ประกาศ โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ ๑๗

เรื่อง ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศโรงพยาบาล

(สำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ)

เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเป็นไปอย่างมั่นคงปลอดภัย มีประสิทธิภาพ และสอดคล้องกับพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง จึงกำหนดระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศโรงพยาบาล (ฉบับผู้ดูแลระบบเทคโนโลยีสารสนเทศ) เพื่อให้ถือปฏิบัติ ดังต่อไปนี้

ข้อ ๑ ขอบเขตการบังคับใช้

ระเบียบนี้ให้ใช้บังคับกับเจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ และบุคคลอื่นใดที่ได้รับมอบหมายให้มีหน้าที่ดูแล บริหารจัดการ หรือควบคุมระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์คอมพิวเตอร์ และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

ข้อ ๒ การควบคุมการเข้าถึงระบบสารสนเทศ

(๑) ต้องกำหนดสิทธิ์การเข้าถึงระบบตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) และหลักการให้สิทธิ์น้อยที่สุด (Least Privilege)

(๒) ต้องดำเนินการสร้าง แก้ไข ระงับ หรือยกเลิกบัญชีผู้ใช้งานตามคำขอที่ได้รับอนุมัติ

(๓) ต้องเพิกถอนสิทธิ์ทันทีเมื่อผู้ใช้งานพ้นสภาพหรือเปลี่ยนหน้าที่

(๔) ต้องทบทวนสิทธิ์ผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓ การบริหารจัดการระบบเครือข่ายและโครงสร้างพื้นฐาน

(๑) ต้องควบคุมและบริหารจัดการการเชื่อมต่อเครือข่าย และอุปกรณ์กระจายสัญญาณอย่างเหมาะสม

(๒) ต้องจัดให้มีมาตรการป้องกันเครือข่าย เช่น Firewall, IPS/IDS หรือเทียบเท่า

(๓) ต้องมีการเฝ้าระวัง ตรวจสอบ และวิเคราะห์พฤติกรรมการใช้งานเครือข่าย

(๔) ต้องมีการแบ่งแยกเครือข่ายสำหรับระบบสำคัญตามระดับความเสี่ยง

ข้อ ๔ การบริหารจัดการระบบและซอฟต์แวร์

(๑) ต้องปรับปรุงระบบและซอฟต์แวร์ให้เป็นเวอร์ชันที่ปลอดภัยอย่างสม่ำเสมอ

(๒) ต้องควบคุมการติดตั้งซอฟต์แวร์ โดยอนุญาตเฉพาะที่ได้รับอนุมัติ

(๓) ต้องมีการควบคุมการเปลี่ยนแปลง Change Management) และบันทึกการเปลี่ยนแปลงทุกครั้ง

(๔) ห้ามใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์

ข้อ ๕...

ข้อ ๕ การบริหารจัดการข้อมูลและการสำรองข้อมูล

(๑) ต้องสำรองข้อมูลระบบสำคัญตามรอบระยะเวลาที่กำหนด

(๒) ต้องจัดเก็บข้อมูลสำรองอย่างปลอดภัยและเหมาะสม

(๓) ต้องมีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

(๔) การเข้าถึงข้อมูลผู้ป่วยต้องเป็นไปตามสิทธิ์ และสามารถตรวจสอบย้อนหลังได้

ข้อ ๖ การบันทึกและเฝ้าระวังเหตุการณ์

(๑) ต้องจัดเก็บ Log ของระบบสำคัญไม่น้อยกว่า ๙๐ วัน หรือเป็นไปตามที่กฎหมายกำหนด

(๒) ต้องมีการตรวจสอบและวิเคราะห์เหตุการณ์ผิดปกติอย่างสม่ำเสมอ

(๓) ต้องมีมาตรการป้องกันการแก้ไขหรือทำลาย Log โดยมิชอบ

ข้อ ๗ การจัดการเหตุการณ์และความต่อเนื่องของระบบ

(๑) ต้องดำเนินการตรวจสอบ วิเคราะห์ และจำกัดผลกระทบทันทีเมื่อเกิดเหตุการณ์

(๒) ต้องรายงานเหตุการณ์ตามลำดับขั้นและภายในระยะเวลาที่กำหนด

(๓) ต้องดำเนินการแก้ไข ฟื้นฟู และป้องกันการเกิดซ้ำ

(๓) ต้องจัดให้มีแผนรองรับเหตุฉุกเฉินด้านเทคโนโลยีสารสนเทศและทดสอบอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๘ การควบคุมทรัพย์สินและความมั่นคงปลอดภัยด้านกายภาพ

(๑) ต้องจัดทำทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน

(๒) ต้องควบคุมการเข้าถึงพื้นที่สำคัญ เช่น ห้อง Data Center เป็นต้น

(๓) ต้องจัดให้มีระบบสนับสนุนด้านสิ่งแวดล้อม เช่น UPS และระบบป้องกันอัคคีภัย เป็นต้น

ข้อ ๑๓ การบังคับใช้ระเบียบ

ผู้ดูแลระบบหรือผู้ที่เกี่ยวข้องต้องปฏิบัติตามระเบียบนี้อย่างเคร่งครัด กรณีไม่ปฏิบัติตามให้ผู้บังคับบัญชาพิจารณาดำเนินการตามลำดับขั้น ได้แก่ การแจ้งเตือน การปรับปรุงแก้ไข และหากยังไม่ดำเนินการหรือก่อให้เกิดความเสียหาย อาจพิจารณาดำเนินการทางวินัย และ/หรือทางกฎหมาย ตามความเหมาะสมของกรณี

ทั้งนี้ ให้ระเบียบนี้มีผลบังคับใช้ตั้งแต่วันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๒๖ มีนาคม พ.ศ. ๒๕๖๙

(นายจิรภัทร กัลยาณพจน์พร)

ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗