ประกาศสำนักวิชาการสุขภาพจิต
เรื่อง แนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control)
สำนักวิชาการสุขภาพจิต

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีผลบังคับใช้เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที มิให้เกิดผลกระทบต่อความมั่นคงปลอดภัยทางด้านสาธารณสุขของประเทศ

กระทรวงสาธารณสุข จึงได้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข ฉบับที่ ๑ เพื่อให้หน่วยงานในสังกัดกระทรวงสาธารณสุขสามารถดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ เห็นผลอย่างเป็นรูปธรรม และให้ทุกหน่วยงานปฏิบัติโดยเคร่งครัดต่อเนื่อง

กรมสุขภาพจิต ได้ดำเนินการตามมาตรการดังกล่าว ภายใต้ตัวชี้วัดค่าคะแนนความสำเร็จในการพัฒนาสู่การเป็นองค์กรดิจิทัล ตามคำรับรองการปฏิบัติราชการของหน่วยงานในสังกัดกรมสุขภาพจิต ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ซึ่งกำหนดให้หน่วยงานจัดทำระเบียบหรือแนวทางปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) ให้สอดคล้องกับมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข ฉบับที่ ๑ โดยจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากผู้ที่เกี่ยวข้อง จึงกำหนดแนวปฏิบัติเพื่อใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่งผลให้การใช้งานระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ และป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อระบบสารสนเทศของหน่วยงาน กองยุทธศาสตร์และแผนงาน จึงได้จัดทำแนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) ขึ้น เพื่อเผยแพร่ให้บุคลากรและบุคคลภายนอกที่ปฏิบัติงานร่วมกับกองยุทธศาสตร์และแผนงาน ได้รับทราบและให้ความร่วมมือปฏิบัติตามอย่างเคร่งครัดต่อไป ตามรายละเอียด ดังนี้

๑. ระเบียบการใช้สารสนเทศภายในสำนักวิชาการสุขภาพจิต การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๑.๑ สำนักวิชาการ...

๑.๑ สำนักวิชาการสุขภาพจิต ดำเนินกิจการภายใต้กฎหมายไทย ดังนั้น การใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อทางอินเทอร์เน็ต ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๒ สำนักวิชาการสุขภาพจิต ไม่สนับสนุน หรือยินยอมให้เจ้าหน้าที่ของหน่วยงานกระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๓ ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายถือเป็นทรัพย์สินของหน่วยงาน ห้ามผู้ไม่ได้รับการอนุญาตหรือผู้ที่ไม่เกี่ยวข้องใช้งานโดยมิได้รับอนุญาต หากผู้ใดกระทำการใด ๆ เป็นการบุกรุกเขตหวงห้ามหรือพยายามบุกรุกเข้าสู่ระบบเครือข่าย ถือเป็นการละเมิดตามกฎหมาย ต้องได้รับโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

๑.๔ สิทธิ์ในการเข้าถึงการใช้สารสนเทศ เป็นไปตามบทบาทหน้าที่ที่เกี่ยวข้องหรือได้รับมอบหมายจากผู้บังคับบัญชา ไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องกับสารสนเทศ หรือในส่วนที่ไม่เกี่ยวข้องกับตนเข้าใช้งาน

๑.๕ การยืมทรัพย์สินสารสนเทศจะต้องทำตามขั้นตอนการยืม และเมื่อสิ้นสุดการใช้งานหรือสิ้นสุดสัญญาณ หรือสิ้นสุดข้อตกลงการจ้างจะต้องคืนทรัพย์สินตามขั้นตอนการคืนทรัพย์สิน

๑.๖ การทำลายอุปกรณ์หรือสื่อบันทึกข้อมูล หรือสารสนเทศ ต้องทำตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการพัสดุ พ.ศ. ๒๕๖๑

๑.๗ เครื่องคอมพิวเตอร์ และอุปกรณ์ประกอบที่สำคัญ จะต้องมีการกำหนดรหัสผ่าน (Password) ที่มีความยาวอย่างน้อย ๖-๘ ตัว เพื่อควบคุมการเข้าถึงและเพื่อป้องกันการเข้าถึงข้อมูล สำนักงานโดยไม่ได้รับอนุญาต

๒. แนวปฏิบัติ

๒.๑ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๒.๑.๑ ระดับชั้นผู้ดูแลระบบ (Administrator)

๒.๑.๒ ระดับชั้นผู้อนุมัติ (Approver)

๒.๑.๓ ระดับชั้นผู้ใช้งาน (User)

๒.๒ การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศกำหนด ดังนี้

๒.๒.๑ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิ์ ตรวจสอบสิทธิ์ ทบทวนสิทธิ์และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๒.๒.๒ ผู้อนุมัติ (Approver) อนุมัติสิทธิ์ให้ผู้ใช้งานตามภารกิจ เพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เฉพาะในส่วนที่ได้รับมอบหมาย ตามความเป็นจำในการใช้งาน

๒.๒.๓ ผู้ใช้งาน (User) ตามสิทธิ์การเข้าถึงข้อมูลที่กำหนด

๒.๓ เกณฑ์...

๒.๓ เกณฑ์ในการอนุญาตการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ดังนี้

๒.๓.๑ สิทธิ์ของผู้ดูแลระบบ (Administrator) แต่ละระบบสารสนเทศ ดังนี้
- อ่านข้อมูล
- ป้อนข้อมูล
- แก้ไข

๒.๓.๒ สิทธิ์ของผู้อนุมัติ (Approver) แต่ละระบบสารสนเทศ ดังนี้
- อ่านข้อมูล
- อนุมัติ

๒.๓.๓ สิทธิ์ของผู้ใช้งาน (User) แต่ละระบบสารสนเทศ ดังนี้
- อ่านอย่างเดียว
- ป้อนข้อมูล
- แก้ไข

ตารางที่ ๑ สิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

ระบบ	ผู้ใช้งาน (ป้อนข้อมูล/อ่านอย่างเดียว)	ผู้อนุมัติ (อนุมัติ)	ผู้ดูแลระบบ (สร้างข้อมูล/แก้ไข)
๑. จองห้องประชุม สำนักวิชาการสุขภาพจิต	บุคลากร สำนักวิชาการสุขภาพจิต	นักวิชาการคอมพิวเตอร์	นักวิชาการคอมพิวเตอร์
๒. ยืม-คืนอุปกรณ์ IT สำนักวิชาการสุขภาพจิต	บุคลากร สำนักวิชาการสุขภาพจิต	นักวิชาการคอมพิวเตอร์	นักวิชาการคอมพิวเตอร์
๓. รายการจัดประชุม สำนักวิชาการสุขภาพจิต	บุคลากร สำนักวิชาการสุขภาพจิต	หัวหน้ากลุ่มบริหารงานทั่วไป	กลุ่มบริหารงานทั่วไป
๔. จองห้องประชุมออนไลน์ Tele-Conference	บุคลากร สำนักวิชาการสุขภาพจิต	นักวิชาการคอมพิวเตอร์	นักวิชาการคอมพิวเตอร์
๕. ระบบวันลา	บุคลากร สำนักวิชาการสุขภาพจิต	หัวหน้ากลุ่มงานและผู้อำนวยการ/รักษาราชการแทนผู้อำนวยการ	นักวิชาการคอมพิวเตอร์

ทั้งนี้ ขอให้บุคลากรทุกท่านถือปฏิบัติตามแนวปฏิบัติในการควบคุมสิทธิ์การเข้าถึงข้อมูลที่สำคัญ (Access Control) อย่างเคร่งครัด ตั้งแต่บัดนี้ เป็นต้นไป

ประกาศ ณ วันที่ ๑๙ กุมภาพันธ์ พ.ศ. ๒๕๖๗

(นายเทอดศักดิ์ เดชคง)
นายแพทย์ทรงคุณวุฒิ (ด้านเวชกรรม สาขาจิตเวช)
ปฏิบัติหน้าที่ผู้อำนวยการสำนักวิชาการสุขภาพจิต