



ประกาศสำนักวิชาการสุภาพจิต
เรื่อง แนวปฏิบัติการควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญ
และรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักวิชาการสุภาพจิต เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้ง ป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหาย

สำนักวิชาการสุภาพจิต จึงได้จัดทำแนวทางปฏิบัติการควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญ และรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรสำนักวิชาการสุภาพจิตมีความรู้ ความเข้าใจ และสามารถปฏิบัติตามแนวทางการปฏิบัติการเข้าถึงการควบคุมการใช้งานและความมั่นคงปลอดภัยด้านสารสนเทศ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงข้อมูลที่สำคัญและการกำหนดสิทธิของหน่วยงาน เพื่อควบคุมสิทธิในการเข้าถึงข้อมูลและติดตามการใช้งานระบบสารสนเทศได้อย่างถูกต้อง ดังนี้

ข้อมูล หมายถึง ข่าวสาร เอกสาร ข้อเท็จจริงเกี่ยวกับบุคคล สิ่งของหรือเหตุการณ์ที่มีอยู่ รูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่าง ๆ ที่มีความหมายเฉพาะตัว ซึ่งยังไม่มีผลการประมวลผลสำหรับการนำไปใช้ได้

ผู้ใช้งาน หมายถึง บุคลากรของสำนักวิชาการสุภาพจิต (ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างเหมาบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศ)

ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ในการรับผิดชอบดูแลระบบสารสนเทศ โดยมีหน้าที่กำหนดสิทธิการเข้าถึงข้อมูลและดูแลรักษาระบบคอมพิวเตอร์และระบบเครือข่าย

การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบหมายให้แก่ผู้ใช้งาน เพื่อเข้าถึงข้อมูลหรือการใช้งานระบบเครือข่ายหรือระบบสารสนเทศ หรืออุปกรณ์ประมวลผลของข้อมูลสารสนเทศ รวมทั้งการอนุญาตให้ใช้งานที่เป็นบุคคลภายนอก

การยืนยันตัวตน หมายถึง การอนุญาต การกำหนดสิทธิ การให้เข้าถึงข้อมูลหรือระบบสารสนเทศต่าง ๆ

ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารส่งข้อมูลสารสนเทศระหว่างเทคโนโลยีต่าง ๆ ของหน่วยงาน ระบบแลน (LAN) ระบบอินเทอร์เน็ต

ระบบสารสนเทศ หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการอำนวยความสะดวกในการปฏิบัติงานต่าง ๆ และสามารถนำไปใช้ประโยชน์ในการวางแผน การบริหารงาน รวมถึงการพัฒนางาน ให้เกิดประสิทธิภาพสูงสุด

ระเบียบการใช้งานระบบสารสนเทศของสำนักวิชาการสุภาพจิต

ระเบียบในการรักษาความปลอดภัยมั่นคงด้านเทคโนโลยีสารสนเทศ ของสำนักวิชาการสุภาพจิต จัดทำเพื่อกำหนดแนวทางปฏิบัติในการรักษาความปลอดภัยมั่นคงด้านสารสนเทศและการควบคุมสิทธิการเข้าถึงข้อมูล ที่สำคัญของระบบสารสนเทศ เพื่อให้บุคลากรสำนักวิชาการสุภาพจิตตระหนักถึง

ความสำคัญของระบบเทคโนโลยีสารสนเทศของหน่วยงาน พร้อมทั้งสามารถให้ใช้งานระบบสารสนเทศช่วยในการปฏิบัติงาน ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น มีความปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ (อ้างอิงจากแนวทางปฏิบัติการรักษาความปลอดภัยไซเบอร์ สำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต <https://ict.dmh.go.th/iso/view.asp?id=6>)

๑. แนวปฏิบัติ

การควบคุมการเข้าถึงข้อมูลสารสนเทศ (Access Control) สำนักวิชาการสุขภาพจิตให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัยเป็นหลัก ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) จะอนุญาตให้ผู้ใช้งานเข้าถึงข้อมูลระบบสารสนเทศ ในส่วนที่ผู้ใช้งานรับผิดชอบเท่านั้น และต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

๑.๒ ผู้ใช้งาน (User) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะได้รับอนุญาตตามสิทธิของผู้ใช้งานเท่านั้น

๑.๓ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้ตรงตามการเข้าใช้งานของผู้ใช้งาน และมีหน้าที่ทบทวนสิทธิในการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ

๑.๔ การกำหนดสิทธิในการอนุญาตให้เข้าถึงข้อมูลสารสนเทศ ของสำนักวิชาการสุขภาพจิต

๑.๕ การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

(๑) อ่านอย่างเดียว

(๒) สร้างข้อมูล

(๓) เพิ่มข้อมูล

(๔) แก้ไขข้อมูล

(๕) ลบข้อมูล

(๖) อนุมัติสิทธิ

๒. สิทธิการเข้าถึงข้อมูลสารสนเทศ สำนักวิชาการสุขภาพจิต

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่ได้รับมอบหมายหรือเกี่ยวข้องในการปฏิบัติงานเข้าถึงระบบสารสนเทศและระบบเครือข่ายโดยมิได้รับอนุญาต รวมถึงการจำกัดสิทธิในการใช้งานระบบสารสนเทศ เพื่อให้สามารถตรวจสอบสิทธิติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานในระบบสารสนเทศของสำนักวิชาการสุขภาพจิต โดยกำหนดแนวทางปฏิบัติในการควบคุมสิทธิในการเข้าถึงข้อมูลสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๒.๑ จัดทำแบบฟอร์มลงทะเบียนเป็นผู้ใช้งานระบบสารสนเทศเพื่อตรวจสอบสิทธิการใช้งานของผู้ใช้งานในระบบสารสนเทศ

๒.๒ มีการลงทะเบียนผู้ใช้งาน

๒.๓ กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ

(๑) ต้องเป็นบุคลากรในสำนักวิชาการสุขภาพจิต หรือบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของสำนักวิชาการสุขภาพจิต

(๒) การใช้งานที่ขัดต่อข้อกำหนด หรือกระทำการใด ๆ ที่ส่งผลให้เกิดความเสียหายต่อระบบสารสนเทศ

๒.๔ การกำหนดในการยกเลิกการอนุญาตในการเข้าถึงระบบสารสนเทศ

(๑) การตัดออกจากทะเบียนสิทธิ การโยกย้ายหน่วยงาน การระงับการใช้งานหรือการสิ้นสุดสถานภาพการเป็นผู้ใช้งานในระบบสารสนเทศ

(๒) การใช้งานที่ขัดต่อข้อกำหนด หรือกระทำการใด ๆ ที่ส่งผลให้เกิดความเสียหายต่อระบบสารสนเทศ

๒.๕ ต้องมีการบริหารจัดการการกำหนดสิทธิ์ให้ผ่านสำหรับผู้ใช้งาน

๒.๖ มีการทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์ในการเข้าถึงอย่างน้อยปีละ ๑ ครั้ง

๓. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญของข้อมูลให้ใช้แนวทางปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔

๓.๑ ข้อมูลทั่วไปที่เปิดเผยได้

๓.๒ ข้อมูลที่ต้องกำหนดสิทธิ์

(๑) ข้อมูลระบบสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลบุคลากร ข้อมูลยุทธศาสตร์

(๒) ข้อมูลสารสนเทศสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลทรัพยากรบุคคล ข้อมูลด้านการให้บริการสนับสนุนการบริหาร

๔. การบริหารจัดการ การเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่เกี่ยวข้องในการปฏิบัติงานเข้าถึงระบบสารสนเทศ โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ์ในการใช้งานระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

๔.๑ การแบ่งกลุ่มผู้ใช้งานระบบสารสนเทศ เพื่อควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศโดยระบบข้อบัญญัติผู้ใช้งานแยกแบบรายบุคคล

(๑) ผู้อำนวยการ สำนักวิชาการสุภาพจิต

(๒) บุคลากรสำนักวิชาการสุภาพจิต

๔.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องดำเนินการลงทะเบียนผู้ใช้งานเพื่อควบคุมสิทธิ์ในการใช้งานระบบสารสนเทศ

๔.๓ ผู้ใช้งานที่มีชื่อในบัญชีรายชื่อผู้มีสิทธิ์ใช้งานทั่วไปในการเข้าถึงระบบสารสนเทศตามกลุ่มผู้ใช้งานทั่วไป

๔.๔ หน่วยงานเจ้าของระบบเป็นผู้กำหนดสิทธิ์ในการใช้งานระบบสารสนเทศรวมถึงการกำหนดระยะเวลาในการใช้งาน

๔.๕ การแจ้งยกเลิกสิทธิ์การใช้งานในระบบสารสนเทศ

(๑) ผู้บริหารของสำนักวิชาการสุภาพจิตที่ขอใช้แจ้งยกเลิกสิทธิ์การใช้งานของผู้ใช้งานทั่วไป

(๒) ผู้ดูแลระบบทำการยกเลิกสิทธิ์ในการใช้งานตามคำขอ และทำการลบข้อมูลผู้ใช้งานทั่วไปออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๔.๖ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานทั่วไป (User Password Management)

(๑) ต้องกำหนดรหัสผ่านสำหรับผู้ใช้งานทั่วไปให้มีความปลอดภัย โดยมีชุดตัวอักษรผสมตัวเลข หรืออักขระ หรือสัญลักษณ์ เข้าด้วยกัน อย่างน้อยรวมกัน ๘ ตัวอักษร

(๒) ส่งมอบรหัสผ่านผู้ใช้งานทั่วไปให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งเป็นเอกสารให้ส่งมอบโดยการส่งทางจดหมายอิเล็กทรอนิกส์ (E-mail)

๔.๗ ผู้ดูแลระบบต้องกำหนดการใช้งานและรหัสผ่านเป็นรายบุคคล ให้กับผู้ใช้งาน

๔.๘ ผู้ดูแลระบบต้องส่งมอบรหัสผ่านให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย และผู้ใช้ต้องทำการเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อใช้งานระบบครั้งแรก

๔.๙ ผู้ใช้งานต้องทำการยืนยันตัวตนที่ถูกต้อง ก่อนการเปลี่ยนรหัสผ่าน

๔.๑๐ ผู้ใช้งานต้องไม่เจต หรือบันทึกรหัสผ่านของตนเองไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น ทั้งนี้ ให้ถือปฏิบัติตามแนวทางปฏิบัติการควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญ และรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของสำนักวิชาการสุภาพจิต อย่างเคร่งครัดต่อไปด้วย

ประกาศ ณ วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๘



(นายบุรินทร์ สุรอรุณสัมฤทธิ์)
นายแพทย์ทรงคุณวุฒิ (ด้านเวชกรรม สาขาจิตเวช)
ปฏิบัติหน้าที่ผู้อำนวยการสำนักวิชาการสุภาพจิต