แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

ตามประกาศกรมสุขภาพจิตเรื่องนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมสุขภาพจิต กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เพื่อให้ระบบ เทคโนโลยีสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถ ดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะ ที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้นั้น

สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เรื่อง แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ พ.ศ. 2566”

ข้อ 2 ประกาศนี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 คำนิยาม

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายถึง ผู้มีอำนาจใน ด้านเทคโนโลยีสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ซึ่งมีบทบาทหน้าที่และความรับผิดชอบใน ส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ศูนย์สารสนเทศ หมายถึง งานคอมพิวเตอร์และสารสนเทศซึ่งเป็นหน่วยงานที่ให้บริการด้าน เทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่าย ภายในสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

ผู้อำนวยการศูนย์สารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยี สารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ และมีอำนาจตัดสินใจเกี่ยวกับระบบ สารสนเทศ ภายในสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยี สารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ(Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้ สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือ ดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่ง สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้กำหนดไว้ดังนี้

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เช่น ผู้อำนวยการสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ รองผู้อำนวยการสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เป็นต้น

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้า ที่ที่ได้รับมอบหมายจาก ผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถ เข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้เช่น บัญชีผู้ใช้ระบบ คอมพิวเตอร์(User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

เจ้าหน้าที่ หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานกระทรวงสาธารณสุข เป็นต้น ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้อนุญาต ให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบ คอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัด ระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถ เข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้า ด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุด อุปกรณ์ทำ หน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่ง ข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่ เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการ ติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่าย คอมพิวเตอร์ต่างๆของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของ หน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้าง สารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารการสนับสนุนการให้ บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบเช่น ระบบคอมพิวเตอร์ระบบ เครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศโดยแบ่งเป็น พื้นที่ ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และ คอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน พื้นที่ทำงานของผู้ดูแลระบบ

(System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญ หาย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบ เทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบ อำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทาง กายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความ ถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้รวมถึง คุณสมบัติในด้าน ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การ ห้าม ปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึงกรณีที่ระบุการเกิด เหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบาย ด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจ เกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตรีและความมั่นคง ปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์(Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่าน เครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพ กราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP,POP3 และIMAPเป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการ ตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคง ปลอดภัยของ ข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือ ชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ ตรงตามคำสั่งที่กำหนดไว้

Remote Access หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ (ผ่านช่องทางการสื่อสารภายในโรงพยาบาล) หรือ จากภายนอกสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ (ผ่าน Internet

VDO Teleconference หมายถึง การประชุมทางไกล โดยการนำเทคโนโลยีสาขาต่างๆ เช่น คอมพิวเตอร์ เครื่องถ่ายโทรทัศน์ และเครือข่ายอินเตอร์เน็ต เพื่อสนับสนุนในการประชุมให้มี ประสิทธิภาพ ถูกออกแบบมาเพื่อให้คนหรือกลุ่ม คน ซึ่งอยู่กันคนละสถานที่สามารถติดต่อกันได้ทั้ง ภาพและเสียง โดยผ่านทางจอภาพซึ่งอาจเป็นคอมพิวเตอร์หรือโทรทัศน์ ผู้ชมที่ฝั่งหนึ่งจะเห็นภาพของ อีกฝั่งหนึ่งปรากฏอยู่บนจอโทรทัศน์

ข้อ 4 สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแนวปฏิบัติ ในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรพร้อมทั้งได้กำหนดให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบ กำกับดูแล ติดตามให้ผู้ใช้งาน (User) ปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวไว้อย่างชัดเจนดังนี้

4.1 การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุม การเข้าถึงสารสนเทศ (Business Requirements for Access Control)

4.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

4.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

4.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

4.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

4.6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

4.7 การจัดทำระบบสำรองสำหรับระบบสารสนเทศ (Data Recovery)

4.8 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk Assessment and Risk Management) โดยมีรายละเอียดปรากฏตามเอกสารแนบท้ายประกาศนี้

ข้อ 5 สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ได้ประกาศนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศทางเว็บไซต์หลัก สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ และหนังสือเวียนภายในระบบสารบรรณอิเล็กทรอนิกส์ให้ผู้ใชงาน เจ้าหน้าที่ และบุคคลภายนอกทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามได้อย่างถูกต้อง

ข้อ 6 หน่วยงานในสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ที่ต้องบริหารระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง แต่ต้องสอดคล้องกับ “ประกาศสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้เรื่องแนวนโยบาย และการปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้”

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หมวดที่ 1

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

วัตถุประสงค์

1. เพื่อกำหนดการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัยด้านสารสนเทศ
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิและการมอบอำนาจของหน่วยงานของรัฐ
3. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความ สำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
4. เพื่อให้การตรวจสอบและติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

นโยบาย

บุคลากรสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อ ควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

1. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น
2. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้อง ขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน
3. ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์ระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น
4. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และ หน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึง อย่างสม่ำเสมอ ดังนี้

    4.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

        4.1.1 กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น – อ่านอย่างเดียว - สร่างข้อมูล - ป้อนข้อมูล - แก้ไข - อนุมัติ - ไม่มีสิทธิ์

        4.1.2 กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

        4.1.3 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์ อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

    4.2 การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางตาม ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด

รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความ ปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

4.2.1 จัดแบ่งประเภทของข้อมูลออกเป็น

– ข้อมูลสารสนเทศด้านการบริหารเช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

– ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่นข้อมูลผู้ป่วยข้อมูลทางทางแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

4.2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด - ข้อมูลที่มีระดับความสำคัญปานกลาง

– ข้อมูลที่มีระดับความสำคัญน้อย

4.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะ ก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

- ข้อมูลลับ หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด ความเสียหายแก่ประโยชน์แห่งรัฐ

- ข้อมูลใช้งานภายในองค์กร หมายถึง ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้ นำไปใช้งานภายนอกองค์กร

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัย ข้อมูลที่ เผยแพร่สู่สาธารณะ ผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณาอนุมัติ หากข้อมูลสูญหาย หรือถูกเปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร

4.2.4 จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

4.2.5 รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ซึ่งมี รูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT Format, Document Format, PDF Format (Portable Document Format)

- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ มี รูปแบบที่ใช้ เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

5. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

6. เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ระบบสารสนเทศและอุปกรณ์ในการประมวลผล ข้อมูล (Process Device) ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าวต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากสำนักเทคโนโลยีสารสนเทศและต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายบุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

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

7.1 สำนักเทคโนโลยีสารสนเทศต้องกำหนดหลักเกณฑ์สำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center)

7.2 การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจาก สำนักเทคโนโลยีสารสนเทศก่อนเริ่มดำเนินการทุกครั้ง

7.3 ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ

7.4 ผู้ใช้งาน (User) หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา และต้อง ไม่นำอาหาร หรือเครื่องดื่มเข้าไปในห้องศูนย์ข้อมูล (Data Center) และห้ามสูบบุหรี่ในห้องศูนย์ข้อมูล (Data Center)

8. ผู้ดูแลระบบต้องจัดใหมีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไข เปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

9. ผู้ดูแลระบบต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ตารางการแบ่งระดับชั้นของข้อมูล (Information Classification)

ระดับชั้น ความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
ประเภท ข้อมูล	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะ ก่อให้เกิดความเสียหายแก่ประโยชน์ แห่งรัฐอย่างร้ายแรง ที่สุด **สิทธิส่วนบุคคล** ละเมิดสิทธิส่วน	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง **สิทธิส่วนบุคคล** ละเมิดสิทธิส่วน	ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผย ทั้งหมดหรือเพียง บางส่วนจะก่อให้เกิดความเสียหายแก่ ประโยชน์แห่งรัฐ **สิทธิส่วนบุคคล** ละเมิดสิทธิส่วนบุคคล แต่ไม่ทำให้	• ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกองค์กร • หากข้อมูลสูญหาย หรือ ถูกเปิดเผยโดยไม่ได้รับ อนุญาตจะส่งผลเสียหาย ต่อองค์กรในระดับต่ำหรือ อาจจะ	• ข้อมูลที่ไม่จำเป็นต้องได้รับ การคุ้มครองความมั่นคงปลอดภัย ข้อมูลที่เผยแพร่สู่ สาธารณะผ่านช่องทางที่เหมาะสมซึ่งองค์กรพิจารณา อนุมัติ หากข้อมูลสูญหาย หรือถูก

ระดับชั้น ความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
	บุคคลทำให้เสียชื่อเสียงและทรัพย์สินอย่างร้ายแรง หากข้อมูลสูญหาย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อองค์กรในระดับสูงมาก	บุคคลทำให้เสียชื่อเสียงและทรัพย์สิน	เสียชื่อเสียงและทรัพย์สิน	ไม่มีผลกระทบใดๆ	เปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร
ตัวอย่าง เอกสาร	คำสั่งพิเศษที่ห้ามเปิดเผยข้อมูล	ข้อมูลใดๆ ที่เจ้าหน้าที่พิจารณาแล้วกำหนดให้เป็นชั้นความลับมาก	ขอมูลความลับทางราชการ ผลประเมินความเสี่ยง, แผนการซ่อม BCP, รายงานการซ่อม BCP Infrastructure Diagram, Key License, Asset Inventory List, สัญญาว่าจ้าง NDA, บันทึกต่างๆ ที่มีข้อมูลส่วนตัวของพนักงาน เป็นต้น	ข้อมูลคำรับรอง ข้อมูลบุคลากร, คู่มือการปฏิบัติงาน, IT Policy, Procedure, แบบฟอร์ม เป็นต้น	หลักเกณฑ์ต้องสื่อสารให้ ได้ข้อมูลนโยบาย ระบบ ความมั่นคงปลอดภัย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคลที่เจ้าของข้อมูล ให้เผยแพร่ได้ถ้ามี รายงาน วิชาการ หลักฐานทางวิทยาศาสตร์ งานวิจัยที่มี การตีพิมพ์, ข้อมูลงบประมาณการเงินบัญชี Supplier, ประกาศต่างๆ ที่ต้องการสื่อสาร, ข้อมูลใน Web Site เป็นต้น
การเคลื่อนย้ายเอกสารภายนอกองค์กร	แสดงเครื่องหมายอักษรตัวโต สีแดง หรือ สีที่เห็นได้ชัด ที่กระดาษด้านบนและล่างของทุกหน้า รวมด้านนอกหน้าปกหน้า และหลังเอกสารที่เป็น ม้วน	แสดงเครื่องหมายอักษรตัวโต สีแดง หรือ สีที่เห็นได้ชัด ที่กระดาษด้านบนและล่างของทุกหน้า รวมด้านนอกหน้าปกหน้า และหลังเอกสารที่เป็น ม้วน	แสดงเครื่องหมายอักษร ตัวโต สีแดง หรือสีที่เห็น ได้ชัด ที่กระดาษด้านบน และล่างของทุกหน้า รวมด้านนอกหน้าปก หน้าและหลัง เอกสารที่เป็นม้วนหรือพับให้	สอดซองปิดผนึก และระบุ ชื่อ-ที่อยู่ของผู้รับ และ ระบุใชงานภายในองค์กร เท่านั้น	ไม่มีข้อจำกัด

ระดับชั้น ความลับ	ข้อมูลลับที่สุด (Top Secret)	ข้อมูลลับมาก (Secret)	ข้อมูลลับ (Confidential)	ข้อมูลใช้งานภายในองค์กร (Internal Use Only)	ข้อมูลทั่วไป (Public)
	หรือพับให้แสดงที่ม้วนหรือพับอยู่ แถวบันทึกที่อยู่ในกล่องหรือภาชนะ ต้องแสดง **ชั้นความลับที่สุด** ที่ กล่องหรือภาชนะบรรจุ ซองหรือภาชนะทึบ แสง 2ชั้นระบุชื่อตำแหน่งผู้รับ, หน่วยงานที่ส่ง,ระบุเครื่องหมายแสดงชั้น ความลับด้านหลังและด้านหลังของซองหรือ ภาชนะและปิดผนึก ด้วยเทปกาวหรือวัสดุ ที่สามารถป้องกันการ ลักลอบเปิดอ่านได้	หรือพับให้แสดงที่ม้วนหรือพับอยู่แถวบันทึกที่อยู่ในกล่องหรือภาชนะ ต้องแสดง **ชั้นความลับมาก** ที่ กล่องหรือภาชนะ บรรจุซองหรือภาชนะ ทึบแสง 2ชั้นระบุชื่อตำแหน่งผู้รับ, หน่วยงานที่ส่ง,ระบุเครื่องหมายแสดงชั้น ความลับด้านหลังและด้านหลังของซองหรือ ภาชนะและปิดผนึก ด้วยเทปกาวหรือวัสดุ ที่สามารถป้องกันการ ลักลอบเปิดอ่านได้	แสดงที่ม้วนหรือพับอยู่แถวบันทึกที่อยู่ในกล่อง หรือภาชนะต้องแสดง **ชั้นความลับ** ที่ กล่อง หรือภาชนะบรรจุซอง หรือภาชนะทึบแสง2ชั้น ระบุชื่อตำแหน่งผู้รับ, หน่วยงานที่ส่ง,ระบุเครื่องหมายแสดงชั้นความลับด้านหลังและด้านหลังของซองหรือภาชนะและปิดผนึกด้วย เทปกาว หรือวัสดุที่ สามารถป้องกันการ ลักลอบเปิดอ่านได้		
วิธีการดูแล รักษาข้อมูล	จัดเก็บในแผนกที่เกี่ยวข้องเท่านั้นและมี การเข้ารหัสข้อมูล ทั้งหมดในระหว่างที่ จัดเก็บ	จัดเก็บในแผนกที่เกี่ยวข้องเท่านั้นและมี การเข้ารหัสข้อมูล ทั้งหมดในระหว่างที่ จัดเก็บ	จัดเก็บในแผนกที่เกี่ยวข้องเท่านั้น และมี การเข้ารหัสข้อมูลทั้งหมดในระหว่างที่จัดเก็บ	เก็บใน Folder ของแต่ละแผนก	แผนกที่ทำ การจัดเก็บ
การส่งต่อ ข้อมูล	มีการเข้ากำหนดรหัส เข้าไฟล์ข้อมูล	มีการเข้ากำหนดรหัส เข้าไฟล์ข้อมูล	มีการเข้ากำหนดรหัสเข้าไฟล์ข้อมูล	ส่งทางอีเมล์หรือส่งมาใน Share Drive เท่านั้น	ส่งทางอีเมล์ ทำเป็นประกาศขึ้น เวปไซต์ทาง ไลน์
การทำลายเอกสาร	เผาทำลาย	เผาทำลาย	เผาทำลาย	ใช้เครื่องทำลายเอกสาร	ไม่มีข้อจำกัด
การเข้าถึง ข้อมูล	ผู้บริหาร, ผู้อำนวยการ	ผู้บริหาร, ผู้อำนวยการ	ผู้บริหาร,ผู้อำนวยการ, หัวหน้ากลุ่มงาน, DC	ผู้ดูแลระบบ หรือผู้ที่ได้รับ มอบหมาย	ผู้ใช้งาน ทั่วไป

10. การจัดการสื่อบันทึกข้อมูล (Media Handing)

10.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยก/เคลื่อนย้ายได้ (Management of Removable Media) กรณีที่ไม้มีความจำเป็นต้องใช้ข้อมูล ต้องจัดให้มีกระบวนการทำลายข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล และไม่ให้สามารถกู้คืนข้อมูลได้

10.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

10.2.1 ผู้ดูแลระบบ/ผู้ใช้งานต้องทำลายข้อมูลที่เป็นความลับ ที่บันทึกในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบ หรือเขียนข้อมูลที่มี ความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้ งานต่อ เพื่อป้องกันการรั่วไหลของข้อมูล หรือป้องกันไม่ให้ข้อมูลสำคัญนั้นได้ และ พิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้เครื่องหั่นแผ่น CD/DVD หรือกรรไกรตัดทำลาย
ฮาร์ดดิสก์	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ – ใช้วิธีการทุบหรือบดให้เสียหาย

10.2.2 กรณีที่จัดเก็บเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูล อาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้ใหม่

10.3 การขนย้ายสื่อบันทึก (Physical Media Transfer)

10.3.1 ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทำการจะต้องดูแลรักษาความปลอดภัย จากการถูกเข้าถึงโดยไม้ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือทำให้เสียหายระหว่างการขนย้าย

10.3.2 ผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึกที่มีข้อมูลออกจากพื้นที่ทาการ ต้องชดใช้ค่าเสียหาย ไม่ว่าทรัพย์สินนั้นจะชำรุด หรือ สูญหายตามมูลค่าของทรัพย์สิน หากความเสียหาย นั้นเกิดจากความประมาทเลินเล่อของผู้ที่มีหน้าที่ได้รับมอบหมายให้เคลื่อนย้ายสื่อบันทึก

หมวดที่ 2
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน (User) ที่ได้รับอนุญาตแลว และ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ และ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

2. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานแล้ว

3. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัดและเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับ มอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ

4. กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุมโดยเริ่มตั้งแต่ กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ได้รับของผู้ใช้งาน (User) การส่ง มอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการ กำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

5. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

6. กำหนดให้มีการสรางความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

7. กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติ

1. การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

1.1 กรณีบุคลากรสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

1.1.1 บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้สำนักเทคโนโลยีสารสนเทศเพื่อสร้างบัญชีผู้ใช้งาน (Username) และ กำหนดรหัสผ่านการใช้งาน

1.1.2 ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งานระบบฯ ให้บุคลากรใหม่ ตามสิทธิพร้อมทั้งแจ้งให้บุคลากรใหม่ได้รับทราบ

1.2 กรณีบุคคลภายนอก

1.2.1 ให้สำนัก/กอง/ศูนย์/กลุ่ม แจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบ คอมพิวเตอร์และระบบสารสนเทศโดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก

1.2.2 ให้สำนักเทคโนโลยีสารสนเทศพิจารณาเหตุผลดังกล่าวก่อนดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านในการใช้งาน วันหมดอายุ ส่งต่อให้สำนัก/กอง/ศูนย์/กลุ่ม เพื่อแจ้งให้บุคคลภายนอกได้รับทราบ

1.3 การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

1.3.1 การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานเพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

1.3.2 การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย 8 ตัวขึ้นไป ซึ่งต้องประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) ประกอบด้วยตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวอักษรพิเศษ (Special character)

– ตัวอักษร (a-z, A-Z)

– ตัวเลข (0-9)

– เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือในการ ตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

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

1.3.4 เมื่อบุคลากรมีการเปลี่ยนชื่อหรือนามสกุลให้แจ้งสำนักเทคโนโลยีสารสนเทศเพื่อเปลี่ยนแปลงข้อมูลส่วนบุคคลให้ถูกต้อง

1.4 การยกเลิกสิทธิการใช้งานของบุคลากร สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ หรือบุคคลภายนอกให้ดำเนินการ ดังนี้

1.4.1 กรณีบุคลากรสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

1.4.1.1 ให้สำนัก/กอง/ศูนย์/กลุ่ม แจ้งสำนักเทคโนโลยีสารสนเทศ เพื่อขอยกเลิกสิทธิใน การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง

1.4.1.2 สำนักเทคโนโลยีสารสนเทศจะปิดบัญชีผู้ใช้งาน (Username) ชั่วคราวเป็นเวลา 90 วัน หากบุคลากรที่มีความประสงค์จะใช้ข้อมูลในบัญชีผู้ใช้งาน (Username) ดังกล่าว ให้แจ้งความประสงค์พร้อมเหตุผลต่อสำนักเทคโนโลยีสารสนเทศ เพื่อขอเปิดใช้งานบัญชีผู้ใช้งาน (Username) ทั้งนี้เมื่อครบกำหนด 90 วันนับจากมีคำสั่งเป็นลาย ลักษณ์อักษร สำนักเทคโนโลยีสารสนเทศ จะลบข้อมูลสารสนเทศของบัญชีผู้ใช้งาน (Username) ดังกล่าวเป็นการถาวร

1.4.2 กรณีบุคคลภายนอก ระบบจะยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศอัตโนมัติเมื่อครบ กำหนดเวลาการใช้งานตามทำขอใช้งาน

2. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และ ระบบสารสนเทศของผู้ใช้งาน (User) ให้ดำเนินการ ดังนี้

2.1 ผู้ดูแลระบบ (Administrator) ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับบุคลากร หรือบุคคล ภายนอกให้สอดคล้องกับคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ หรือเหตุผลความ จำเป็นของสำนัก/กอง/ศูนย์/กลุ่ม ที่ได้แจงความประสงค์ในการให้บุคคลากรเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ แล้วแต่กรณี

2.2 ในกรณีที่มีการเปลี่ยนแปลงตำแหน่ง หรือหน้าที่ที่ได้รับมอบหมาย ให้สำนัก/กอง/ศูนย์/กลุมแจ้งสำนักเทคโนโลยีสารสนเทศเพื่อเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้ สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

2.3 ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อ พ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ ถึงระดับใดได้บ้าง

3. ให้สำนักเทคโนโลยีสารสนเทศจัดฝึกอบรมให้แก่ผู้ใช้งาน (User) เพื่อให้มีความรู้ ความเข้าใจและเกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศโดยไม่ระมัด ระวัง หรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ 1ครั้ง หรือจัดให้ผู้ใช้งาน (User) เข้าร่วมการฝึกอบรมที่หน่วย งานอื่นจัดขึ้น

4. ให้สำนักเทคโนโลยีสารสนเทศกำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศตามความเหมาะสมได้แก่ ยกเลิกการใช้งาน Internet กรณีที่มีการตรวจพบ Package จาก Users นั้น ๆ มากผิดปกติ หรือการแจ้งเตือนผู้ใช้งาน (User) เมื่อมีไวรัสแพร่ระบาด

5. เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

หมวดที่ 3
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และ ระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

1. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

2. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์ และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

3. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้ สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

4. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูลที่สำคัญหรือ ข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544

แนวปฏิบัติ

1. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

1.1 ผู้ใช้งาน (User) ต้องกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษอย่างน้อย 8 ตัว ขึ้นไป ซึ่งต้องประกอบด้วยตัวเลข (Numerical character), ตัวอักษร (Alphabet) ประกอบด้วยตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวอักษรพิเศษ (Special character)

– ตัวอักษร (a-z, A-Z)

– ตัวเลข (0-9)

– เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

1.2 ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก 9 เดือน และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

1.3 ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเองห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

1.4 ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

1.5 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

1.6 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

1.7 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

1.8 กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่าน ให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

1.9 การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการ รักษาความลับ ทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

1.10 การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

2. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อก หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

2.1 คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

2.2 การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

2.3 การใช้งานอินเตอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอก ตัวตนบุคคลผู้ใช้งานได้

2.4 เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

2.5 เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาไม่เกิน 15 นาที

3. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานขอมูล ไม่ว่าข้อมูลนั้นจะเป็นของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ หรือเป็น ข้อมูลของบุคคลภายนอก

4. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

5. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการ รับผิดชอบต่อความเสียหายนั้นด้วย

6. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

7. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตาม เห็นสมควร สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูล ส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้น ในกรณีที่สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ต้องการ ตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ซึ่งสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ อาจแต่งตั้งให้ผู้ทำหน้าที่ ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดย ไม่ต้องแจ้งให้ผู้ใช้งานทราบ

8. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หมายถึง วิธีการจัดเครือข่าย คอมพิวเตอร์แบบหนึ่งที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมี โปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์ เครื่องใดก็ได้แทนที่จะต้องใช

จากเครื่องบริการแฟ้ม (File Server เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับ เดียวกัน เช่น บิทเทอร์แรนท์ (Bit torrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

9. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

10. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มี ลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

11. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใด อันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

12. ห้ามใช้สินทรัพย์ของกรมสุขภาพจิต เพื่อประโยชน์ทางการค้า

13. ห้ามกระทำการใดๆเพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกรมสุขภาพจิตโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

14. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

15. ห้ามใช้ระบบสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

16. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

17. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเขาถึงระบบสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ โดยไม่ได้รับอนุญาต จากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

หมวดที่ 4
การควบคุมการเข้าถึงเครือข่าย
(Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2. กำหนดแนวปฏิบัติการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถ เข้าใช้งานเครือข่ายระบบคอมพิวเตอร์และระบบสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ได้

3. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

4. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้ง การเข้าถึงทางกายภาพและทางเครือข่าย

5. กำหนดแนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in Networks) โดยต้องแบ่งแยกเครือข่ายตามกลุ่มของ การให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภทของเครือข่าย

6. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ และการส่งข้อมูล สารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อ ควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

7. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

แนวปฏิบัติ

1. การเข้าถึงเครือข่ายของผู้ใช้งาน (User)

1.1 การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้

1.1.1 กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าใช้งาน ระบบเครือข่ายภายนอก (Internet)

1.1.2 ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครอง แบนด์วิดท์ (Bandwidth) สูงที่ ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ Youtube หนังออนไลน์ หรือรายการบันเทิงต่างๆ ในเวลาราชการ

1.1.3 ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามกอนาจาร เว็บไซต์ที่มี เนื้อหาที่ทาให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย

1.1.4 ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ผ่านระบบเครือข่าย ภายนอก (Internet) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

1.1.5 ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ ที่แก้ไขเพิ่มเติม โดยเคร่งครัด ได้แก่ ห้ามเผยแพร่ภาพหรือข้อมูลใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือที่มีลักษณะลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว ผ่านระบบเครือข่ายภายนอก (Internet) ห้ามเผยแพร่ภาพของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

1.1.6 ต้องระมัดระวังการดาวน์โหลด (Download) ไฟล์ข้อมูล หรือโปรแกรมต่างๆจากระบบเครือข่าย ภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุกโจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ

1.1.7 หลังจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้วให้ Logout ออกจากระบบ ปิดเว็บ บราวเซอร์ (Web Browser) เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

1.2 การถ่ายโอนข้อมูลของสำนักเทคโนโลยีสารสนเทศ ที่รับส่งผ่านระบบเทคโนโลยีสารสนเทศโดยมีแนวปฏิบัติ ดังนี้

1.2.1 จำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลลับ

1.2.2 กำหนดผู้ใช้งานใดที่มีสิทธิหรือได้รับอนุญาตให้เข้าถึง

1.2.3 ไม่อนุญาตการใช้งานข้อมูลสำคัญ หรือข้อมูลลับ ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

1.2.4 การรับ-ส่งข้อมูล หรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่างหน่วยงานภายในหรือภายนอกที่ได้รับอนุมัติเท่านั้น

1.2.5 มีการนำเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ ผ่านช่องทางการสื่อสารบางประเภทที่ ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing เป็นต้น

ข้อตกลงสำหรับการถ่ายโอนข้อมูลสารสนเทศ (Agreements on Information Transfer)

1) กำหนดให้ผู้เข้ามาใช้งานขอรหัสผ่านเพื่อเข้าใช้งานระบบจากผู้ดูแลระบบจากผู้ดูแลระบบ ซึ่งรหัสผ่านสามารถใช้ได้ในช่วงเวลาที่กำหนดไว้เท่านั้น

2) กำหนดข้อตกลง แนวทาง วิธีปฏิบัติ ระยะเวลา ของการถ่ายโอนสารสนเทศ

3) มีการบันทึก วันเวลาที่มีการถ่ายโอนสารสนเทศ

4) จำกัดการเข้าถึงสารสนเทศเมื่อมีการโอนย้ายเสร็จสิ้นแล้ว

โดยกรอกข้อมูลตาม แบบขอรายงานผู้มารับบริการของหน่วยงานในสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ยื่นสำนัก เทคโนโลยีสารสนเทศโดยมีรายละเอียด ดังนี้วัน เดือน ปี ที่ขอข้อมูล, ชื่อ-สกุล (ผู้ขอรายงาน), ตำแหน่ง, หน่วยงาน/สังกัด, เบอร์โทรศัพท์, E-mail, จุดประสงค์ในการขอรายงาน, ช่วงเวลาของข้อมูล, รายละเอียดของรายงาน,ลงลายมือชื่อ-ตำแหน่ง หัวหน้าฝ่าย/หัวหน้างาน ผู้ขอข้อมูล

หมายเหตุ : กรณีที่เป็นข้อมูลส่วนบุคคลก่อนส่งข้อมูลจะมีการเข้ารหัสข้อมูล (Encryption) เพื่อปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกเปิดเผย

2. การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้ดำเนินการ ดังนี้

2.1 ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ ที่แก้ไขเพิ่มเติม โดยเคร่งครัด และห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

2.2 ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ส่งโดยโดเมนเนม @dmh.mail.go.th

2.3 ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มีนามสกุล .exe, .com, .bat และ .inf

2.4 หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องออกจากระบบ (Log Out) ทันที เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

3. การใช้งานเครือข่ายไร้สาย (Wi Fi) ให้ดำเนินการ ดังนี้

3.1 ผู้ดูแลระบบ (Administrator) ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้ง เพื่อใช้งาน

3.2 ผู้ใช้งาน (User) ต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเอง ในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (Wi Fi)

3.3 ในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศผ่านเครือข่ายไร้สาย (Wi Fi)ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิของ เครือข่ายไร้สาย (Wi Fi) เท่านั้น

3.4 ห้ามผู้ใช้งาน (User) ติดตั้งและเปิดการทำงานโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของกรมสุขภาพจิต และมีความผิดตาม พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

4. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

4.1 การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์หรือเครื่องหมายแสดงสังกัดได้

4.2 การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับภารกิจงานของกรมสุขภาพจิต ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสารที่เป็น ประโยชน์ มีความถูกต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความ เห็นชอบจากผู้บังคับบัญชากก่อนทุกครั้ง

4.3 ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของกรมสุขภาพจิต ผ่านเครือข่ายสังคม ออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

4.4 กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผลงดเว้นการโต้ตอบ ด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่ เกี่ยวข้องต่อไป

4.5 ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ และต้องแสดง ข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

4.6 หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

5. การแบ่งแยกเครือข่าย (Segregation in Networks) แบ่งเป็น 4 กลุ่ม ดังนี้

5.1 กลุ่มของการให้บริการสารสนเทศ ได้แก่ ระบบสารสนเทศเพื่อการสนับสนุนภารกิจหลักและ ระบบสารสนเทศเพื่อการสนับสนุนการปฏิบัติงาน

5.2 กลุ่มการใช้งาน ได้แก่ เจ้าของระบบ (System Owner) ผู้ดูแลระบบ (Administrator) และ ผู้ใช้งาน (User)

5.3 กลุ่มของอุปกรณ์สารสนเทศ ได้แก่ อุปกรณ์รักษาความมั่นคงปลอดภัยสารสนเทศและอุปกรณ์บริหารจัดการเครือข่าย

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

6. มาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

6.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตร ผู้ติดต่อ (Visitor) แล้วทำการ ลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

6.2 ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ใน แบบฟอร์มการขอ อนุญาตเข้า-ออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

6.3 ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้า-ออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

7. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอก แบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยดาวน์โหลดผ่านเว็บไซต์สำนักเทคโนโลยีสารสนเทศ https://ict.dmh.go.th

8. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการ กระทำของระบบและผู้ใช้งานอื่นๆ

9. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

10. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

10.1 ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

10.2 ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

10.3 ตhองจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

10.4 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก หน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกรวมทั้งต้องมีความสามารถในการตรวจจับ โปรแกรมประสงค์ร้าย (Malware) ด้วย

10.5 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention system/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้า ใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ

10.6 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้อง มีการลง บันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

10.7 ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

10.8 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

10.9 การระบุอุปกรณ์บนเครือข่าย

(1) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

(2) ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใชอุปกรณ์ได้

(3) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

(4) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและ ปลายทางได้

(5) การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

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

12. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

13. กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มี ความมั่นคงปลอดภัย

14. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ 2550

15. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบตามแนวทางปฏิบัติ ดังต่อไปนี้

15.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่อง คอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็น ลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน

15.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

15.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาต จากหัวหน้าหน่วยงาน

15.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นใน การดำเนินงานกับหน่วยงานอย่างเพียงพอ

15.5 การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการ ลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความ ถูกต้องของผู้ใช้งานก่อนทุกครั้ง

16. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวน การกำหนดค่า Parameter ต่างๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

17. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

18. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบ เครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

19. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบ และ จำกัดการใช้งานเฉพาะเท่าที่จำเป็น

หมวดที่ 5
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม้ได้รับอนุญาต

นโยบาย

1. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยต้องมีการ ควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

2. กำหนดแนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยต้องกำหนดให้ผู้ใช้งาน (User) มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน (User) ได้ และเลือกใช้ ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการยืนยันว่าเป็นผู้ใช้งาน (User) ที่ได้รับอนุญาต

3. กำหนดแนวปฏิบัติในการบริหารจัดการรหัสผ่าน (Password Management System) โดยต้องจัดทำระบบบริหารจัดการรหัสผ่าน (Password) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะ อัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่าน (Password) ที่มีคุณภาพ

4. กำหนดแนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและ ควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคง ปลอดภัยที่ได้กำหนดไว้

5. กำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน (Session Time - Out)

6. กำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time)

แนวปฏิบัติ

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

2. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้

3. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบ ความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบปฏิบัติการ (Operating System)

4. สำนักเทคโนโลยีสารสนเทศต้องจัดให้มีระบบการบริหารจัดการรหัสผ่าน (Password Management System) โดยผู้ใช้งาน (User) สามารถเปลี่ยนรหัสผ่าน (Password) ใหม่ หรือขอรหัสผ่าน (Password) ใหม่ได้ผ่านระบบ บริหารจัดการรหัสผ่าน (Password Management System) กำหนด

5. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

5.1.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

5.1.2 หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัส ผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

6. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

7. ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

8. ผู้ใช้งานตองไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้ งานเครื่องคอมพิวเตอร์ของหน่วยงานรวมกัน

9. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ เป็นเวลานาน

10. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาต จากหัวหน้าหน่วยงาน

11. ซอฟต์แวร์ที่กรมสุขภาพจิต ใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหนาที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

12. ซอฟท์แวร์ที่สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

13. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เพื่อประโยชน์ทางการค้า

14. ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพ ไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

15. ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

16. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้

16.1 ผู้ใชงาน (User) ต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใดๆ บนระบบปฏิบัติการทั้งนี้ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจงความประสงค์ต่อสำนักเทคโนโลยีสารสนเทศ

16.2 การใช้งานโปรแกรมอรรถประโยชน์ขอื่นๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ ได้แก่ โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatter กำหนดให้ผู้ดูแลระบบ (Administrator) เท่านั้นที่มีสิทธิใช้งาน

17. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศเมื่อเว้นว่างจากการใช้งาน (Session Time - Out) เมื่อครบ 15 นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

18. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลาเชื่อมต่อ ระบบคอมพิวเตอร์ และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time) โดยให้ใช้งานได้เป็นเวลา 3 ชั่วโมงต่อ การเชื่อมต่อหนึ่งครั้ง และในกรณีที่เชื่อมต่อจากภายนอก กำหนดให้ใช้งานได้ภายในวันและเวลาราชการ เว้นแต่กรณี ที่มีเหตุผลความจำเป็นให้ขออนุญาตผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

หมวดที่ 6
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม้ได้รับอนุญาต

นโยบาย

1. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)ของผู้ใช้งาน (User) และฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น (Application and Information Access Control) ตามสิทธิ์ที่กำหนดไว้

2. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวนมีผลกระทบ และมีความสำคัญสูงต่อสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ โดยต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อม โดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking)

3. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติ และมาตรการที่เหมาะสมเพื่อปกป้อง ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจาก ความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

4. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติ

1. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

1.1 ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิ์ตามตำแหน่ง และหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ 1ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศด้วย

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

1.3 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับ ความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

1.4 ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้น จากตำแหน่ง หรือยกเลิกการใช้งาน

(2) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ ไม่ได้ป้องกันการเข้าถึง

(3) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(4) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่า เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

1.5 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลาย ข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ตองควบคุมการเข้าถึงข้อมูลแตละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่าน ระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบ ตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

(3) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็น มาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(5) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(6) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของขอมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

1.6 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

(1) แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ

(2) มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน

(3) มีการกำหนดสิทธิ์ห็เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

1.7 การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

(1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพ พร้อมใช้งาน หรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มี การเผยแพรเป็นการทั่วไป

(3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(4) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(5) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

1.8 การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) ผ่านระบบ

1.8.1 ก่อนปฏิบัติงาน

(1) ผู้รับจ้าง (Outsource) ต้องขออนุญาตผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เพื่อเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาต เข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับผู้รับจ้างพร้อมแนบสำเนาสัญญาจ้าง หรือเหตุผลในการปฏิบัติงาน

(2) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการ ขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร

(3) ผู้ดูแลระบบ (Administrator) ดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนด รหัสผ่านชั่วคราว (Temporary Password) สำหรับเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(4) ผู้ดูแลระบบ (Administrator) แจ้งให้ผู้รับจ้าง (Outsource) ได้รับทราบ

1.8.2 ระหว่างปฏิบัติงาน

(1) ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

(2) เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการสำนักเทคโนโลยี สารสนเทศต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง (Outsource) ตลอดระยะเวลาการ ดำเนินการ

(3) ผู้รับจ้าง (Outsource) ต้องปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายเท่านั้น และต้อง คำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่าง การปฏิบัติงานให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่กำกับดูแลการปฏิบัติงานทันที

1.8.3 หลังปฏิบัติงาน

(1) ผู้รับจ้าง (Outsource) แจ้งความประสงค์ต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือตัวแทนฝ่ายบริหาร ISMR เพื่อยกเลิกสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

(2) ผู้ดูแลระบบ (Administrator) จะยกเลิกสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบ สารสนเทศและลบข้อมูลสารสนเทศของผู้รับจ้าง (Outsource) เป็นการถาวรเมื่อพ้นกำหนด 90 วัน

1.8.4 การรักษาความลับ ผู้รับจ้าง (Outsource)ต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

หมวดที่ 7
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสุขภาพจิต ซึ่งได้รวม การบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินและการบริหารความต่อเนื่องในสภาวะวิกฤต ด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้ อย่างต่อเนื่อง แม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลา ที่เหมาะสม และสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

1. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน
2. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสุขภาพจิต เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
3. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่องของ สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ด้านสารสนเทศ
4. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผน
5. บริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสุขภาพจิต อย่างน้อยปีละ 1 ครั้ง
6. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติ

1. สำนักเทคโนโลยีสารสนเทศต้องจัดทำระบบสารสนเทศและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอนดังนี้

1.1 ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศ

1.2 ผู้ดูแลระบบ (Administrator) กำหนดรูปแบบการสำรองข้อมูลของระบบการสำรองข้อมูล (Backup System) ดังนี้

1.2.1 รายชื่อระบบคอมพิวเตอร์และระบบสารสนเทศที่ได้รับการพิจารณาคัดเลือก ดังนี้

(1) ระบบคอมพิวเตอร์เครื่องลูกข่ายเสมือน (Virtual Desktop Infrastructure: VDI)

(2) ระบบติดตามการดำเนินการของโครงการ (Tracking System)

(3) ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(4) ระบบสำนักงานอัตโนมัติ (E-Office)

(5) ระบบสารบรรณอิเล็กทรอนิกส์ (E-Saraban)

(6) ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ – รัฐวิสาหกิจ (GFMIS - SOE)

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

1.2.3 กำหนดรูปแบบการสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ทั้งนี้ เนื่องจากสำนักเทคโนโลยีสารสนเทศได้ดำเนินการสำรองข้อมูลระบบคอมพิวเตอร์ และระบบสารสนเทศแบบสมบูรณ์ (Full Backup) ทุกระบบงานจึงได้รับการสำรองข้อมูลด้วย

1.3 ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรือ External Disk และอื่นๆ ที่ใช้สำหรับการสำรองข้อมูลได้แก่รูปแบบการสำรองข้อมูลแบบรายวัน หรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

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

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

1.4.2 การกู้คืนข้อมูลรายสัปดาห์หรือรายเดือนจากอุปกรณ์ที่ใช้ในการสำรองข้อมูลแบบสมบูรณ์ (Full Backup)

2. สำนักเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

2.1 กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ

2.2 กำหนดผู้มีหน้าที่รับผิดชอบระบบสำรองข้อมูลสารสนเทศ

2.3 กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว

2.4 กำหนดให้ปรับปรุงแผนดังกล่าวทุก 2 ปี

3. สำนักเทคโนโลยีสารสนเทศต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้อย่างน้อยปีละ 1 ครั้งทั้งนี้ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และแผนการสำรองข้อมูลกรมสุขภาพจิต รวมถึงการทดสอบสภาพความพร้อมใช้งาน ได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องในสภาวะวิกฤต ด้านสารสนเทศของกรมสุขภาพจิต รายละเอียดปรากฏตามเอกสารภาคผนวก

หมวดที่ 8 การเข้ารหัสข้อมูล
(Cryptographic)

วัตถุประสงค์

เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลง แก้ไขข้อมูลที่เป็นความลับ หรือ มีความสำคัญ

นโยบาย

1. กำหนดนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูลที่คำนึงถึงชนิด และวิธีการ เข้ารหัสข้อมูล ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับ หรือ มีความสำคัญ

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

3. กำหนดผู้รับผิดชอบในการดำเนินนโยบาย และการบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (Key Management)

4. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดย ให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

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

แนวปฏิบัติ

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

2. การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

3. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลที่สำนักบริการคอมพิวเตอร์กำหนดไว้ และให้ใช้ความระมัดระวัง ในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail) ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งผิด

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

5. การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ ผ่านช่องทางการสื่อสารบางประเภท ที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing

6. การบริหารจัดการกุญแจ (Key Management) ทำการคัดเลือกวิธีการเข้ารหัสการกำหนดความยาวของรหัสการใช้งาน และการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้ง ติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบาย และแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ เช่น มาตรการพิเศษสำหรับป้องกันเอกสารข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

หมวดที่ 9
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนด มีความมั่นคงปลอดภัย และหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

1. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

2. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

1. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ 1 ครั้ง

2. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

2.1 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้ดำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

2.2 หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิคให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

3. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

3.1 ผู้ตรวจสอบต้องจัดทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

3.2 สำนักเทคโนโลยีสารสนเทศต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

3.3 ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้สำนักเทคโนโลยีสารสนเทศสร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งสำนักเทคโนโลยีสารสนเทศทราบ

3.4 สำนักเทคโนโลยีสารสนเทศต้องจัดสรรอุปกรณ์ที่จำเป็นต้องใช้ในการตรวจสอบเชิงเทคนิค

3.5 ในกรณีมีการติดตั้งเครื่องมือที่ใช้ในการตรวจประเมินความเสี่ยงระบบคอมพิวเตอร์ และระบบสารสนเทศสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

3.6 ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

3.7 ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ตรวจสอบเป็นระยะเวลาไม่น้อยกว่า 90 วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

ภาคผนวก

แนวปฏิบัติ เมื่อเกิดฟิชชิ่ง (Phishing) ที่เว็บเซอร์เวอร์ของหน่วยงาน

วัตถุประสงค์

เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชชิ่ง (Phishing) ให้สามารถดำเนินการได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหาย และส่งผลกระทบต่อหน่วยงานทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

แนวปฏิบัติ

ข้อ 1. เมื่อผู้ดูแลระบบเครือข่ายของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ได้รับแจ้งหรือตรวจพบว่าเว็บเซอร์เวอร์ของ หน่วยงานใดๆ เป็นช่องทางให้ผู้ไม่หวังดีทำฟิชชิ่ง (Phishing) ผู้ดูแลระบบของกรมฯจะดำเนินการ ดังนี้

(1) ดำเนินการบล็อค IP Address ของเว็บเซอร์เวอร์ที่โดนฟิชชิ่งนั้น หรือแจ้งผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานดำเนินการโดยเร่งด่วน

(2) แจ้งผู้ดูแลเว็บเซอร์เวอร์ของหน่วยงานที่ถูกทำฟิชชิ่ง ทาง e-Mail หรือทาง โทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

ข้อ 2. เมื่อหน่วยงานดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานไปยังเมื่อผู้ดูแลระบบเครือข่ายของกรมฯหรือผู้ให้บริการเส้นทางเครือข่ายของหน่วยงานเพื่อปลด บล็อค IP Address

ข้อ 3. ผู้ดูแลเว็บเซอร์เวอร์ของหน่วยงานต้องตรวจสอบเว็บเซอร์เวอร์และเว็บไซต์ภายใน หน่วยงานของตนเอง รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) อย่าง สม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีในการเข้ามาทำฟิชชิ่ง

หมายเหตุ : ทางผู้เสียหายส่วนใหญ่ เป็นหน่วยงานที่มีการทำธุรกรรมอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการเงิน เช่น ธนาคาร เว็บไซต์ที่เกี่ยวกับการซื้อขายออนไลน์ ฯลฯ หากการดำเนินการแก้ไขปัญหาดังกล่าวล่าช้าและมีความเสียหาย อาจมีผลทางกฎหมายต่อหน่วยงานของท่าน

แนวปฏิบัติ เมื่อเกิดภัยคุกคามทางไซเบอร์เกี่ยวกับมัลแวร์เรียกค่าไถ่ (ransomware)

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการดำเนินการเพื่อรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์เกี่ยวกับมัลแวร์เรียกค่าไถ่ (ransomware) ได้อย่างทันท่วงที

แนวปฏิบัติ

ข้อ 1. IDENTIFY คอมพิวเตอร์ทุกเครื่อง โดยแยกเป็นกลุ่มตามระดับผลกระทบหาถูกโจมตีจากมัลแวร์ (ระบุผู้รับผิดชอบเครื่องแต่ละเครื่อง เช่น หน่วยงาน, ส่วนกลาง, ข้อมูลติดต่อ Vendor)

<u>กลุ่มตามผลกระทบ</u>

A+ : สำคัญต่อชีวิตคนไข้ และ Operation ที่มีการต่อเชื่อมกับระบบเครือข่าย

A : ระบบที่เกี่ยวข้องกับการเก็บข้อมูลผู้ป่วย ที่มีการต่อเชื่อมกับระบบเครือข่าย

B : ระบบที่เชื่อมต่อกับ HIS ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ที่มีการต่อเชื่อมกับระบบเครือข่าย

C : ระบบที่ไม่ได้ต่อเชื่อมกับ HIS ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ 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 แอร์ ลิฟต์ CCTV)

P : Personal Computer (PC) ทั่วไป

M : Mobile Device

ข้อ 2. วางแผนการจัดการ การตรวจสอบเครื่องแต่ละกลุ่ม และดำเนินการป้องกัน

ข้อ 3. Backup ข้อมูลที่สำคัญออกจากเครื่อง ไว้ใน External Hard disk อย่างน้อย 3 แหล่ง (ที่ไม่ต่อเชื่อมกับระบบเครือข่าย เพื่อป้องกันการถูกเข้ารหัสไฟล์ข้อมูล)

ข้อ 4. สื่อสาร ให้ความรู้เกี่ยวกับการป้องกัน/การลดความเสี่ยงแก่ผู้ใช้งาน (Users) มิให้เป็นพาหะนำมัลแวร์เข้าสู่เครือข่าย เช่น ไม่เปิดอีเมล์ที่ไม่รู้จัก ไม่คลิกเปิดหรือ Download ไฟล์แนบที่ไม่ระบุแหล่งที่มาที่รู้จัก รวมถึง ไฟล์น่าสงสัยอื่น ๆ

ข้อ 5. จัดทีมเพื่อดำเนินการป้องกัน (ติดตั้ง/Update Patch OS) และสื่อสารให้ความรู้กับผู้ใช้ และให้มีผู้จัดการกำกับ และติดตามสถานะอย่างใกล้ชิด

ข้อ 6. ผู้ดูแลระบบ

1.) ระบบให้บริการผู้ป่วยหรือระบบเครือข่ายของหน่วยงานต้องมีการติดตั้งระบบป้องกันเครือข่าย (Firewall)

2.) ระบบพิสูจน์ตัวตน อย่างน้อยต้องมีการพิสูจน์ตัวตน (Authentication) ในการใช้งานระบบบริการหรือระบบเครือข่ายของหน่วนงาน และมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตาม พรบ.คอมพิวเตอร์ (Log file) อย่างเหมาะสม

3.) จัดตารางระบบสำรองข้อมูลเช่น ฐานข้อมูล โปรแกรมที่มีความจำเป็นเพื่อเป็นการป้องกันข้อมูลสูญหาย และสามารถนำกลับมาใช้ได้โดยไม่เกิดผลกระทบกับระบบที่ต้องการใช้งาน

4.) จัดทำแผนการทดสอบและการกู้คืนข้อมูลที่สำคัญหลังจากสำรองข้อมูลไปแล้ว

5.) จัดให้มีเครื่องแม่ข่ายสำรองสำหรับระบบที่จำเป็นใช้งาน เช่น ระบบให้บริการผู้ป่วย เว็บไซต์ หลังจากระบบหลักมีปัญหาสามารถใช้งานได้โดยไม่เกิดผลกระทบกับการบริการหรือเปิดผลกระทบน้อยที่สุด

6.) หลังจากทำการสำรองข้อมูลแล้วให้ตัดการเชื่อต่อกับระบบเพื่อป้องกันการโดนโจมตี

ข้อ 7. ผู้ใช้งานระบบ

1.) ผู้ใช้งานระบบต้องไม่ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาตจากผู้ดูและรบบ

2.) ไม่เปิดไฟล์ที่ไม่ทราบแหล่งที่มาที่ชัดเจน

3.) ไม่ใช้งานเว็บไซต์ที่มีความเสี่ยงในเครื่องที่เป็นระบบ HIS

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

แนวปฏิบัติการนำเข้าข้อมูลสารสนเทศ (Import Data)

วัตถุประสงค์

เพื่อควบคุมการการนำเข้าข้อมูลสารสนเทศ (Import Data) ให้เป็นไปตามข้อกำหนดของกรมสุขภาพจิต และสร้างความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

1. กำหนดให้มีผู้รับผิดชอบในการกำหนดสิทธิการใช้งาน

2. กำหนดให้มีกระบวนการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุม โดยให้มีการควบคุมจำกัดและเปลี่ยนแปลงสิทธิการนำเข้าข้อมูลสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ

3. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการนำเข้าสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

4. กำหนดให้มีมาตรการในการป้องกันตามกฎหมายที่เกี่ยวข้อง

แนวปฏิบัติ

ข้อ 1. การขออนุญาตการนำเข้าสารสนเทศ ให้ดำเนินการ ดังนี้

1.1 การนำเข้าข้อมูลผู้ป่วยด้านสุขภาพจิต และจิตเวช

1.1.1 ให้สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ทำหนังสือแต่งตั้งผู้รับผิดชอบในการนำเข้าข้อมูล ลงนามโดยผู้มีอำนาจภายในหน่วยงานถึงสำนักเทคโนโลยีสารสนเทศ เพื่อพิจารณาอนุมัติ และดำเนินการสอดคล้องกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.1.2 ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งาน และเวลาในการเข้าถึงระบบฯ ตามสิทธิที่ร้องขอพร้อมทั้งกำหนดให้มีการจัดเก็บข้อมูลการเข้าใช้งาน (log files)

1.1.3 แจ้งช่องทางการเข้าถึงและระเบียบการใช้งานให้ผู้ขอใช้งานรับทราบ

1.1.4 เมื่อครบกำหนดตามระยะเวลาการร้องขอผู้ดูแลระบบจะต้องยกเลิกสิทธิการเข้าถึงระบบฯ

1.2 กรณีบุคคลภายนอก

1.2.1 ให้สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ทำหนังสือแจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ลงนามโดยผู้มีอำนาจภายในหน่วยงานถึงสำนักเทคโนโลยีสารสนเทศ เพื่อพิจารณาอนุมัติ และดำเนินการสอดคล้องกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.2.2 ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการใช้งานและเวลาในการเข้าถึงระบบฯ ตามสิทธิที่ร้องขอพร้อมทั้งกำหนดให้มีการจัดเก็บข้อมูลการเข้าใช้งาน (log files)

1.2.3 แจ้งช่องทางการเข้าถึงและระเบียบการใช้งานให้ผู้ขอใช้งานรับทราบ

1.2.4 เมื่อครบกำหนดตามระยะเวลาการร้องขอ ผู้ดูแลระบบจะต้องยกเลิกสิทธิการเข้าถึงระบบฯ

แนวปฏิบัติการพัฒนา Website ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้

วัตถุประสงค์

เพื่อควบคุมการการดำเนินการพัฒนา Website ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ เพื่อให้เกิดมาตรฐานความมั่นคงปลอดภัยในการพัฒนา Website ของหน่วยงาน

นโยบาย

1. กำหนดให้สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ ที่มีการให้บริการ Website มีมาตรฐานการให้บริการตามระเบียบของกระทรวงสาธารณสุข

2. การพัฒนา Website ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ มีมาตรฐานสอดคล้องกับมาตรฐานเว็บไซต์ภาครัฐ, มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่

3. สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ มีอัตลักษณ์ในการให้บริการ Domain เดียวกัน

4. สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้ พัฒนา Website ตรงตามกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

1. Website ของหน่วยงาน ต้องใช้ Domain ของหน่วยงาน หรือ Domain ของสถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้เท่านั้น

2. การพัฒนา Website ให้ปฏิบัติตามนโยบายการพัฒนามาตรฐานเว็บไซต์ภาครัฐ, มาตรฐานแอปพลิเคชันภาครัฐสำหรับอุปกรณ์เคลื่อนที่ เวอร์ชั่นปัจจุบัน

3. Website ที่ให้บริการแก่เจ้าหน้าที่และบุคคลภายนอก ให้ดำเนินการติดตั้งใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์ (SSL Certificate : https://) จากผู้ให้บริการที่ได้รับการรับรอง/น่าเชื่อถือ

4. จัดให้มีระบบป้องกันการบุกรุกและโปรแกรมป้องกันไวรัส

5. โปรแกรมที่ใช้งานต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

6. กรณีที่ใช้งานโปรแกรมเว็บไซต์สำเร็จรูปจะต้องมีคณะกรรมการไอซีที (ICT) ของหน่วยงานพิจารณาก่อนทำการติดตั้ง

7. กรณีที่ไม่สามารถทำตามข้อกำหนด ให้ทำหนังสือชี้แจงมาที่ งานเทคโนโลยีสารสนเทศ สถาบันสุขภาพจิตเด็กและวัยรุ่นภาคใต้