ประกาศโรงพยาบาลสองแคว

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

.....

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานมีความเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง

เพื่อให้การดำเนินงานด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสองแคว เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถสนับสนุนการให้บริการประชาชนได้อย่างต่อเนื่อง และเพื่อป้องกันความเสี่ยงที่อาจเกิดจากการใช้งานระบบสารสนเทศที่ไม่ถูกต้อง การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล หรือภัยคุกคามที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

โรงพยาบาลสองแคว จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อใช้เป็นแนวทางในการบริหารจัดการ ควบคุม ดูแล และป้องกันระบบสารสนเทศ ข้อมูล อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบงานที่เกี่ยวข้อง ให้มีความมั่นคงปลอดภัย ดังต่อไปนี้

๑. การกำหนดประเภทข้อมูลและผู้รับผิดชอบข้อมูล

โรงพยาบาลสองแควกำหนดประเภทข้อมูลสำคัญของโรงพยาบาล และกำหนดหน่วยงานหลักหรือผู้รับผิดชอบในการดูแล อนุญาต และควบคุมการเข้าถึงข้อมูลแต่ละประเภท ดังนี้

๑.๑ ข้อมูลผู้ป่วย: หน่วยงานหลัก คือ ห้องบัตรและเวชระเบียน

๑.๒ ข้อมูลบุคลากรโรงพยาบาล: หน่วยงานหลัก คือ ฝ่ายบริหารงานทั่วไป/งานบุคลากร

๑.๓ ข้อมูลการเงินและบัญชี: หน่วยงานหลัก คือ ฝ่ายบริหารงานทั่วไป/งานการเงินและบัญชี

๑.๔ ข้อมูลทางการรักษาพยาบาล: หน่วยงานหลัก คือ แพทย์ พยาบาล และเวชระเบียน

๑.๕ ข้อมูลทางการบริหาร: หน่วยงานหลัก คือ ฝ่ายบริหารงานทั่วไป

๑.๖ ข้อมูลการจราจรทางคอมพิวเตอร์และข้อมูลระบบสารสนเทศ: หน่วยงานหลัก คือ งานเทคโนโลยีสารสนเทศ

๒. การกำหนดพื้นที่ควบคุมด้านสารสนเทศ

โรงพยาบาลสองแควกำหนดพื้นที่ที่เกี่ยวข้องกับข้อมูลสำคัญ ระบบสารสนเทศ และอุปกรณ์เทคโนโลยีสารสนเทศ ให้เป็นพื้นที่ควบคุม โดยอนุญาตให้เฉพาะผู้ปฏิบัติงานที่เกี่ยวข้องเข้าออกได้ บุคคลอื่นต้องได้รับอนุญาตจากผู้รับผิดชอบหลักก่อนทุกครั้ง ได้แก่

๒.๑ ห้องเก็บเวชระเบียนผู้ป่วยนอก: ผู้รับผิดชอบหลัก คือ งานผู้ป่วยนอก/เวชระเบียน

๒.๒ ห้องเก็บเวชระเบียนผู้ป่วยใน: ผู้รับผิดชอบหลัก คือ กลุ่มงานประกันสุขภาพ ยุทธศาสตร์ และสารสนเทศทางการแพทย์

๒.๓ ห้องเก็บเอกสารทางการเงินและบัญชี: ผู้รับผิดชอบหลัก คือ ฝ่ายบริหารงานทั่วไป/งานการเงินและบัญชี

๒.๔ ห้องติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย: ผู้รับผิดชอบหลัก คือ ผู้ดูแลระบบ/งานเทคโนโลยีสารสนเทศ

๒.๕ ห้องเก็บอุปกรณ์สำรองคอมพิวเตอร์และอุปกรณ์สารสนเทศ: ผู้รับผิดชอบหลัก คือ ผู้ดูแลระบบ/งานเทคโนโลยีสารสนเทศ

๓. การกำหนดระดับชั้นความลับของข้อมูล

โรงพยาบาลสองแควกำหนดระดับชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้การเข้าถึง ใช้งาน เปิดเผย และจัดเก็บข้อมูลเป็นไปอย่างเหมาะสม ดังนี้

๓.๑ ข้อมูลลับ: เป็นข้อมูลที่อนุญาตให้เฉพาะผู้มีหน้าที่เกี่ยวข้องโดยตรงหรือผู้ได้รับอนุญาตเท่านั้นเข้าถึง เช่น ข้อมูลผู้ป่วยเฉพาะโรค ข้อมูลด้านวินัยหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว

๓.๒ ข้อมูลใช้ภายในเท่านั้น: เป็นข้อมูลที่ใช้ภายในหน่วยงานหรือภายในโรงพยาบาล เช่น ข้อมูลผู้ป่วย ข้อมูลทางการรักษา ข้อมูลการเงินและบัญชี และข้อมูลการบริหารภายใน

๓.๓ ข้อมูลส่วนบุคคล: เป็นข้อมูลที่เกี่ยวข้องกับบุคคล ซึ่งต้องได้รับการคุ้มครองและใช้งานตามความจำเป็น เช่น ข้อมูลบุคลากร ข้อมูลผู้รับบริการ บัญชีผู้ใช้งาน และรหัสผ่านประจำตัว

๓.๔ ข้อมูลเปิดเผยได้: เป็นข้อมูลที่สามารถเผยแพร่ได้โดยไม่กระทบต่อความมั่นคงปลอดภัยของโรงพยาบาล หรือสิทธิของบุคคล เช่น ข้อมูลประชาสัมพันธ์ ข้อมูลวิชาการทั่วไป หรือข้อมูลสถานการณ์โรคที่ได้รับอนุญาตให้เผยแพร่

๔. การเข้าถึงข้อมูลและระบบสารสนเทศ

๔.๑ กำหนดให้ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย เป็นผู้บริหารจัดการ ตรวจสอบ อนุมัติ และกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ใช้งาน ตามหน้าที่ความรับผิดชอบและความจำเป็นในการปฏิบัติงาน

๔.๒ ผู้ใช้งานที่ต้องการใช้งานระบบสารสนเทศของโรงพยาบาล เช่น ระบบสารสนเทศโรงพยาบาล HOSxP ระบบเครือข่าย หรือระบบงานอื่นที่เกี่ยวข้อง ต้องได้รับบัญชีผู้ใช้งานและรหัสผ่านจากผู้ดูแลระบบ

๔.๓ ผู้ใช้งานต้องรักษาบัญชีผู้ใช้งานและรหัสผ่านของตนเอง ห้ามเปิดเผย ให้ยืม หรืออนุญาตให้บุคคลอื่นใช้งานบัญชีของตนโดยเด็ดขาด

๔.๔ สิทธิ์การใช้งานต้องเป็นไปตามบทบาทหน้าที่ของผู้ใช้งาน โดยแบ่งเป็น:

- ผู้ใช้งานทั่วไป สามารถเข้าถึง บันทึก แก้ไข หรือใช้งานข้อมูลได้ตามสิทธิ์ที่ได้รับมอบหมายเท่านั้น
- ผู้ดูแลระบบ สามารถบริหารจัดการระบบ กำหนดสิทธิ์ ตรวจสอบการใช้งาน แก้ไขปัญหาระบบ และดำเนินการในระดับฐานข้อมูลหรือระบบงานตามภารกิจที่ได้รับมอบหมาย

๔.๕ เมื่อผู้ใช้งานย้ายหน่วยงาน เปลี่ยนหน้าที่ ลาออก หรือพ้นจากหน้าที่ ต้องมีการปรับปรุง ระงับ หรือยกเลิกสิทธิ์การใช้งานโดยเร็ว เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕. การใช้เครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศ

๕.๑ เครื่องคอมพิวเตอร์แม่ข่าย

๕.๑.๑ เครื่องคอมพิวเตอร์แม่ข่ายต้องติดตั้งอยู่ในพื้นที่ควบคุม มีการปิดล็อก จำกัดการเข้าออก และดูแลสภาพแวดล้อมให้เหมาะสมต่อการทำงานของอุปกรณ์

๕.๑.๒ กำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบดูแล ตรวจสอบ บำรุงรักษา และปรับปรุงเครื่องคอมพิวเตอร์แม่ข่ายให้สามารถใช้งานได้อย่างมั่นคง ปลอดภัย และมีประสิทธิภาพ

๕.๑.๓ ห้ามบุคคลที่ไม่เกี่ยวข้องเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบหรือผู้มีอำนาจอนุมัติ

๕.๒ เครื่องคอมพิวเตอร์สำนักงานและคอมพิวเตอร์พกพา

๕.๒.๑ เครื่องคอมพิวเตอร์ของโรงพยาบาลต้องมีการกำหนดหมายเลข IP หรือข้อมูลประจำเครื่องตามความเหมาะสม และมีการลงทะเบียนควบคุมไว้โดยงานเทคโนโลยีสารสนเทศ

๕.๒.๒ ห้ามผู้ใช้งานเปลี่ยนแปลงหมายเลข IP การตั้งค่าระบบ หรือการตั้งค่าเครือข่ายของเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

๕.๒.๓ ห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน โปรแกรมละเมิดลิขสิทธิ์ หรือโปรแกรมที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๕.๒.๔ ผู้ใช้งานต้องระมัดระวังการใช้งานสื่อบันทึกข้อมูลภายนอก เช่น USB Flash Drive, External Hard Disk หรืออุปกรณ์อื่น ๆ และควรตรวจสอบไวรัสหรือมัลแวร์ก่อนใช้งานทุกครั้ง

๖. การใช้งานอินเทอร์เน็ตและระบบเครือข่ายไร้สาย

๖.๑ โรงพยาบาลไม่อนุญาตให้อุปกรณ์ภายนอกเชื่อมต่อระบบเครือข่ายของโรงพยาบาลได้อย่างอิสระ เว้นแต่ได้รับอนุญาตเป็นกรณีไป

๖.๒ กรณีเจ้าหน้าที่มีความจำเป็นต้องนำอุปกรณ์ส่วนตัวหรืออุปกรณ์ภายนอกมาเชื่อมต่อระบบเครือข่ายของโรงพยาบาล ต้องแจ้งผู้ดูแลระบบเพื่อพิจารณาอนุญาตและกำหนดสิทธิ์การใช้งานตามความเหมาะสม

๖.๓ กรณีผู้รับบริการหรือบุคคลภายนอกมีความประสงค์จะใช้งานเครือข่ายไร้สายของโรงพยาบาล ต้องติดต่อผู้รับผิดชอบหรือผู้ดูแลระบบ เพื่อขอรับสิทธิ์การใช้งานตามระยะเวลาที่กำหนด

๖.๔ ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและระบบเครือข่ายของโรงพยาบาลเพื่อประโยชน์ในการปฏิบัติงานราชการ การให้บริการ หรือภารกิจของโรงพยาบาลเท่านั้น และต้องไม่ใช้งานในลักษณะที่ผิดกฎหมายหรือก่อให้เกิดความเสียหายต่อโรงพยาบาล

๗. การรักษาความปลอดภัยของระบบเครือข่ายและระบบป้องกันภัยคุกคาม

๗.๑ กำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ดำเนินการติดตั้ง กำหนดค่า และดูแลระบบป้องกันภัยคุกคาม เช่น Firewall ระบบป้องกันไวรัส หรือมาตรการควบคุมการเชื่อมต่อเครือข่าย ตามความเหมาะสม

๗.๒ การเชื่อมต่ออินเทอร์เน็ตหรือระบบเครือข่ายที่ไม่เป็นไปตามนโยบาย หรือมีความเสี่ยงต่อความมั่นคงปลอดภัย อาจถูกจำกัด ระงับ หรือบล็อกการใช้งาน

๗.๓ ผู้ดูแลระบบมีสิทธิ์ระงับหรือจำกัดการใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่มีพฤติกรรมเสี่ยง เช่น ติดไวรัส ใช้งานผิดวัตถุประสงค์ เข้าถึงระบบโดยไม่ได้รับอนุญาต หรืออาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศของโรงพยาบาล จนกว่าจะได้รับการแก้ไข

๘. การสำรองข้อมูลและการกู้คืนข้อมูล

๘.๑ โรงพยาบาลต้องจัดให้มีการสำรองข้อมูลสำคัญของระบบสารสนเทศอย่างสม่ำเสมอ โดยกำหนดผู้รับผิดชอบในการดำเนินการ ตรวจสอบ และติดตามผลการสำรองข้อมูล

๘.๒ ข้อมูลสำรองต้องจัดเก็บไว้ในพื้นที่หรือระบบที่ปลอดภัย สามารถนำกลับมาใช้ได้เมื่อเกิดเหตุขัดข้อง เช่น ระบบเสียหาย ข้อมูลสูญหาย หรือเกิดเหตุฉุกเฉิน

๘.๓ ข้อมูลสำคัญที่อยู่ในรูปแบบเอกสาร เช่น ข้อมูลเวชระเบียน ข้อมูลการเงินและบัญชี หรือเอกสารราชการสำคัญ ต้องจัดเก็บในพื้นที่ที่เหมาะสม มีการจำกัดการเข้าถึง และมีกระบวนการทำลายเอกสารตามระเบียบที่เกี่ยวข้อง

๘.๔ กรณีข้อมูลของผู้ใช้งานถูกลบ สูญหาย หรือเสียหาย ให้แจ้งผู้ดูแลระบบเพื่อพิจารณาดำเนินการกู้คืน ทั้งนี้ ความสมบูรณ์ของข้อมูลที่กู้คืนได้ขึ้นอยู่กับรอบการสำรองข้อมูลและสภาพความเสียหายที่เกิดขึ้น

๙. ระบบกล้องวงจรปิด

๙.๑ กำหนดให้เจ้าหน้าที่ที่ได้รับมอบหมายเป็นผู้ดูแล บำรุงรักษา และตรวจสอบความพร้อมใช้งานของระบบกล้องวงจรปิดของโรงพยาบาล

๙.๒ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเป็นผู้กำหนดสิทธิ์การเข้าถึงระบบกล้องวงจรปิด โดยต้องเป็นไปตามความจำเป็นและได้รับความเห็นชอบจากผู้บริหารหรือผู้มีอำนาจที่เกี่ยวข้อง

๙.๓ การขอดูหรือขอข้อมูลจากระบบกล้องวงจรปิด ต้องมีการบันทึกคำขอหรือกรอกแบบฟอร์มการขอดูข้อมูล และต้องได้รับอนุมัติจากผู้อำนวยการโรงพยาบาลหรือผู้ที่ได้รับมอบหมาย ทั้งนี้ ให้พิจารณาตามเหตุการณ์และความจำเป็นเป็นกรณีไป

๑๐. การปฏิบัติตามนโยบาย

บุคลากรทุกระดับของโรงพยาบาลสองแคว รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของโรงพยาบาล ต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด หากมีการฝ่าฝืนหรือกระทำการที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ข้อมูล หรือชื่อเสียงของโรงพยาบาล อาจถูกพิจารณาดำเนินการตามระเบียบ วินัย หรือกฎหมายที่เกี่ยวข้อง

จึงประกาศมาให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ เมษายน พ.ศ. ๒๕๖๙

(ลงชื่อ) กลพล

(นายกุลพล ตั้งรัตนาพิบูล)

ผู้อำนวยการโรงพยาบาลสองแคว