ประกาศโรงพยาบาลสองแคว

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์

.....

เพื่อให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสองแคว เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถสนับสนุนการให้บริการประชาชนได้อย่างต่อเนื่อง รวมทั้งเพื่อป้องกันปัญหาที่อาจเกิดจากภัยคุกคามทางไซเบอร์ การใช้งานระบบสารสนเทศที่ไม่ถูกต้อง การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล หรือเหตุการณ์อื่นใดที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ข้อมูลผู้รับบริการ ข้อมูลส่วนบุคคล และภาพลักษณ์ของโรงพยาบาล

โรงพยาบาลสองแคว จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของกระทรวงสาธารณสุข และกฎหมายหรือระเบียบอื่นที่เกี่ยวข้อง

จึงกำหนดนโยบายและแนวปฏิบัติดังต่อไปนี้

๑. วัตถุประสงค์

๑.๑ เพื่อให้การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของโรงพยาบาลสองแควมีความมั่นคงปลอดภัย เชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง

๑.๒ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศให้แก่ผู้บริหาร บุคลากร ผู้ดูแลระบบ และบุคคลภายนอกที่เกี่ยวข้อง

๑.๓ เพื่อป้องกัน ลดความเสี่ยง และรับมือกับภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบสารสนเทศของโรงพยาบาล

๑.๔ เพื่อคุ้มครองข้อมูลส่วนบุคคล ข้อมูลสุขภาพ ข้อมูลผู้รับบริการ และข้อมูลสำคัญของโรงพยาบาล

๑.๕ เพื่อสร้างความตระหนักรู้ให้บุคลากรทุกระดับเห็นความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๖ เพื่อใช้เป็นแนวทางในการตรวจสอบ ทบทวน ปรับปรุง และพัฒนาระบบบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลอย่างต่อเนื่อง

๒. ขอบเขตการบังคับใช้

นโยบายและแนวปฏิบัติฉบับนี้ใช้บังคับกับบุคลากรทุกระดับของโรงพยาบาลสองแคว ได้แก่ ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้าง ผู้ปฏิบัติงานชั่วคราว นักศึกษาฝึกงาน ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบสารสนเทศของโรงพยาบาล

โดยครอบคลุมถึงระบบคอมพิวเตอร์ ระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์สารสนเทศ ซอฟต์แวร์ ฐานข้อมูล ระบบสารสนเทศโรงพยาบาล ระบบคลาวด์ ระบบสื่อสาร ข้อมูลอิเล็กทรอนิกส์ เอกสารดิจิทัล และข้อมูลอื่นใดที่เกี่ยวข้องกับการดำเนินงานของโรงพยาบาล

๓. นิยาม

ความมั่นคงปลอดภัยสารสนเทศ หมายถึง การรักษาไว้ซึ่งความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลสารสนเทศ

ข้อมูลสารสนเทศ หมายถึง ข้อมูล ข้อความ เอกสาร หรือสารสนเทศใด ๆ ที่อยู่ในรูปแบบอิเล็กทรอนิกส์หรือกายภาพ ซึ่งโรงพยาบาลสร้าง จัดเก็บ ประมวลผล ใช้งาน หรือเผยแพร่

ระบบสารสนเทศ หมายถึง ระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ ซอฟต์แวร์ ฐานข้อมูล และระบบงานที่ใช้ในการจัดเก็บ ประมวลผล หรือให้บริการข้อมูล

ภัยคุกคามไซเบอร์ หมายถึง เหตุการณ์หรือการกระทำที่อาจส่งผลกระทบต่อระบบสารสนเทศ เช่น มัลแวร์ ฟิชชิง การโจมตีระบบ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล หรือการทำให้ระบบไม่สามารถให้บริการได้ตามปกติ

บุคลากร หมายถึง เจ้าหน้าที่ทุกระดับของโรงพยาบาลสองแคว รวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาล หรือได้รับอนุญาตให้ใช้ระบบสารสนเทศของโรงพยาบาล

๔. นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

๔.๑ การกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศ

๑. โรงพยาบาลสองแควกำหนดให้มีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อใช้เป็นแนวทางในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

๒. สนับสนุนทรัพยากร งบประมาณ บุคลากร และองค์ความรู้ที่จำเป็นต่อการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ตามความเหมาะสม

๓. แต่งตั้งหรือมอบหมายคณะทำงาน ผู้รับผิดชอบด้านระบบสารสนเทศ หรือผู้ดูแลระบบ เพื่อขับเคลื่อน ติดตาม และประสานงานการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

๔. กำหนดให้มีการประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานสาธารณสุขจังหวัด หน่วยประสานงานด้านไซเบอร์ของกระทรวงสาธารณสุข ThaiCERT หรือหน่วยงานอื่นตามความเหมาะสม

๕. ทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีกฎหมาย เทคโนโลยี โครงสร้างระบบสารสนเทศ หรือสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงอย่างมีนัยสำคัญ

๔.๒ การควบคุมการเข้าถึงระบบสารสนเทศ

๔.๒.๑ ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบสารสนเทศทุกครั้ง

๔.๒.๒ กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศตามหน้าที่ความรับผิดชอบ และตามหลักความจำเป็นในการใช้งาน

๔.๒.๓ ห้ามผู้ใช้งานเปิดเผยบัญชีผู้ใช้หรือรหัสผ่านของตนให้ผู้อื่นทราบ

๔.๒.๔ ห้ามใช้บัญชีผู้ใช้งานของบุคคลอื่นในการเข้าถึงระบบสารสนเทศของโรงพยาบาล

๔.๒.๕ เมื่อบุคลากรย้ายงาน เปลี่ยนหน้าที่ ลาออก หรือพ้นจากหน้าที่ ต้องมีการปรับปรุง ระงับ หรือยกเลิกสิทธิ์การใช้งานโดยเร็ว

๔.๒.๖ ผู้ใช้งานต้องล็อกหน้าจอหรือออกจากระบบทุกครั้งเมื่อไม่ได้ใช้งานเครื่องคอมพิวเตอร์

๔.๒.๗ ผู้ดูแลระบบต้องตรวจสอบและทบทวนสิทธิ์การใช้งานเป็นระยะ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔.๓ การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม

๔.๓.๑ ห้องเครื่องแม่ข่าย ห้องควบคุมระบบ หรือพื้นที่จัดเก็บอุปกรณ์สำคัญ ต้องมีการควบคุมการเข้าออกอย่างเหมาะสม

๔.๓.๒ ห้ามบุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าวโดยไม่ได้รับอนุญาต

๔.๓.๓ จัดให้มีระบบหรืออุปกรณ์สนับสนุนที่จำเป็น เช่น เครื่องสำรองไฟฟ้า ระบบปรับอากาศ ระบบป้องกันไฟฟ้าขัดข้อง และการดูแลสภาพแวดล้อมให้เหมาะสม

๔.๓.๔ ห้ามเคลื่อนย้าย ถอด เปลี่ยน หรือแก้ไขอุปกรณ์สำคัญโดยไม่ได้รับอนุญาต

๔.๓.๕ หากพบความผิดปกติ เช่น อุปกรณ์สูญหาย ร่องรอยการบุกรุก ไฟฟ้าขัดข้อง น้ำรั่ว หรือความเสียหายต่ออุปกรณ์ ให้แจ้งงานเทคโนโลยีสารสนเทศหรือผู้รับผิดชอบทันที

๔.๔ การป้องกันมัลแวร์และภัยคุกคามทางไซเบอร์

๔.๔.๑ เครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศของโรงพยาบาลควรมีระบบป้องกันไวรัสหรือมาตรการป้องกันมัลแวร์ที่เหมาะสม

๔.๔.๒ ห้ามติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ ซอฟต์แวร์ไม่พึงประสงค์ หรือซอฟต์แวร์ที่ไม่ได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศ

๔.๔.๓ ห้ามเชื่อมต่ออุปกรณ์ภายนอก เช่น USB, External Hard Disk หรืออุปกรณ์เครือข่ายอื่นใด ที่อาจก่อให้เกิดความเสี่ยง โดยไม่ได้รับอนุญาต

๔.๔.๔ ผู้ใช้งานต้องระมัดระวังการเปิดไฟล์แนบ ลิงก์ เว็บไซต์ หรือข้อความที่น่าสงสัย

๔.๔.๕ เมื่อพบความผิดปกติ เช่น เครื่องทำงานผิดปกติ ไฟล์สูญหาย มีข้อความเรียกค่าไถ่ หรือสงสัยว่าติดไวรัส ให้หยุดใช้งานและแจ้งผู้ดูแลระบบทันที

๔.๔.๖ งานเทคโนโลยีสารสนเทศต้องติดตาม เฝ้าระวัง และปรับปรุงมาตรการป้องกันภัยคุกคามให้เหมาะสมกับสถานการณ์

๔.๕ การสำรองข้อมูลและการกู้คืนระบบ

๔.๕.๑ โรงพยาบาลต้องจัดให้มีการสำรองข้อมูลสำคัญอย่างสม่ำเสมอ

๔.๕.๒ ข้อมูลสำรองต้องจัดเก็บไว้ในสถานที่หรือระบบที่ปลอดภัย และสามารถนำกลับมาใช้ได้เมื่อเกิดเหตุขัดข้อง

๔.๕.๓ จัดทำแผนกู้คืนระบบเมื่อเกิดเหตุฉุกเฉิน หรือ Disaster Recovery Plan ตามความเหมาะสมกับบริบทของโรงพยาบาล

๔.๕.๔ กำหนดแนวทางการดำเนินงานต่อเนื่อง หรือ Business Continuity Plan สำหรับระบบที่มีความสำคัญ

๔.๕.๕ ควรมีการทดสอบการกู้คืนข้อมูลและระบบเป็นระยะ เพื่อให้มั่นใจว่าสามารถใช้งานได้จริงเมื่อเกิดเหตุ

๔.๕.๖ กำหนดผู้รับผิดชอบในการสำรองข้อมูล ตรวจสอบข้อมูลสำรอง และรายงานผลการดำเนินงานอย่างเหมาะสม

๔.๖ การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย

๔.๖.๑ เมื่อพบเหตุการณ์ที่น่าสงสัยหรืออาจเป็นการละเมิดความมั่นคงปลอดภัย ต้องแจ้งงานเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ หรือผู้บังคับบัญชาทันที

๔.๖.๒ เหตุการณ์ที่ต้องรายงาน ได้แก่ การเข้าถึงระบบโดยไม่ได้รับอนุญาต การติดมัลแวร์ การรั่วไหลของข้อมูล การสูญหายของอุปกรณ์ หรือพฤติกรรมการใช้งานระบบที่ผิดปกติ

๔.๖.๓ จัดให้มีกระบวนการตรวจสอบ วิเคราะห์ แก้ไข และป้องกันการเกิดซ้ำ

๔.๖.๔ กรณีเหตุการณ์มีผลกระทบรุนแรง ให้รายงานต่อผู้บริหารและประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องตามความเหมาะสม

๔.๖.๕ หลังเกิดเหตุการณ์ ให้มีการสรุปบทเรียนและปรับปรุงมาตรการป้องกันให้เหมาะสมยิ่งขึ้น

๕. กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

โรงพยาบาลสองแควกำหนดกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ โดยอ้างอิงแนวคิดหลัก ๖ ด้าน ดังนี้

๕.๑ การกำกับดูแล

กำหนดโครงสร้าง ผู้รับผิดชอบ นโยบาย และกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจน

๕.๒ การระบุความเสี่ยง

จัดทำทะเบียนสินทรัพย์สารสนเทศ ประเมินความเสี่ยง วิเคราะห์ภัยคุกคาม และกำหนดระดับความสำคัญของระบบงาน

๕.๓ การป้องกัน

กำหนดมาตรการควบคุมการเข้าถึง การใช้รหัสผ่าน การสำรองข้อมูล การป้องกันมัลแวร์ การเข้ารหัสข้อมูล และการให้ความรู้แก่บุคลากร

๕.๔ การเฝ้าระวัง

ติดตาม ตรวจสอบ บันทึกเหตุการณ์ และวิเคราะห์ความผิดปกติของระบบสารสนเทศอย่างเหมาะสม

๕.๕ การตอบสนอง

จัดทำแนวทางหรือแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดผู้รับผิดชอบ และช่องทางการรายงานเหตุการณ์

๕.๖ การฟื้นฟู

จัดทำแผนกู้คืนระบบและข้อมูล ทดสอบการกู้คืนเป็นระยะ และปรับปรุงกระบวนการหลังเกิดเหตุการณ์

๖. ความรับผิดชอบของบุคลากร

บุคลากรทุกคนของโรงพยาบาลสองแควมีหน้าที่ร่วมกันในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยต้องปฏิบัติดังนี้

๖.๑ ใช้งานระบบสารสนเทศของโรงพยาบาลเพื่อประโยชน์ในการปฏิบัติงานราชการเท่านั้น

๖.๒ รักษาความลับของข้อมูลผู้รับบริการ ข้อมูลส่วนบุคคล ข้อมูลสุขภาพ และข้อมูลภายในของโรงพยาบาล

๖.๓ ไม่เปิดเผย ส่งต่อ คัดลอก ถ่ายภาพ หรือเผยแพร่ข้อมูลของโรงพยาบาลโดยไม่ได้รับอนุญาต

๖.๔ ไม่ใช้บัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น และไม่อนุญาตให้ผู้อื่นใช้บัญชีของตนเอง

๖.๕ ไม่ติดตั้งโปรแกรมหรือเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาต

๖.๖ ไม่ใช้อินเทอร์เน็ตหรืออีเมลของโรงพยาบาลเพื่อกระทำผิดกฎหมาย แสวงหาผลประโยชน์ส่วนตน หรือกระทำการที่อาจกระทบต่อชื่อเสียงของโรงพยาบาล

๖.๗ ระมัดระวังการใช้สื่อสังคมออนไลน์ การส่งข้อมูลผ่านช่องทางออนไลน์ และการเผยแพร่ข้อมูลที่เกี่ยวข้องกับโรงพยาบาล

๖.๘ แจ้งเหตุการณ์ผิดปกติด้านระบบสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์ต่อผู้รับผิดชอบทันที

๖.๙ ให้ความร่วมมือในการอบรม ซักซ้อมแผน ทบทวนแนวปฏิบัติ และการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ

๗. แนวปฏิบัติในการใช้เทคโนโลยีปัญญาประดิษฐ์และบริการออนไลน์

๗.๑ การใช้เครื่องมือปัญญาประดิษฐ์หรือบริการออนไลน์ต้องเป็นไปเพื่อประโยชน์ในการปฏิบัติงาน และต้องไม่ขัดต่อกฎหมายหรือระเบียบของโรงพยาบาล

๗.๒ ห้ามนำข้อมูลผู้ป่วย ข้อมูลส่วนบุคคล ข้อมูลลับ หรือข้อมูลอ่อนไหวของโรงพยาบาลไปป้อนในระบบ Generative AI หรือบริการออนไลน์ภายนอก โดยไม่ได้รับอนุญาต

๗.๓ ห้ามใช้เทคโนโลยี AI เพื่อสร้างข้อมูลเท็จ ปลอมแปลงข้อมูล หรือเผยแพร่ข้อมูลที่อาจทำให้เกิดความเข้าใจผิด

๗.๔ ข้อมูลหรือเอกสารที่ได้จากการใช้ AI ต้องได้รับการตรวจสอบความถูกต้องก่อนนำไปใช้ในการปฏิบัติงานจริง

๗.๕ หากมีความจำเป็นต้องใช้ระบบภายนอกในการประมวลผลข้อมูลสำคัญ ให้ปรึกษางานเทคโนโลยีสารสนเทศก่อนดำเนินการ

๘. การสื่อสาร อบรม และสร้างความตระหนักรู้

๘.๑ โรงพยาบาลสองแควจะสื่อสารนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศให้บุคลากรทุกระดับรับทราบ

๘.๒ กำหนดให้เรื่องความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลเป็นหัวข้อหนึ่งในการปฐมนิเทศบุคลากรใหม่

๘.๓ มีการทบทวนหรือให้ความรู้แก่บุคลากรเป็นระยะ เช่น การป้องกันฟิชชิง การตั้งรหัสผ่าน การใช้ระบบงานอย่างปลอดภัย และการรายงานเหตุการณ์ผิดปกติ

๘.๔ ส่งเสริมให้บุคลากรตระหนักว่าการรักษาความปลอดภัยของข้อมูลเป็นหน้าที่ร่วมกันของทุกคน

๙. การตรวจสอบกิจกรรมและการปฏิบัติตามกฎหมาย

๙.๑ ข้อมูล ระบบงาน และอุปกรณ์ที่จัดทำหรือจัดเก็บอยู่ในระบบของโรงพยาบาล ถือเป็นทรัพย์สินของโรงพยาบาลสองแคว

๙.๒ โรงพยาบาลมีสิทธิ์ตรวจสอบกิจกรรมการใช้งานระบบสารสนเทศ อุปกรณ์ อินเทอร์เน็ต และเครือข่ายของโรงพยาบาล เพื่อรักษาความมั่นคงปลอดภัย ป้องกันการใช้งานที่ไม่เหมาะสม และตรวจสอบเหตุการณ์ผิดปกติ

๙.๓ การตรวจสอบต้องดำเนินการตามความจำเป็น เหมาะสม และสอดคล้องกับกฎหมายที่เกี่ยวข้อง

๙.๔ บุคลากรทุกคนต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลอย่างเคร่งครัด

๙.๕ หากมีการฝ่าฝืนหรือกระทำการที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศหรือข้อมูลของโรงพยาบาล อาจถูกพิจารณาดำเนินการตามระเบียบ วินัย หรือกฎหมายที่เกี่ยวข้อง

๑๐. การทบทวนและปรับปรุงนโยบาย

นโยบายและแนวปฏิบัติฉบับนี้จะได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็น เมื่อมีการเปลี่ยนแปลงด้านกฎหมาย นโยบาย เทคโนโลยี โครงสร้างระบบสารสนเทศ หรือสถานการณ์ภัยคุกคามทางไซเบอร์ เพื่อให้มีความเหมาะสม ทันสมัย และสามารถใช้ปฏิบัติได้จริง

จึงประกาศมาให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ เมษายน พ.ศ. ๒๕๖๙

(ลงชื่อ) กลพล

(นายกุลพล ตั้งรัตนาพิบูล)

ผู้อำนวยการโรงพยาบาลสองแคว