



ประกาศศูนย์สุขภาพจิตที่ ๖ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ มีผลบังคับใช้เมื่อวันที่ ๒๔ สิงหาคม ๒๕๖๔ กำหนดให้สำนักงานปลัดกระทรวงสาธารณสุข เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านสาธารณสุข สำหรับหน่วยงานที่มีลักษณะการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยาเวชภัณฑ์ และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ปลัดกระทรวงสาธารณสุข จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อประสานงาน เผื่อระวังรับมือ และแก้ไขภัยคุกคามทางไซเบอร์ ด้านสาธารณสุข รวมถึงสอดคล้องกับนโยบายของกระทรวงสาธารณสุข คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของศูนย์สุขภาพจิตที่ ๖ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานที่ไม่ถูกต้อง จากภัยคุกคามต่าง ๆ ซึ่งจะก่อให้เกิดความเสียหายต่อองค์กร ศูนย์สุขภาพจิตที่ ๖ ขอประกาศแนวปฏิบัติ เพื่อให้สอดคล้องตามนโยบาย ดังนี้

- กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และให้การสนับสนุนในเรื่องงบประมาณ ทรัพยากร ความรู้ความเข้าใจแก่บุคลากร
- กำหนดแนวทางปฏิบัติที่เกี่ยวข้องในเรื่องการรักษาความลับ (Confidentiality) โดยการทำสัญญาการรักษาความลับ การรักษาความถูกต้อง ความสมบูรณ์ (Integrity) กำหนดสิทธิการเข้าถึงข้อมูลตามหน้าที่ที่เกี่ยวข้อง ความพร้อมใช้งาน (Availability) มีระบบอุปกรณ์สำรอง การกำหนดสิทธิการเข้าออกพื้นที่เพื่อป้องกันการโจรกรรมข้อมูล กำหนดรหัสเข้าใช้งาน และปรับปรุงตามนโยบายองค์กร
- สื่อสาร ให้ความรู้ความเข้าใจด้านกฎหมาย ข้อบังคับ ข้อตกลงที่เกี่ยวข้องกับการให้บริการด้านเทคโนโลยีสารสนเทศ ความต่อเนื่อง และข้อมูลความปลอดภัย
- กำหนดเป็นหัวข้อการอบรมปฐมนิเทศบุคลากรใหม่ และทบทวนในที่ประชุมของศูนย์สุขภาพจิตที่ ๖ ประจำปี
- ดำเนินการซักซ้อมแผนความต่อเนื่อง พัฒนา ปรับปรุง ทดสอบให้เหมาะสมและมั่นใจว่าพร้อมรับในทุกสถานการณ์
- มีการทำข้อตกลงกับผู้ให้บริการภายนอก ผู้ขายอุปกรณ์ ในการให้ความร่วมมือเมื่อเกิดอุบัติการณ์ที่ส่งผลต่อความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศในการให้บริการ และทบทวนข้อตกลงปีละ ๑ ครั้ง

๗. ผู้ที่เกี่ยวข้องทำการวางแผน และจัดการเรื่องความปลอดภัยของข้อมูล ระบบโครงข่าย เครื่องมือและอุปกรณ์ ให้อยู่ในระบบมาตรฐานซึ่งเป็นที่ยอมรับและเชื่อถือได้ รวมทั้งให้การดูแลเป็นพิเศษ

๘. การเก็บรักษาความปลอดภัยของข้อมูล จะต้องระบุไว้เป็นส่วนหนึ่งในสัญญาบริการที่หน่วยงาน ทำกับผู้ใช้บริการ ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งจะต้องถือปฏิบัติโดยเคร่งครัด

๙. ศูนย์สุขภาพจิตที่ ๖ มีหน้าที่ในการจัดเก็บและเก็บรักษาข้อมูลของผู้ใช้บริการตามแบบ และวิธีการที่ได้ทำความตกลงร่วมกันไว้ระหว่างหน่วยงานกับผู้ใช้บริการ รวมทั้งการไม่เปิดเผยข้อมูลใด ๆ ที่มีได้รับความ ยินยอมจากผู้ใช้บริการสู่สาธารณชน หรือบุคคลภายนอก เพื่อมิให้มีการรั่วไหลหรือการสูญหายของข้อมูลของ ผู้ใช้บริการ ไม่ว่าจะในกรณีใด ๆ

๑๐. ศูนย์สุขภาพจิตที่ ๖ จะต้องจัดทำเอกสารที่ระบุไว้อย่างชัดเจนว่าบุคลากรจะไม่นำข้อมูลของ หน่วยงานหรือข้อมูลของผู้ใช้บริการไปเปิดเผยแก่บุคคลภายนอก หรือที่ใด ๆ หากมิได้รับความยินยอมจากหน่วยงาน หรือจากผู้ใช้บริการ

๑๑. ศูนย์สุขภาพจิตที่ ๖ ต้องดำเนินการตามแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์สุขภาพจิตที่ ๖ ที่ประกาศไว้ <https://mh6.dmh.go.th/web1/cyber/2.pdf>

๑๒. มาตรการเกี่ยวกับความปลอดภัยของข้อมูล ถือเป็นหน้าที่ของบุคลากรทุกคนของ ศูนย์สุขภาพจิตที่ ๖ จะต้องปฏิบัติตามและหากมีการฝ่าฝืน ให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง ถือเป็น หน้าที่ที่จะต้องแจ้งให้บุคลากรทุกคนทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล

นโยบายและแนวปฏิบัตินี้ บุคลากรของศูนย์สุขภาพจิตที่ ๖ จะต้องให้ความร่วมมือและถือปฏิบัติ ร่วมกัน เพื่อให้มั่นใจว่าศูนย์สุขภาพจิตที่ ๖ จะรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และมีการปรับปรุง ประสิทธิภาพอย่างต่อเนื่อง

ประกาศ ณ วันที่ กุมภาพันธ์ พ.ศ. ๒๕๖๘

(นางภัทรานิษฐ์ ทองตันไตรย์)
ผู้อำนวยการศูนย์สุขภาพจิตที่ ๖