



ประกาศโรงพยาบาลนครปฐม  
เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์  
โรงพยาบาลนครปฐม

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI) และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ มีผลบังคับใช้เมื่อ ๒๔ สิงหาคม พ.ศ. ๒๕๖๔ กำหนดให้สำนักงานปลัดกระทรวงสาธารณสุข เป็นหน่วยงานควบคุมหรือกำกับดูแลด้านสาธารณสุข สำหรับหน่วยงานที่มีลักษณะการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านยาเวชภัณฑ์ และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ปลัดกระทรวงสาธารณสุข จึงมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CIRT) เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ ด้านสาธารณสุขรวมถึงสอดคล้องกับนโยบายของกระทรวงสาธารณสุข คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลนครปฐม เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานที่ไม่ถูกต้อง จากภัยคุกคามต่าง ๆ ซึ่งจะก่อให้เกิดความเสียหายต่อองค์กร

โรงพยาบาลนครปฐม ขอประกาศแนวทางปฏิบัติเพื่อให้สอดคล้องตามนโยบาย ดังนี้

- กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และให้การสนับสนุนในเรื่องงบประมาณ ทรัพยากร ความรู้ความเข้าใจแก่บุคลากร
- กำหนดแนวทางปฏิบัติที่เกี่ยวข้องในเรื่องของการรักษาความลับ (Confidentiality) โดยการทำสัญญาการรักษาความลับ การรักษาความถูกต้อง ความสมบูรณ์ (Integrity) กำหนดสิทธิการเข้าถึงข้อมูลตามหน้าที่ที่เกี่ยวข้อง ความพร้อมใช้งาน (Availability) มีระบบอุปกรณ์สำรอง การกำหนดสิทธิการเข้าออกพื้นที่เพื่อป้องกันการโจรกรรมข้อมูล กำหนดรหัสเข้าใช้งาน และปรับปรุงตามนโยบายองค์กร
- สื่อสาร ให้ความรู้ความเข้าใจด้านกฎหมาย ข้อบังคับ ข้อตกลงที่เกี่ยวข้องกับการให้บริการด้านเทคโนโลยีสารสนเทศ ความต่อเนื่อง ข้อมูลความปลอดภัย
- แต่งตั้งคณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีการขับเคลื่อนนโยบาย และรักษาระบบบริหารงานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง รวมถึงการประสานกับหน่วยประสานการรักษาความมั่นคงปลอดภัยไซเบอร์
- กำหนดเป็นหัวข้อการอบรมปฐมนิเทศบุคลากรใหม่ และทบทวนในที่ประชุมของหน่วยงานประจำปี

๖. ดำเนิน...

๖. ดำเนินการซักซ้อมแผนความต่อเนื่อง พัฒนา ปรับปรุง ทดสอบให้เหมาะสมและมั่นใจว่าพร้อมรับในทุกสถานการณ์

๗. มีการทำข้อตกลงกับผู้ให้บริการภายนอก ผู้ขายอุปกรณ์ ในการให้ความร่วมมือเมื่อเกิดอุบัติเหตุที่ส่งผลต่อความปลอดภัยด้านข้อมูลสารสนเทศในการให้บริการ และทบทวนข้อตกลงปีละ ๑ ครั้ง

๘. การเก็บรักษาความปลอดภัยของข้อมูล จะต้องระบุไว้เป็นส่วนหนึ่งในสัญญาบริการที่หน่วยงาน ทำกับผู้ให้บริการ ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งจะต้องถือปฏิบัติโดยเคร่งครัด

๙. มาตรการเกี่ยวกับความปลอดภัยของข้อมูล ถือเป็นหน้าที่ของบุคลากรทุกคน จะต้องปฏิบัติตามและหากมีการฝ่าฝืน ให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง ถือเป็นหน้าที่ที่จะต้องแจ้งให้บุคลากรทุกคนทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล นโยบายและแนวปฏิบัติ จะต้องให้ความร่วมมือและถือปฏิบัติร่วมกัน เพื่อให้มั่นใจว่าโรงพยาบาลนครปฐมจะรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และมีการปรับปรุงประสิทธิภาพอย่างต่อเนื่อง

ประกาศ ณ วันที่ ๑ พฤษภาคม พ.ศ. ๒๕๖๗

(นายสุรชัย โสภครรชิตไชย)

ผู้อำนวยการโรงพยาบาลนครปฐม