ประกาศโรงพยาบาลศรีนคร
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของโรงพยาบาลศรีนคร พ.ศ.๒๕๖๖

.....

เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศของโรงพยาบาลศรีนครเป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง และภัยคุกคามต่างๆ โรงพยาบาลศรีนครจึงเห็นสมควรกำหนด นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกากำหนด หลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐ ต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและ เชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร โรงพยาบาลศรีนคร เห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ นโยบายในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลศรีนคร มีวัตถุประสงค์ ดังต่อไปนี้

๑.๑.เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการ สื่อสาร หรือเครือข่ายคอมพิวเตอร์ของโรงพยาบาลศรีนครให้เป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒.เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการ สื่อสารของโรงพยาบาลศรีนครอ้างอิงตามมาตรฐาน ISO/IEC27001 และมีการปรับปรุงอย่างต่อเนื่อง

๑.๓.เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร ข้าราชการ เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานร่วมกับโรงพยาบาลศรีนครตระหนักถึงความสำคัญของการรักษา ความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลศรีนครในการดำเนินงานและถือปฏิบัติตามอย่างเคร่งครัด

๑.๔.เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๑.๕.เพื่อเผยแพร่และส่งเสริมให้กับข้าราชการ เจ้าหน้าที่ บุคลากรทุกระดับ ในโรงพยาบาลศรีนคร มีความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และถือปฏิบัติอย่างเคร่งครัด

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลศรีนคร กำหนดประเด็นสำคัญดังต่อไปนี้

๒.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๒.๑.๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๒.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๒.๑.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒.๑.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒.๑.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ

๒.๑.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control

๒.๑.๘ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑.๙ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑.๑๐ การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room)

๒.๑.๑๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๒.๑.๑๒ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๒.๑.๑๓ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

๒.๑.๑๔ การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)

๒.๑.๑๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๒.๑.๑๖ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๒.๒ ระบบสารสนเทศและระบบสำรองของสารสนเทศ

๒.๒.๑ การสำรองข้อมูลและระบบคอมพิวเตอร์

๒.๒.๒ การกู้คืนระบบ

๒.๒.๓ การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายโรงพยาบาลศรีนคร

๒.๒.๔ การบริหารจัดการการเข้าถึงระบบเครือข่าย

๒.๒.๕ การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๒.๒.๖ การบริหารจัดการการบันทึกและตรวจสอบ

๒.๒.๗ การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์เทคโนโลยีสารสนเทศ

๒.๒.๘ การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๒.๒.๙ การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ (Third Party Access Control)

๒.๒.๑๐ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๓ แผนเตรียมความพร้อมกรณีฉุกเฉิน มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถปรับใช้ได้อย่างเหมาะสม อย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งมีการกำหนดขั้นตอนการดำเนินงานและผู้รับผิดชอบอย่างชัดเจน

๒.๔ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีการตรวจสอบจากผู้ตรวจสอบภายในหน่วยงานและจากภายนอก อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒.๕ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของโรงพยาบาลศรีนคร อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

ข้อ ๓ ให้ถือปฏิบัติตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลศรีนคร พ.ศ.๒๕๖๖ ตามที่แนบท้ายประกาศนี้

จึงประกาศมาเพื่อทราบและถือปฏิบัติอย่างเคร่งครัด

ประกาศ ณ วันที่ 4 มกราคม พ.ศ. ๒๕๖๖

(นายพงศธร เหลือหลาย)
ผู้อำนวยการโรงพยาบาลศรีนคร