นโยบายความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Policy)
ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐

เพื่อให้ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ มีการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงด้านไซเบอร์อย่างมีประสิทธิภาพ สอดคล้องกับแนวปฏิบัติที่เป็นมาตรฐานสากล เพื่อป้องกันภัยคุกคาม การโจมตี การทำลายระบบสารสนเทศ และการจารกรรมข้อมูลทางไซเบอร์ จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ โดยมีสาระสำคัญ ดังนี้

๑. ให้มีคณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีตัวแทนจากกลุ่มงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ จากกระบวนการดำเนินงานเป็นผู้รับผิดชอบความมั่นคงปลอดภัยทางไซเบอร์ และให้กำหนดหน้าที่ความรับผิดชอบพร้อมทั้งวิธีการบริหารจัดการ

๒. พัฒนาและรักษากรอบการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้สอดคล้องกับมาตรฐานสากล และติดตามกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง และพิจารณาการปฏิบัติตามให้สอดคล้อง

๓. ให้มีการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ โดยการประเมินจากภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) ความเป็นไปได้ (Likelihoods) และผลกระทบ (Impact) ต่อการดำเนินงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ รวมทั้งให้มีการจัดการความเสี่ยง ที่มีความสอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดขององค์กร อีกทั้งหน่วยงานภายนอกที่เกี่ยวข้อง

๔. สื่อความและจัดอบรมให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อสร้างความตระหนักรู้ ความรับผิดชอบ และความเข้าใจการรับมือกับภัยคุกคามทางไซเบอร์ให้กับเจ้าหน้าที่ อย่างน้อยปีละ ๑ ครั้ง

๕. ให้มีการติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ ให้ครอบคลุมระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๐ พร้อมทั้งจัดให้มีการเฝ้าระวัง และให้คณะที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ ต้องรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างน้อยปีละครั้ง

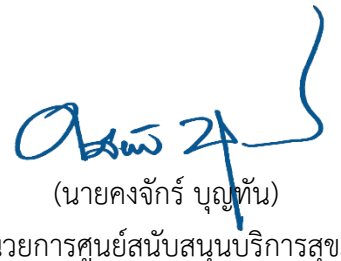
๖. ให้จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งลดผลกระทบต่อกระบวนการดำเนินงานที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนการตอบสนองฯ อย่างน้อยปีละ ๑ ครั้ง

๗. ให้จัดทำแผนฟื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติ เพื่อลดผลกระทบต่อกระบวนการดำเนินงานที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนฟื้นฟูฯ เพื่อประเมินความถูกต้องและมีประสิทธิผลของแผน อย่างน้อยปีละ ๑ ครั้ง

๘. ให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) หรือ การทดสอบเจาะระบบ (Penetration Test) โดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามด้านไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่ วันที่ ๓ มกราคม พ.ศ. ๒๕๖๖ เป็นต้นไป

สั่ง ณ วันที่ ๓ มกราคม พ.ศ. ๒๕๖๖



(นายคงจักร์ บุญทัน)
ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑๐