ประกาศโรงพยาบาลวัฒนานคร

เรื่อง นโยบายและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลวัฒนานคร เป็นไปอย่างราบรื่นเหมาะสมและมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง ทั้งยังป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและป้องกันการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลวัฒนานครและหน่วยงานภายในสังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติมรวมถึงกฎหมายอื่นที่เกี่ยวข้อง โรงพยาบาลวัฒนานครจึงเห็นสมควรกำหนดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศต่อไป

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงออกประกาศไว้ ดังต่อไปนี้

วัตถุประสงค์

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านระบบสารสนเทศของโรงพยาบาลวัฒนานคร ทำให้การดำเนินการมีประสิทธิภาพและประสิทธิผล

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงาน โรงพยาบาลวัฒนานครได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับโรงพยาบาลวัฒนานคร ตระหนักถึงความสำคัญของระบบการรักษาความปลอดภัยในการใช้งานด้านสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

กำหนดประเด็นสำคัญ

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความปลอดภัยในระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวข้องกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดไว้อย่างเคร่งครัด

๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งานตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน

/เพื่อให้ผู้ใช้งาน...

เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้งานระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลการจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน และต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องการกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่ต้องการจะเข้าใช้งานลงบันทึกการเข้าใช้งาน (Login) โดยแสดงตัวตนของผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่สำนักงานสาธารณสุขจังหวัดสระแก้วจัดสรรไว้ และมีการออกแบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุมป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต กำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน กำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ตลอดจนมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ เพื่อไม่ได้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่างๆ

๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอพพลิเคชั่น กำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอพพลิเคชั่นต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) และระบบต่างๆ โดยต้องใช้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๑.๖ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ จัดทำระบบสารสนเทศและระบบสำรองข้อมูลที่เหมาะสมในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑.๗ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีล่ะ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

/๒.แนวปฏิบัติ...

๒. แนวปฏิบัติและข้อกำหนดการรักษาความมั่นคงและปลอดภัยสารสนเทศ เพื่อกำกับดูแลการดำเนินงานการบริหารจัดการระบบสาสนเทศให้มีความมั่นคงและปลอดภัย
ได้กำหนดเป็นแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ ดังนี้

๒.๑ แนวปฏิบัติด้านการควบคุมการเข้าถึงและควบคุมการใช้งาน

๒.๒ แนวปฏิบัติด้านการเข้าถึงผู้ใช้งาน

๒.๓ แนวปฏิบัติด้านการเข้าถึงระบบเครือข่าย

๒.๔ แนวปฏิบัติด้านการเข้าถึงระบบปฏิบัติการ

๒.๕ แนวปฏิบัติด้านการเข้าถึง Application และสารสนเทศ

๒.๖ แนวปฏิบัติด้านการจัดระบบสำรองกรณีฉุกเฉิน

๓. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๔. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงและปลอดภัยด้านสารสนเทศตามที่แนบประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑๙ กุมภาพันธ์ พ.ศ. ๒๕๖๑

(นายสุขุม พิริยะพรพิพัฒน์)
นายแพทย์ชำนาญการพิเศษ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลวัฒนานคร