหัสเข้าไฟล์ข้อมูล	มีการกำหนดรหัสเข้าไฟล์ข้อมูล	ส่งทางอีเมล หรือส่งมาใน Share Drive เท่านั้น	ส่งทางอีเมล ทำเป็นประกาศขึ้นเว็บไซต์ ทางไลน์
การทำลายเอกสาร	เผาทำลาย	เผาทำลาย	เผาทำลาย	ใช้เครื่องทำลายเอกสาร	ไม่มีข้อจำกัด
การเข้าถึงข้อมูล	ผู้บริหาร, ผู้อำนวยการ	ผู้บริหาร, ผู้อำนวยการ	ผู้บริหาร, ผู้อำนวยการ, หัวหน้ากลุ่มงาน, DC	ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย	ผู้ใช้งานทั่วไป

๑๐. การจัดการสื่อบันทึกข้อมูล (Media Handing)

๑๐.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยก/เคลื่อนย้ายได้ (Management of Removable Media) กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ต้องจัดให้มีกระบวนการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล และไม่ให้สามารถกู้คืนข้อมูลได้

๑๐.๒ การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

๑๐.๒.๑ ผู้ดูแลระบบ/ผู้ใช้งานต้องทำลายข้อมูลที่เป็นความลับ ที่บันทึกในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบ หรือเขียนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันการรั่วไหลของข้อมูล หรือป้องกันไม่ให้ข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้เครื่องหั่นแผ่น CD/DVD หรือกรรไกตัดทำลาย
ฮาร์ดดิสก์	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

๑๐.๒.๒ กรณีที่จัดเก็บเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูล อาจเสื่อมสภาพรวมทั้ง วิธีการนำข้อมูลกลับมาใช้ใหม่

๑๐.๓ การขนย้ายสื่อบันทึก (Physical Media Transfer)

๑๐.๓.๑ ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการจะต้องดูแลรักษาความปลอดภัย จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์หรือทำให้เสียหายระหว่างการขนย้าย

๑๐.๓.๒ ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการ ต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าของทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทเลินเล่อของผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึก

หมวดที่ ๒
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน (User) ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานแล้ว

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัดและเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ

๔. กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุมโดยเริ่มตั้งแต่ กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ได้รับของผู้ใช้งาน (User) การส่งมอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการกำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

๕. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

๖. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๗. กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติ

๑. การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

- ๑.๑ กรณีบุคลากรศูนย์สุขภาพจิตที่ ๖
  - ๑.๑.๑ บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้ศูนย์สุขภาพจิตที่ ๖ เพื่อสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านการใช้งาน
  - ๑.๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งานระบบฯ ให้บุคลากรใหม่ ตามสิทธิพร้อมทั้งแจ้งให้บุคลากรใหม่ได้รับทราบ
- ๑.๒ กรณีบุคคลภายนอก

๑.๒.๑ ให้สำนัก/กอง/ศูนย์/กลุ่ม แจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบ คอมพิวเตอร์และระบบสารสนเทศโดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบ คอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก

๑.๒.๒ ให้ศูนย์สุขภาพจิตที่ ๖ พิจารณาเหตุผลดังกล่าวก่อนดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านในการใช้งาน วันหมดอายุ ส่งต่อให้สำนัก/กอง/ศูนย์/กลุ่ม เพื่อแจ้งให้บุคคลภายนอกได้รับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานเพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย ๘ ตัวขึ้นไป ซึ่งต้องประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) ประกอบด้วย ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวอักษรพิเศษ (Special character)

- ตัวอักษร (a-z, A-Z)
- ตัวเลข (๐-๙)
- เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๓.๓ ให้ผู้ดูแลระบบ (Administrator) แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน (User) ทราบโดยตรง

๑.๓.๔ เมื่อบุคลากรมีการเปลี่ยนชื่อหรือนามสกุลให้แจ้งศูนย์สุขภาพจิตที่ ๖ เพื่อเปลี่ยนแปลงข้อมูลส่วนบุคคลให้ถูกต้อง

๑.๔ การยกเลิกสิทธิการใช้งานของบุคลากรศูนย์สุขภาพจิตที่ ๖ หรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๑.๔.๑ กรณีบุคลากรศูนย์สุขภาพจิตที่ ๖

๑.๔.๑.๑ ให้บุคลากร แจ้งศูนย์สุขภาพจิตที่ ๖ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง

๑.๔.๑.๒ ศูนย์สุขภาพจิตที่ ๖ จะปิดบัญชีผู้ใช้งาน (Username) ชั่วคราว เป็นเวลา ๙๐ วัน หากบุคลากรที่มีความประสงค์จะใช้ข้อมูลในบัญชีผู้ใช้งาน (Username) ดังกล่าว ให้แจ้งความประสงค์พร้อมเหตุผลต่อศูนย์สุขภาพจิตที่ ๖ เพื่อขอเปิดใช้งาน บัญชีผู้ใช้งาน (Username) ทั้งนี้เมื่อครบกำหนด ๙๐ วันนับจากมีคำสั่งเป็นลายลักษณ์อักษร ศูนย์สุขภาพจิตที่ ๖ จะลบข้อมูลสารสนเทศของบัญชีผู้ใช้งาน (Username) ดังกล่าวเป็นการถาวร

๑.๔.๒ กรณีบุคคลภายนอก

ระบบจะยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศอัตโนมัติเมื่อครบกำหนดเวลาการใช้งานตามคำขอใช้งาน

๒. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน (User) ให้ดำเนินการ ดังนี้

๒.๑ ผู้ดูแลระบบ (Administrator) ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับบุคลากร หรือบุคคลภายนอกให้สอดคล้องกับคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ หรือเหตุผลความจำเป็นของสำนัก/กอง/ศูนย์/กลุ่ม ที่ได้แจ้งความประสงค์ในการให้บุคคลากรเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ แล้วแต่กรณี

๒.๒ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่ง หรือหน้าที่ที่ได้รับมอบหมาย ให้แจ้งศูนย์สุขภาพจิตที่ ๖ เพื่อเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้ สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

๒.๓ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบ และอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ ถึงระดับใดได้บ้าง

๓. ให้ศูนย์สุขภาพจิตที่ ๖ จัดฝึกอบรมให้แก่ผู้ใช้งาน (User) เพื่อให้มีความรู้ ความเข้าใจและเกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง หรือจัดให้ผู้ใช้งาน (User) เข้าร่วมการฝึกอบรมที่หน่วยงานอื่นจัดขึ้น

๔. ให้ศูนย์สุขภาพจิตที่ ๖ กำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศตามความเหมาะสม ได้แก่ ยกเลิกการใช้งาน Internet กรณีที่มีการตรวจพบ Package จาก Users นั้น ๆ มากผิดปกติ หรือการแจ้งเตือนผู้ใช้งาน (User) เมื่อมีไวรัสแพร่ระบาด

๕. เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

หมวดที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)
๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์ และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล
๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้ สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน
๔. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้
   ๑.๑ ผู้ใช้งาน (User) ต้องกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย ๘ ตัว ขึ้นไป ซึ่งต้องประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) ประกอบด้วย ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวอักษรพิเศษ (Special character)
      - ตัวอักษร (a-z, A-Z
      - ตัวเลข (๐-๙)
      - เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
   ๑.๒ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ เดือน และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม
   ๑.๓ ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
   ๑.๔ ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

๑.๕ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑.๖ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๑.๗ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑.๘ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๑.๙ การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑.๑๐ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๒. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อก หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

๒.๑ คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๒.๒ การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

๒.๓ การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๒.๔ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๒.๕ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาไม่เกิน ๑๕ นาที

๓. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของศูนย์สุขภาพจิตที่ ๖ หรือเป็นข้อมูลของบุคคลภายนอก

๔. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๕. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของศูนย์สุขภาพจิตที่ ๖ และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๖. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๗. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตาม

เห็นสมควร ศูนย์สุขภาพจิตที่ ๖ จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่ศูนย์สุขภาพจิตที่ ๖ ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับศูนย์สุขภาพจิตที่ ๖ ซึ่งศูนย์สุขภาพจิตที่ ๖ อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๘. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่งที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์แรนท์ (Bit torrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

๙. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกม เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

๑๐. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของศูนย์สุขภาพจิตที่ ๖

๑๑. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของศูนย์สุขภาพจิตที่ ๖

๑๒. ห้ามใช้สินทรัพย์ของศูนย์สุขภาพจิตที่ ๖ เพื่อประโยชน์ทางการค้า

๑๓. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของศูนย์สุขภาพจิตที่ ๖ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๑๔. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๑๕. ห้ามใช้ระบบสารสนเทศของศูนย์สุขภาพจิตที่ ๖ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑๖. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๑๗. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของศูนย์สุขภาพจิตที่ ๖ โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

หมวดที่ ๔
การควบคุมการเข้าถึงเครือข่าย
(Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒. กำหนดแนวปฏิบัติการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายระบบคอมพิวเตอร์และระบบสารสนเทศของศูนย์สุขภาพจิตที่ ๖ ได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in Networks) โดยต้องแบ่งแยกเครือข่ายตามกลุ่มของการให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภทของเครือข่าย

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

๗. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน (User)

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าใช้งานระบบเครือข่ายภายนอก (Internet)

๑.๑.๒ ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ Youtube

หนังออนไลน์ หรือรายการบันเทิงต่าง ๆ ในเวลาราชการ

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย โดยทำการกรองเว็บไซต์ผ่าน Web Application Firewall ที่ฟังก์ชั่น Web Filter

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของศูนย์สุขภาพจิตที่ ๖ ผ่านระบบเครือข่ายภายนอก (Internet) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม โดยเคร่งครัด ได้แก่ ห้ามเผยแพร่ภาพหรือข้อมูลใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือที่มีลักษณะลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว ผ่านระบบเครือข่ายภายนอก (Internet) ห้ามเผยแพร่ภาพของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลด (Download) ไฟล์ข้อมูล หรือโปรแกรมต่าง ๆ จากระบบเครือข่ายภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุกโจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๑.๗ หลังจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้วให้ Logout ออกจากระบบ ปิดเว็บบราวเซอร์ (Web Browser) เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๒ การถ่ายโอนข้อมูลของศูนย์สุขภาพจิตที่ ๖ ที่รับส่งผ่านระบบเทคโนโลยีสารสนเทศโดยมีแนวปฏิบัติ ดังนี้

๑.๒.๑ จำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลลับ

๑.๒.๒ กำหนดผู้ใช้งานใดที่มีสิทธิหรือได้รับอนุญาตให้เข้าถึง

๑.๒.๓ ไม่อนุญาตการใช้งานข้อมูลสำคัญ หรือข้อมูลลับ ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๑.๒.๔ การรับ-ส่งข้อมูล หรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่างหน่วยงานภายในหรือภายนอกที่ได้รับอนุมัติเท่านั้น

๑.๒.๕ มีการนำเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ ผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing เป็นต้น

ข้อตกลงสำหรับการถ่ายโอนข้อมูลสารสนเทศ (Agreements on Information Transfer)

๑) กำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

๒) กำหนดข้อตกลง แนวทาง วิธีปฏิบัติ ระยะเวลา ของการถ่ายโอนสารสนเทศ

๓) มีการบันทึก วันเวลาที่มีการถ่ายโอนสารสนเทศ

๔) จำกัดการเข้าถึงสารสนเทศเมื่อมีการโอนย้ายเสร็จสิ้นแล้ว

โดยกรอกข้อมูลตามแบบขอรายงานผู้มารับบริการของศูนย์สุขภาพจิตที่ ๖ ยื่นศูนย์สุขภาพจิตที่ ๖ โดยมีรายละเอียด ดังนี้ วัน เดือน ปี ที่ขอข้อมูล, ชื่อ-สกุล (ผู้ขอรายงาน), ตำแหน่ง, หน่วยงาน/สังกัด, เบอร์โทรศัพท์, E-mail, จุดประสงค์ในการขอรายงาน, ช่วงเวลาของข้อมูล, รายละเอียดของรายงาน, ลงลายมือชื่อ-ตำแหน่ง หัวหน้าฝ่าย/หัวหน้างาน ผู้ขอข้อมูล

หมายเหตุ : กรณีที่เป็นข้อมูลส่วนบุคคลก่อนส่งข้อมูลจะมีการเข้ารหัสข้อมูล (Encryption) เพื่อปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกเปิดเผย

๒. การใช้งานไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ให้ดำเนินการ ดังนี้

๒.๑ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม โดยเคร่งครัด และห้ามใช้งานไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ในทางที่ไม่ถูกต้องผิดกฎหมาย ละเมิดศีลธรรม

๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้งานไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ที่ส่งโดยโดเมนเนม @dmh.mail.go.th

๒.๓ ต้องตรวจสอบชื่อผู้ส่งไปรษณีย์อิเล็กทรอนิกส์ (Sender) ก่อนเปิดไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มีนามสกุล .exe, .com, .bat และ .inf

๒.๔ หลังจากการใช้งานไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ต้องออกจากระบบ (Log Out) ทันทีเพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๓. การใช้งานเครือข่ายไร้สาย (Wi Fi) ให้ดำเนินการ ดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๓.๒ ผู้ใช้งาน (User) ต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (Wi Fi)

๓.๓ ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (Wi Fi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิของเครือข่ายไร้สาย (Wi Fi) เท่านั้น

๓.๔ ห้ามผู้ใช้งาน (User) ติดตั้งและเปิดการทำงานโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของศูนย์สุขภาพจิตที่ ๖ และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๔.๑ การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของศูนย์สุขภาพจิตที่ ๖ ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

๔.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับภารกิจงานของศูนย์สุขภาพจิตที่ ๖ ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสารที่เป็นประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้บังคับบัญชาก่อนทุกครั้ง

๔.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของศูนย์สุขภาพจิตที่ ๖ ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๔.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผลงดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๔.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากศูนย์สุขภาพจิตที่ ๖ และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๔.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

๕. การแบ่งแยกเครือข่าย (Segregation in Networks) แบ่งเป็น ๔ กลุ่ม ดังนี้

๕.๑ กลุ่มของการให้บริการสารสนเทศ ได้แก่ ระบบสารสนเทศเพื่อการสนับสนุนภารกิจหลักและระบบสารสนเทศเพื่อการสนับสนุนการปฏิบัติงาน

๕.๒ กลุ่มการใช้งาน ได้แก่ เจ้าของระบบ (System Owner) ผู้ดูแลระบบ (Administrator) และผู้ใช้งาน (User)

๕.๓ กลุ่มของอุปกรณ์สารสนเทศ ได้แก่ อุปกรณ์รักษาความมั่นคงปลอดภัยสารสนเทศและอุปกรณ์บริหารจัดการเครือข่าย

๕.๔ กลุ่มประเภทของเครือข่ายคอมพิวเตอร์ ได้แก่ ระบบเครือข่ายภายใน (Intranet) ระบบเครือข่ายภายนอก (Internet) และระบบเครือข่ายโซนพิเศษ (Demilitarized Zone : DMZ)

๖. มาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๖.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๖.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

๖.๓ ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้า-ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

๗. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอก แบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยดาวน์โหลดผ่านเว็บไซต์ศูนย์สุขภาพจิตที่ ๖ https://mhc6.dmh.go.th

๘. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

๙. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๑๐. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๑๐.๑ ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๑๐.๒ ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๑๐.๓ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๑๐.๔ ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๑๐.๕ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention system/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention system/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน

๑๐.๖ การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๑๐.๗ ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

๑๐.๘ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๐.๙ การระบุอุปกรณ์บนเครือข่าย

(๑) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการรายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

(๒) ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

(๓) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

(๔) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

(๕) การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๑๑. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๑๒. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

๑๓. กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๑๔. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์

๑๕. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบตามแนวทางปฏิบัติดังต่อไปนี้

๑๕.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน

๑๕.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๑๕.๓ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

๑๕.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๑๕.๕ การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๑๖. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวน การกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๑๗. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๑๘. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบ เครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งาน ในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑๙. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

หมวดที่ ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยต้องกำหนดให้ผู้ใช้งาน (User) มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน (User) ได้ และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการยืนยันว่าเป็นผู้ใช้งาน (User) ที่ได้รับอนุญาต

๓. กำหนดแนวปฏิบัติในการบริหารจัดการรหัสผ่าน (Password Management System) โดยต้องจัดทำระบบบริหารจัดการรหัสผ่าน (Password) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่าน (Password) ที่มีคุณภาพ

๔. กำหนดแนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

๕. กำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน (Session Time - Out)

๖. กำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time)

แนวปฏิบัติ

๑. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้

๓. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองเพื่อตรวจสอบความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบปฏิบัติการ (Operating System)

๔. ศูนย์สุขภาพจิตที่ ๖ ต้องจัดให้มีระบบการบริหารจัดการรหัสผ่าน (Password Management System) โดยผู้ใช้งาน (User) สามารถเปลี่ยนรหัสผ่าน (Password) ใหม่ หรือขอรหัสผ่าน (Password) ใหม่ได้ผ่านระบบ บริหารจัดการรหัสผ่าน (Password Management System) กำหนด

๕. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน
   ๕.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
   ๕.๒ หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที
๖. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
๗. ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง
๘. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
๙. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
๑๐. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน
๑๑. ซอฟต์แวร์ที่ศูนย์สุขภาพจิตที่ ๖ ใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
๑๒. ซอฟท์แวร์ที่ศูนย์สุขภาพจิตที่ ๖ จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
๑๓. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของศูนย์สุขภาพจิตที่ ๖ เพื่อประโยชน์ทางการค้า
๑๔. ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพ ไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์
๑๕. ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน
๑๖. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้
   ๑๖.๑ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใด ๆ บนระบบปฏิบัติการทั้งนี้ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อศูนย์สุขภาพจิตที่ ๖
   ๑๖.๒ การใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ ได้แก่ โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatter กำหนดให้ผู้ดูแลระบบ (Administrator) เท่านั้นที่มีสิทธิใช้งาน
๑๘. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศเมื่อเว้นว่างจากการใช้งาน (Session Time - Out) เมื่อครบ ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๑๙. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลาเชื่อมต่อ ระบบคอมพิวเตอร์ และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time) โดยให้

ใช้งานได้เป็นเวลา ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และในกรณีที่เชื่อมต่อจากภายนอกกำหนดให้ใช้งานได้ภายในวันและเวลาราชการ เว้นแต่กรณีที่มีเหตุผลความจำเป็นให้ขออนุญาตผู้อำนวยการศูนย์สุขภาพจิตที่ ๖

หมวดที่ ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ของผู้ใช้งาน (User) และฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน (Application and Information Access Control) ตามสิทธิ์ที่กำหนดไว้

๒. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อศูนย์สุขภาพจิตที่ ๖ โดยต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking)

๓. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติ และมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๔. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนดข้อปฏิบัติแผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิ์ตามตำแหน่ง และหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๑.๒ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภายนอกให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (VPN : Virtual Private Network) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

๑.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น

ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๑.๔ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่า เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๑.๕ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูล แต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลาย ข้อมูลแต่ละประเภทชั้นความลับดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑.๖ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(๑) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ

(๒) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(๓) มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

๑.๗ การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๑.๘ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) ผ่านระบบ

๑.๘.๑ ก่อนปฏิบัติงาน

(๑) ผู้รับจ้าง (Outsource) ต้องขออนุญาตผู้อำนวยการศูนย์สุขภาพจิตที่ ๖ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับผู้รับจ้างพร้อมแนบสำเนาสัญญาจ้างหรือเหตุผลในการปฏิบัติงาน

(๒) ผู้อำนวยการศูนย์สุขภาพจิตที่ ๖ หรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร

(๓) ผู้ดูแลระบบ (Administrator) ดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password) สำหรับเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ผู้ดูแลระบบ (Administrator) แจ้งให้ผู้รับจ้าง (Outsource) ได้รับทราบ

๑.๘.๒ ระหว่างปฏิบัติงาน

(๑) ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

(๒) เจ้าหน้าที่ศูนย์สุขภาพจิตที่ ๖ ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์สุขภาพจิตที่ ๖ ต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง (Outsource) ตลอดระยะเวลาการดำเนินการ

(๓) ผู้รับจ้าง (Outsource) ต้องปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมาย

เท่านั้น และต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งเจ้าหน้าที่ศูนย์สุขภาพจิตที่ ๖ ที่กำกับดูแลการปฏิบัติงานทันที

๑.๘.๓ หลังปฏิบัติงาน

(๑) ผู้รับจ้าง (Outsource) แจ้งความประสงค์ต่อผู้อำนวยการศูนย์สุขภาพจิตที่ ๖ หรือตัวแทนฝ่ายบริหาร ISMR เพื่อยกเลิกสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

(๒) ผู้ดูแลระบบ (Administrator) จะยกเลิกสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศและลบข้อมูลสารสนเทศของผู้รับจ้าง (Outsource) เป็นการถาวรเมื่อพ้นกำหนด ๙๐ วัน

๑.๘.๔ การรักษาความลับ

ผู้รับจ้าง (Outsource) ต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๘.๕ การปกปิดข้อมูล

ผู้ดูแลระบบจะกำหนดสิทธิการเข้าถึงข้อมูลโดยการระบุตัวตนเพื่อยืนยันก่อนการเข้าถึงข้อมูลทุกครั้ง กรณีที่มีการถ่ายโอนข้อมูลหรือส่งต่อข้อมูลไปยังหน่วยงานภายนอกจะทำสัญลักษณ์เพื่อปกปิดข้อมูลที่แท้จริง เช่น เบลอข้อมูลแทนค่าตัวอักษรตัวอื่นแทนข้อมูลเดิม เป็นต้น

หมวดที่ ๗
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สุขภาพจิตที่ ๖ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินและการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่อง แม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม และสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน
๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สุขภาพจิตที่ ๖ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
๓. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่องของศูนย์สุขภาพจิตที่ ๖ ด้านสารสนเทศ
๔. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผน
๕. บริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สุขภาพจิตที่ ๖ อย่างน้อยปีละ ๑ ครั้ง
๖. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติ

๑. ศูนย์สุขภาพจิตที่ ๖ ต้องจัดทำระบบสารสนเทศและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอน ดังนี้
   ๑.๑ ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศ
   ๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดรูปแบบการสำรองข้อมูลของระบบการสำรองข้อมูล (Backup System) ดังนี้
      ๑.๒.๑ รายชื่อระบบคอมพิวเตอร์และระบบสารสนเทศที่ได้รับการพิจารณาคัดเลือก ดังนี้
         (๑) ระบบคอมพิวเตอร์เครื่องลูกข่ายเสมือน (Virtual Desktop Infrastructure: VDI)
         (๒) ระบบติดตามการดำเนินการของโครงการ (Tracking System)
         (๓) ระบบไปรษณีย์อิเล็กทรอนิกส์ (E-Mail)
         (๔) ระบบสำนักงานอัตโนมัติ (E-Office)

(๕) ระบบสารบรรณอิเล็กทรอนิกส์ (E-Saraban)

(๖) ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ – รัฐวิสาหกิจ (GFMIS - SOE)

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลเฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน

๑.๒.๓ กำหนดรูปแบบการสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ทั้งนี้ เนื่องจากศูนย์สุขภาพจิตที่ ๖ ได้ดำเนินการสำรองข้อมูลระบบคอมพิวเตอร์ และระบบสารสนเทศแบบสมบูรณ์ (Full Backup) ทุกระบบงานจึงได้รับการสำรองข้อมูลด้วย

๑.๓ ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรือ External Disk และอื่น ๆ ที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

๑.๔ ผู้ดูแลระบบ (Administrator) ต้องกำหนดรูปแบบการกู้คืนข้อมูลของระบบการสำรองข้อมูล (Backup System) โดยมีความถี่และรูปแบบ ดังนี้

๑.๔.๑ การกู้คืนข้อมูลรายวันจากอุปกรณ์ที่ใช้ในการสำรองข้อมูล เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือที่สำรองข้อมูลเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup)

๑.๔.๒ การกู้คืนข้อมูลรายสัปดาห์หรือรายเดือนจากอุปกรณ์ที่ใช้ในการสำรองข้อมูลแบบสมบูรณ์ (Full Backup)

๒. ศูนย์สุขภาพจิตที่ ๖ ดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สุขภาพจิตที่ ๖ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

๒.๑ กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ

๒.๒ กำหนดผู้มีหน้าที่รับผิดชอบระบบสำรองข้อมูลสารสนเทศ

๒.๓ กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว

๒.๔ กำหนดให้ปรับปรุงแผนดังกล่าวทุก ๒ ปี

๓. ศูนย์สุขภาพจิตที่ ๖ ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้อย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และแผนการสำรองข้อมูลศูนย์สุขภาพจิตที่ ๖ รวมถึงการทดสอบสภาพความพร้อมใช้งาน ได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของศูนย์สุขภาพจิตที่ ๖ รายละเอียดปรากฏตามเอกสารภาคผนวก

หมวดที่ ๘
การเข้ารหัสข้อมูล
(Cryptographic)

วัตถุประสงค์

เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลง แก้ไขข้อมูลที่เป็นความลับ หรือมีความสำคัญ

นโยบาย

๑. กำหนดนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูลที่คำนึงถึงชนิด และวิธีการเข้ารหัสข้อมูลที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับ หรือมีความสำคัญ

๒. ใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

๓. กำหนดผู้รับผิดชอบในการดำเนินนโยบาย และการบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (Key Management)

๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดย ให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับหรือข้อมูลที่สำคัญยิ่งยวด

๕. บริหารจัดการกุญแจ (Key Management) เพื่อการเข้ารหัสข้อมูลตลอดช่วงเวลาการใช้งาน (Key Management Whole Life Cycle)

แนวปฏิบัติ

๑. ผู้ดูแลระบบต้องกำหนดรูปแบบ Wireless Security ให้เป็น WPA/WPA2 (Wifi Protected Access) ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจาย สัญญาณแบบไร้สาย (Access Point)

๒. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๓. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่สำนักบริการคอมพิวเตอร์กำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิด

๔. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายคอมพิวเตอร์สาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML encryption เป็นต้น

๕. การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ ผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing

๖. การบริหารจัดการกุญแจ (Key Management) ทำการคัดเลือกวิธีการเข้ารหัสการกำหนด

ความยาวของรหัส การใช้งาน และการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบาย และแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ เช่น มาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

หมวดที่ ๙
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

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

แนวปฏิบัติ

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

ภาคผนวก

แนวปฏิบัติ เมื่อเกิดฟิชชิ่ง (Phishing) ที่เว็บเซิร์ฟเวอร์ของหน่วยงาน

วัตถุประสงค์

เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชชิ่ง (Phishing) ให้สามารถดำเนินการได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหาย และส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

แนวปฏิบัติ

๑. เมื่อผู้ดูแลระบบเครือข่ายของศูนย์สุขภาพจิตที่ ๖ ได้รับแจ้งหรือตรวจพบว่าเว็บเซิร์ฟเวอร์ของหน่วยงานเป็นช่องทางให้ผู้ไม่หวังดีทำฟิชชิ่ง (Phishing) ผู้ดูแลระบบของศูนย์สุขภาพจิตที่ ๖ จะดำเนินการ ดังนี้

(๑) ดำเนินการบล็อค IP Address ของเว็บเซิร์ฟเวอร์ที่โดนฟิชชิ่งนั้น หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานดำเนินการโดยเร่งด่วน

(๒) แจ้งผู้ดูแลเว็บเซอร์เวอร์ของหน่วยงานที่ถูกทำฟิชชิ่ง ทาง e-Mail หรือทางโทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

๒. เมื่อหน่วยงานดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ทำการปลด บล็อค IP Address

๓. ผู้ดูแลเว็บเซิร์ฟเวอร์ของหน่วยงานต้องตรวจสอบเว็บเซิร์ฟเวอร์และเว็บไซต์ภายในหน่วยงานรวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) อย่างสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทำฟิชชิ่ง

หมายเหตุ : ทางผู้เสียหายส่วนใหญ่ เป็นหน่วยงานที่มีการทำธุรกรรมอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการเงิน เช่น ธนาคาร เว็บไซต์ที่เกี่ยวกับการซื้อขายออนไลน์ ฯลฯ หากการดำเนินการแก้ไขปัญหาดังกล่าวล่าช้าและมีความเสียหาย อาจมีผลทางกฎหมายต่อหน่วยงาน

แนวปฏิบัติ เมื่อเกิดภัยคุกคามทางไซเบอร์เกี่ยวกับมัลแวร์เรียกค่าไถ่ (ransomware)

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการดำเนินการเพื่อรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์เกี่ยวกับมัลแวร์เรียกค่าไถ่ (ransomware) ได้อย่างทันท่วงที

แนวปฏิบัติ

๑. IDENTIFY คอมพิวเตอร์ทุกเครื่อง โดยแยกเป็นกลุ่มตามระดับผลกระทบหากถูกโจมตีจากมัลแวร์ (ระบุผู้รับผิดชอบเครื่องแต่ละเครื่อง เช่น หน่วยงาน, ส่วนกลาง, ข้อมูลติดต่อ Vendor)

<u>กลุ่มตามผลกระทบ</u>

A+ : สำคัญต่อชีวิตคนไข้ และ Operation ที่มีการต่อเชื่อมกับระบบเครือข่าย
A : ระบบที่เกี่ยวข้องกับการเก็บข้อมูลผู้ป่วย ที่มีการต่อเชื่อมกับระบบเครือข่าย
B : ระบบที่เชื่อมต่อกับ HIS ของโรงพยาบาล ที่มีการต่อเชื่อมกับระบบเครือข่าย
C : ระบบที่ไม่ได้ต่อเชื่อมกับ HIS ของโรงพยาบาล ที่มีการต่อเชื่อมกับระบบเครือข่าย เช่น ระบบสำนักงาน (Back Office)
D : ไม่มีการต่อเชื่อมกับระบบเครือข่าย (Stand Alone)

<u>ประเภทบริการ</u>

M : Medical Equipment’s
L : Laboratory Equipment’s
U : Utility Equipment’s (ไฟฟ้า เครื่องปรับอากาศ ลิฟต์ CCTV)
P : Personal Computer (PC) ทั่วไป
M : Mobile Device

๒. วางแผนการจัดการ การตรวจสอบเครื่องแต่ละกลุ่ม และดำเนินการป้องกัน

๓. Backup ข้อมูลที่สำคัญออกจากเครื่อง ไว้ใน External Hard disk อย่างน้อย ๓ แหล่ง (ที่ไม่ต่อเชื่อมกับระบบเครือข่าย เพื่อป้องกันการถูกเข้ารหัสไฟล์ข้อมูล)

๔. สื่อสาร ให้ความรู้เกี่ยวกับการป้องกัน/การลดความเสี่ยงแก่ผู้ใช้งาน (Users) มิให้เป็นพาหะนำมัลแวร์เข้าสู่เครือข่าย เช่น ไม่เปิดอีเมลที่ไม่รู้จัก ไม่คลิกเปิดหรือ Download ไฟล์แนบที่ไม่ระบุแหล่งที่มาที่รู้จัก รวมถึงไฟล์น่าสงสัยอื่น ๆ

๕. จัดทีมเพื่อดำเนินการป้องกัน (ติดตั้ง/Update Patch OS) และสื่อสารให้ความรู้กับผู้ใช้ และให้มีผู้จัดการกำกับ และติดตามสถานะอย่างใกล้ชิด

๖. ผู้ดูแลระบบ

๑.) ระบบให้บริการผู้ป่วยหรือระบบเครือข่ายของหน่วยงานต้องมีการติดตั้งระบบป้องกันเครือข่าย (Firewall)

๒.) ระบบพิสูจน์ตัวตน อย่างน้อยต้องมีการพิสูจน์ตัวตน (Authentication) ในการใช้งานระบบบริการหรือระบบเครือข่ายของหน่วยงาน และมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตาม พรบ. คอมพิวเตอร์ (Log file) อย่างเหมาะสม

๓.) จัดตารางระบบสำรองข้อมูล เช่น ฐานข้อมูล โปรแกรมที่มีความจำเป็นเพื่อเป็นการ

ป้องกันข้อมูลสูญหาย และสามารถนำกลับมาใช้ได้โดยไม่เกิดผลกระทบกับระบบที่ต้องการใช้งาน

๔.) จัดทำแผนการทดสอบและการกู้คืนข้อมูลที่สำคัญหลังจากสำรองข้อมูลไปแล้ว

๕.) จัดให้มีเครื่องแม่ข่ายสำรองสำหรับระบบที่จำเป็นใช้งาน เช่น ระบบให้บริการผู้ป่วย เว็บไซต์ หลังจากระบบหลักมีปัญหาสามารถใช้งานได้โดยไม่เกิดผลกระทบกับการบริการหรือเปิดผลกระทบน้อยที่สุด

๖.) หลังจากทำการสำรองข้อมูลแล้วให้ตัดการเชื่อมต่อกับระบบเพื่อป้องกันการโดนโจมตี

๗. ผู้ใช้งานระบบ

๑.) ผู้ใช้งานระบบต้องไม่ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาตจากผู้ดูและระบบ

๒.) ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มาที่ชัดเจน

๓.) ไม่ใช้งานเว็บไซต์ที่มีความเสี่ยง

ข้อแนะนำ : ในการใช้งานระบบเครือข่ายภายนอกในกรณีที่ไม่สามารถแยกกลุ่มของเครือข่ายได้ VLAN (Virtual Area Network) แนะนำให้ใช้อินเทอร์เน็ตบ้าน (Fiber to home) เพื่อใช้งานระบบเครือข่ายภายนอก

แนวปฏิบัติการนำเข้าข้อมูลสารสนเทศ (Import Data)

วัตถุประสงค์

เพื่อควบคุมการนำเข้าข้อมูลสารสนเทศ (Import Data) ให้เป็นไปตามข้อกำหนดของศูนย์สุขภาพจิตที่ ๖ และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

๑. กำหนดให้มีผู้รับผิดชอบในการกำหนดสิทธิการใช้งาน
๒. กำหนดให้มีกระบวนการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุม โดยให้มีการควบคุม จำกัดและเปลี่ยนแปลงสิทธิการนำเข้าข้อมูลสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ
๓. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัย และผลกระทบที่เกิดจากการนำเข้าสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์
๔. กำหนดให้มีมาตรการในการป้องกันตามกฎหมายที่เกี่ยวข้อง

แนวปฏิบัติ

๑. การขออนุญาตการนำเข้าสารสนเทศ ให้ดำเนินการ ดังนี้
   ๑.๑ การนำเข้าข้อมูลผู้ป่วยด้านสุขภาพจิต และจิตเวช
      ๑.๑.๑ ให้ศูนย์สุขภาพจิตที่ ๖ ทำหนังสือแต่งตั้งผู้รับผิดชอบในการนำเข้าข้อมูลลงนามโดยผู้มีอำนาจภายในหน่วยงาน เพื่อพิจารณาอนุมัติ และดำเนินการสอดคล้องกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
      ๑.๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งาน และเวลาในการเข้าถึงระบบฯ ตามสิทธิที่ร้องขอพร้อมทั้งกำหนดให้มีการจัดเก็บข้อมูลการเข้าใช้งาน (log files)
      ๑.๑.๓ แจ้งช่องทางการเข้าถึงและระเบียบการใช้งานให้ผู้ขอใช้งานรับทราบ
      ๑.๑.๔ เมื่อครบกำหนดตามระยะเวลาการร้องขอ ผู้ดูแลระบบจะต้องยกเลิกสิทธิการเข้าถึงระบบฯ
   ๑.๒ กรณีบุคคลภายนอก
      ๑.๒.๑ ให้ศูนย์สุขภาพจิตที่ ๖ ทำหนังสือแจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ลงนามโดยผู้มีอำนาจภายในหน่วยงานเพื่อพิจารณาอนุมัติ และดำเนินการสอดคล้องกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
      ๑.๒.๒ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งานและเวลาในการเข้าถึงระบบฯ ตามสิทธิที่ร้องขอพร้อมทั้งกำหนดให้มีการจัดเก็บข้อมูลการเข้าใช้งาน (log files)
      ๑.๒.๓ แจ้งช่องทางการเข้าถึงและระเบียบการใช้งานให้ผู้ขอใช้งานรับทราบ

๑.๒.๔ เมื่อครบกำหนดตามระยะเวลาการร้องขอ ผู้ดูแลระบบจะต้องยกเลิกสิทธิการเข้าถึงระบบฯ

แนวปฏิบัติการพัฒนา Website ศูนย์สุขภาพจิตที่ ๖

วัตถุประสงค์

เพื่อควบคุมการดำเนินการพัฒนา Website ของศูนย์สุขภาพจิตที่ ๖ เพื่อให้เกิดมาตรฐานความมั่นคงปลอดภัยในการพัฒนา Website ของหน่วยงาน

นโยบาย

๑. กำหนดให้มีผู้รับผิดชอบในการกำหนดสิทธิการใช้งาน
๒. กำหนดให้มีกระบวนการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุม โดยให้มีการควบคุม จำกัดและเปลี่ยนแปลงสิทธิการนำเข้าข้อมูลสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ เพื่อควบคุมการเข้ารหัสที่ปลอดภัยสำหรับการพัฒนาซอฟต์แวร์
๓. กำหนดให้ศูนย์สุขภาพจิตที่ ๖ ที่มีการให้บริการ Website มีมาตรฐานการให้บริการตามระเบียบของกระทรวงสาธารณสุข
๔. การพัฒนา Website ของศูนย์สุขภาพจิตที่ ๖ มีมาตรฐานสอดคล้องกับมาตรฐานเว็บไซต์ภาครัฐ, มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่
๕. ศูนย์สุขภาพจิตที่ ๖ มีอัตลักษณ์ในการให้บริการ Domain เดียวกันภายใต้กรมสุขภาพจิต
๖. ศูนย์สุขภาพจิตที่ ๖ พัฒนา Website ตรงตามกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑. Website ของหน่วยงาน ต้องใช้ Domain ของหน่วยงาน หรือ Domain ของกรมสุขภาพจิต กระทรวงสาธารณสุขเท่านั้น
๒. การพัฒนา Website ให้ปฏิบัติตามนโยบายการพัฒนามาตรฐานเว็บไซต์ภาครัฐ มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่ เวอร์ชันปัจจุบัน
๓. Website ที่ให้บริการแก่เจ้าหน้าที่และบุคคลภายนอก ให้ดำเนินการติดตั้งใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์ (SSL Certificate : https://) จากผู้ให้บริการที่ได้รับการรับรอง/น่าเชื่อถือ
๔. จัดให้มีระบบป้องกันการบุกรุกและโปรแกรมป้องกันไวรัส
๕. โปรแกรมที่ใช้งานต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย