ประกาศกองบริหารระบบบริการสุขภาพจิต
เรื่อง แนวปฏิบัติในการควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญ (Access Control)

ตามประกาศกรมสุขภาพจิตเรื่อง แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมสุขภาพจิต พ.ศ. ๒๕๖๔ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่องนั้น

กองบริหารระบบบริการสุขภาพจิต จึงจัดทำแนวปฏิบัติในการควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญ (Access Control) ดังนี้

วัตถุประสงค์

๑. เพื่อกำหนดการเข้าถึงข้อมูลสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัยด้านสารสนเทศ

๒. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนด โดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๓. เพื่อให้การตรวจสอบและติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศได้อย่างถูกต้อง

๔. เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. บุคลากรกองบริหารระบบบริการสุขภาพจิต ต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

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

แนวปฏิบัติ

๑. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งานเท่านั้น

๒. ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๓. ผู้ดูแลระบบ...

๓. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ตามคำนิยามดังนี้

"ผู้ดูแลระบบ" หมายถึง บุคลากรกองบริหารระบบบริการสุขภาพจิต ผู้ซึ่งได้รับมอบหมายจากเจ้าของระบบ (System Owner) หรือจากผู้อำนวยการหน่วยงานให้มีหน้าที่รับผิดชอบในการกำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และการบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศของระบบเทคโนโลยีสารสนเทศ

"ผู้ใช้งาน" หมายถึง บุคลากรกองบริหารระบบบริการสุขภาพจิตทุกระดับ ซึ่งเป็นข้าราชการ พนักงานราชการ ลูกจ้างประจำ และพนักงานจ้างเหมา ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่าย และโปรแกรมประยุกต์หรือแอพพลิเคชั่นของกองบริหารระบบบริการสุขภาพจิต และ/หรือเกี่ยวข้องกับการใช้ประโยชน์จากระบบเทคโนโลยีสารสนเทศ

๓.๑ การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๓.๑.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรองข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข เช่น ข้อมูลผู้ป่วยข้อมูลทางการแพทย์ ข้อมูลสถานพยาบาล เป็นต้น

๓.๑.๒ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง
- ข้อมูลลับ หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
- ข้อมูลใช้งานภายในองค์กร หมายถึง ข้อมูลที่ใช้งานภายในองค์กร และไม่ได้รับอนุญาตให้นำไปใช้งานภายนอกองค์กร
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่จำเป็นต้องได้รับการคุ้มครองความมั่นคงปลอดภัย ข้อมูลที่เผยแพร่สู่สาธารณะ ผ่านช่องทางที่เหมาะสม ซึ่งองค์กรพิจารณาอนุมัติหากข้อมูลสูญหายหรือถูกเปิดเผยจะไม่ส่งผลเสียหายต่อองค์กร

๓.๑.๓ จัดแบ่ง...

๓.๑.๓ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- สำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๓.๑.๔ รูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ 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

๔. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๔.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิตามตำแหน่ง และหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออกหรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๔.๒ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๔.๒.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๔.๒.๒ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๔.๒.๓ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

ประกาศ ณ วันที่ ๒๘ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๗

(นางสาวดุษฎี จึงศิรกุลวิทย์)
ผู้อำนวยการกองบริหารระบบบริการสุขภาพจิต