แนวปฏิบัติการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านสารสนเทศ โรงพยาบาลสองแคว จังหวัดน่าน

Risk Assessment and Risk Management Strategy Procedure

.....

โรงพยาบาลสองแควมีการนำระบบเทคโนโลยีสารสนเทศมาใช้สนับสนุนการให้บริการประชาชน การบริหารจัดการข้อมูลสุขภาพ การเชื่อมโยงข้อมูลกับหน่วยงานภายนอก และการดำเนินงานตามนโยบาย Smart Hospital ของกระทรวงสาธารณสุข ส่งผลให้ระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย ฐานข้อมูล และบุคลากรผู้ใช้งานระบบ เป็นทรัพย์สินสารสนเทศที่มีความสำคัญต่อความต่อเนื่องของบริการสุขภาพ

ดังนั้น โรงพยาบาลสองแคว จึงกำหนดแนวปฏิบัติการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านสารสนเทศ เพื่อให้มีการระบุ วิเคราะห์ ประเมิน จัดลำดับ และควบคุมความเสี่ยงอย่างเป็นระบบ ครอบคลุมทรัพย์สินสารสนเทศที่อยู่ภายใต้การให้บริการของโรงพยาบาล และสอดคล้องกับเกณฑ์ HS๔ ด้านที่ ๙ การรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อ ๙.๒.๑ ซึ่งกำหนดให้หน่วยงานมีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศ โดยการมีส่วนร่วมของผู้เกี่ยวข้องทุกฝ่าย

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดแนวทางการประเมินความเสี่ยงด้านสารสนเทศของโรงพยาบาลสองแควอย่างเป็นระบบ

๑.๒ เพื่อให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น ระบบ HIS, Server, Network, Database, Gateway, เครื่องคอมพิวเตอร์ และข้อมูลผู้ป่วย ได้รับการประเมินความเสี่ยงอย่างเหมาะสม

๑.๓ เพื่อจัดลำดับความสำคัญของความเสี่ยงตามระดับโอกาสเกิดและผลกระทบ

๑.๔ เพื่อกำหนดมาตรการควบคุม ป้องกัน ลดผลกระทบ และติดตามความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๑.๕ เพื่อใช้เป็นหลักฐานประกอบการดำเนินงานตามเกณฑ์ HS๔ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ขอบเขตการดำเนินงาน

แนวปฏิบัตินี้ครอบคลุมระบบสารสนเทศและทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการให้บริการของโรงพยาบาลสองแคว ได้แก่

๒.๑ ระบบสารสนเทศโรงพยาบาล เช่น HOSxP, HOSxP XE, ระบบ Lab, ระบบ X-ray, ระบบการเงิน และระบบสนับสนุนบริการ

๒.๒ เครื่องแม่ข่าย ระบบฐานข้อมูล ระบบสำรองข้อมูล และระบบเสมือน

๒.๓ ระบบเครือข่าย อุปกรณ์ Firewall, Switch, Router, Wireless และ Internet

๒.๔ เครื่องคอมพิวเตอร์ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงของหน่วยงาน

๒.๕ ระบบ Gateway หรือเครื่องที่ใช้เชื่อมต่อกับระบบภายนอก

๒.๖ บัญชีผู้ใช้งาน สิทธิ์การเข้าถึง และรหัสผ่าน

๒.๗ ข้อมูลผู้ป่วย ข้อมูลบุคลากร ข้อมูลทางการเงิน และข้อมูลสำคัญของโรงพยาบาล

๒.๘ บุคลากร ผู้ดูแลระบบ ผู้ใช้งานระบบ และผู้เกี่ยวข้องภายนอก

๓. นิยาม

ความเสี่ยงด้านสารสนเทศ หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อความลับ ความถูกต้อง ความพร้อมใช้งาน หรือความต่อเนื่องของระบบสารสนเทศของโรงพยาบาล

ทรัพย์สินสารสนเทศ หมายถึง ข้อมูล ระบบ โปรแกรม อุปกรณ์ บุคลากร กระบวนงาน และเอกสารที่เกี่ยวข้องกับการจัดเก็บ ประมวลผล รับส่ง หรือใช้งานข้อมูลสารสนเทศของโรงพยาบาล

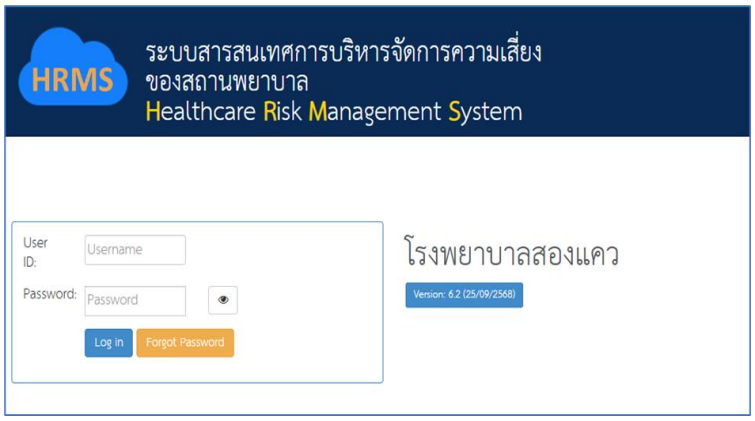
การประเมินความเสี่ยง หมายถึง กระบวนการระบุ วิเคราะห์ และให้คะแนนความเสี่ยง โดยพิจารณาจากโอกาสเกิดและผลกระทบ เพื่อจัดลำดับความสำคัญและกำหนดมาตรการควบคุม

การจัดการความเสี่ยง หมายถึง การกำหนดแนวทางตอบสนองต่อความเสี่ยง เช่น การหลีกเลี่ยง การยอมรับ การควบคุมหรือลดความเสี่ยง และการถ่ายโอนความเสี่ยง

๔. ระบบสนับสนุนการบริหารจัดการความเสี่ยงของโรงพยาบา

โรงพยาบาลสองแควใช้ระบบ HRMS: Healthcare Risk Management System เพื่อบันทึก ติดตาม ประเมิน และรายงานข้อมูลความเสี่ยงของหน่วยงาน โดยระบบดังกล่าวช่วยให้สามารถรวบรวมข้อมูลเหตุการณ์ความเสี่ยง วิเคราะห์ระดับความรุนแรง ติดตามสถานะการดำเนินการ และสรุปภาพรวมความเสี่ยงของโรงพยาบาลได้อย่างเป็นระบบ

ภาพที่ ๑ หน้าจอเข้าสู่ระบบ HRMS ของโรงพยาบาลสองแคว



คำอธิบาย: ภาพแสดงหน้าจอเข้าสู่ระบบ HRMS ของโรงพยาบาลสองแคว ซึ่งเป็นระบบสารสนเทศสำหรับบริหารจัดการความเสี่ยงของสถานพยาบาล ผู้ใช้งานสามารถเข้าสู่ระบบด้วยบัญชีผู้ใช้และรหัสผ่าน เพื่อบันทึกเหตุการณ์ความเสี่ยง ตรวจสอบรายการที่เกี่ยวข้อง และติดตามผลการจัดการความเสี่ยงภายในโรงพยาบาล

ภาพที่ ๒ หน้าจอ Dashboard สถิติและรายงานความเสี่ยงในระบบ HRMS

คำอธิบาย: ภาพแสดงหน้าจอ Dashboard ของระบบ HRMS ซึ่งใช้ติดตามข้อมูลความเสี่ยงในภาพรวม เช่น สถิติความเสี่ยงด้าน Patient Safety Goals, Personnel Safety Goals, Organization Safety Goals และ Specific Clinical Risk Incident โดยข้อมูลที่แสดงในรูปแบบกราฟช่วยให้ผู้บริหารและคณะกรรมการที่เกี่ยวข้องสามารถติดตามแนวโน้มความเสี่ยง จัดลำดับความสำคัญ และกำหนดมาตรการแก้ไขได้อย่างรวดเร็ว

๖. กระบวนการประเมินความเสี่ยงด้านสารสนเทศ

โรงพยาบาลสองแควกำหนดกระบวนการประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๖.๑ การจัดทำทะเบียนทรัพย์สินสารสนเทศ

หน่วยงานสารสนเทศร่วมกับหน่วยงานที่เกี่ยวข้องจัดทำบัญชีรายการทรัพย์สินสารสนเทศ เช่น ระบบงานสำคัญ เครื่องแม่ข่าย ฐานข้อมูล อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ โปรแกรม และข้อมูลสำคัญ พร้อมระบุเจ้าของทรัพย์สิน ผู้รับผิดชอบ และระดับความสำคัญของทรัพย์สิน

๖.๒ การระบุความเสี่ยง

ระบุเหตุการณ์หรือปัจจัยที่อาจส่งผลกระทบต่อทรัพย์สินสารสนเทศ เช่น ระบบล่ม ข้อมูลสูญหาย ไฟฟ้าดับ การโจมตีทางไซเบอร์ การติดไวรัส การตั้งค่าสิทธิ์ไม่เหมาะสม หรือการใช้งานระบบผิดพลาด

๖.๓ การวิเคราะห์ความเสี่ยง

วิเคราะห์ความเสี่ยงโดยพิจารณาจากประเด็นต่อไปนี้

๑. โอกาสเกิดเหตุการณ์

๒. ผลกระทบต่อการให้บริการ

๓. ผลกระทบต่อข้อมูลผู้ป่วย

๔. ผลกระทบต่อความต่อเนื่องของระบบ

๕. มาตรการควบคุมที่มีอยู่ในปัจจุบัน

๖.๔ การให้คะแนนความเสี่ยง

กำหนดคะแนนความเสี่ยงจากค่าระดับโอกาสเกิดและระดับผลกระทบ เพื่อจัดลำดับความสำคัญของความเสี่ยง

เกณฑ์การประเมินโอกาสเกิดและผลกระทบ

ระดับ	โอกาสเกิด	ผลกระทบ
๑	เกิดได้น้อยมาก	กระทบน้อย แก้ไขได้ภายในหน่วยงาน
๒	เกิดได้น้อย	กระทบต่อการทำงานบางส่วน
๓	เกิดได้ปานกลาง	กระทบต่อบริการหรือข้อมูลสำคัญ
๔	เกิดได้บ่อย	กระทบต่อหลายหน่วยงานหรือระบบสำคัญ
๕	เกิดได้สูงมาก	กระทบรุนแรงต่อบริการ ผู้ป่วย หรือข้อมูลสำคัญ

คะแนนความเสี่ยง = โอกาสเกิด × ผลกระทบ

คะแนนความเสี่ยง	ระดับความเสี่ยง	แนวทางดำเนินการ
๑–๔	ต่ำ	เฝ้าระวังและควบคุมตามปกติ
๕–๙	ปานกลาง	กำหนดมาตรการควบคุมเพิ่มเติม
๑๐–๑๖	สูง	จัดทำแผนลดความเสี่ยงและติดตามอย่างใกล้ชิด
๑๗–๒๕	สูงมาก	เร่งดำเนินการแก้ไข รายงานผู้บริหาร และติดตามต่อเนื่อง

๗. กลยุทธ์ในการจัดการความเสี่ยง

โรงพยาบาลสองแควกำหนดแนวทางตอบสนองต่อความเสี่ยง ๔ รูปแบบ ได้แก่

๗.๑ การหลีกเลี่ยงความเสี่ยง (Terminate)

ยกเลิกหรือหลีกเลี่ยงกิจกรรมที่มีความเสี่ยงสูง หากพิจารณาแล้วไม่คุ้มค่าต่อการดำเนินงาน หรืออาจก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างมีนัยสำคัญ

๗.๒ การยอมรับความเสี่ยง (Take)

ยอมรับความเสี่ยงที่อยู่ในระดับต่ำหรืออยู่ในเกณฑ์ที่หน่วยงานสามารถยอมรับได้ โดยยังคงมีการเฝ้าระวังและติดตามอย่างต่อเนื่อง

๗.๓ การควบคุมหรือลดความเสี่ยง (Treat)

กำหนดมาตรการควบคุมหรือลดความเสี่ยง เช่น การสำรองข้อมูล การกำหนดสิทธิ์ผู้ใช้งาน การติดตั้ง Antivirus/Firewall การจัดทำแผนรองรับเหตุขัดข้องด้านเทคโนโลยีสารสนเทศ และการอบรมผู้ใช้งาน

๗.๔ การถ่ายโอนความเสี่ยง (Transfer)

ถ่ายโอนหรือแบ่งความรับผิดชอบบางส่วน เช่น การทำสัญญาบำรุงรักษาอุปกรณ์ การรับประกันระบบ หรือการใช้บริการผู้เชี่ยวชาญภายนอก

๘. ตัวอย่างรายการความเสี่ยงด้านสารสนเทศของโรงพยาบาลสองแคว

ลำดับ	เหตุการณ์ความเสี่ยง	สาเหตุ/ปัจจัยเสี่ยง	มาตรการควบคุมปัจจุบัน	แนวทางเพิ่มเติม
๑	ระบบ HOSxP/HOSxP XE ไม่สามารถใช้งานได้	Server ขัดข้อง, Database มีปัญหา, Network ล่ม	มีผู้ดูแลระบบตรวจสอบและสำรองข้อมูล	จัดทำแผนกู้คืนระบบ และทดสอบ Restore เป็นระยะ
๒	ข้อมูลผู้ป่วยสูญหายหรือเสียหาย	ระบบฐานข้อมูลเสียหาย, Backup ไม่สมบูรณ์	มีการสำรองข้อมูล	กำหนดรอบตรวจสอบ Backup และจัดทำรายงานผล
๓	ผู้ใช้งานเข้าถึงข้อมูลเกินสิทธิ์	การกำหนดสิทธิ์ไม่เหมาะสม หรือใช้บัญชีร่วมกัน	มีบัญชีผู้ใช้งานรายบุคคล	ทบทวนสิทธิ์ผู้ใช้งานเป็นระยะ และยกเลิกบัญชีที่ไม่ใช้งาน
๔	เครื่องคอมพิวเตอร์ติดไวรัสหรือมัลแวร์	เปิดไฟล์แนบไม่ปลอดภัย ใช้ USB ไม่ทราบแหล่งที่มา	มีโปรแกรม Antivirus	อบรมผู้ใช้งาน และจำกัดการใช้อุปกรณ์ภายนอก
๕	ไฟฟ้าดับส่งผลต่อระบบ Server	ระบบไฟฟ้าขัดข้อง หรือ UPS ไม่เพียงพอ	มี UPS สำหรับอุปกรณ์สำคัญ	ตรวจสอบ UPS และจัดทำแผนรองรับไฟฟ้าขัดข้อง
๖	การโจมตีจากภายนอกระบบเครือข่าย	Firewall ตั้งค่าไม่เหมาะสม หรือมีช่องโหว่	มี Firewall ควบคุมการเชื่อมต่อ	ทบทวน Rule Firewall และติดตาม Log อย่างสม่ำเสมอ
๗	ระบบ Gateway หยุดทำงาน	Windows Update, เครื่อง Restart, ไม่มีผู้ Log in	มีผู้รับผิดชอบตรวจสอบ	ตั้งค่าควบคุมการ Restart และจัดทำทะเบียน Gateway
๘	บุคลากรขาดความเข้าใจด้าน Cybersecurity	ขาดการอบรมหรือแนวปฏิบัติที่ชัดเจน	มีการแจ้งแนวทางผ่านหน่วยงาน	จัดอบรม/ประชาสัมพันธ์เรื่องรหัสผ่าน PDPA และภัยไซเบอร์

๙. การมีส่วนร่วมของผู้เกี่ยวข้อง

การประเมินความเสี่ยงด้านสารสนเทศของโรงพยาบาลสองแคว ต้องดำเนินการโดยการมีส่วนร่วมของผู้เกี่ยวข้อง ได้แก่

๙.๑ ผู้บริหารโรงพยาบาล

๙.๒ กลุ่มงานสุขภาพดิจิทัล / งานเทคโนโลยีสารสนเทศ

๙.๓ คณะกรรมการบริหารความเสี่ยง

๙.๔ คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

๙.๕ หัวหน้ากลุ่มงาน / หัวหน้างาน

๙.๖ ผู้ใช้งานระบบสารสนเทศ

๙.๗ ผู้รับผิดชอบระบบงานสำคัญ

๙.๘ หน่วยงานภายนอกหรือผู้ให้บริการระบบ (กรณีเกี่ยวข้อง)

การมีส่วนร่วมดังกล่าวช่วยให้การประเมินความเสี่ยงครอบคลุมมุมมองทั้งด้านเทคนิค ด้านการให้บริการ ด้านข้อมูลผู้ป่วย และด้านการบริหารจัดการองค์กร

๑๐. การติดตาม ทบทวน และรายงานผล

๑๐.๑ งานเทคโนโลยีสารสนเทศดำเนินการติดตามความเสี่ยงด้านสารสนเทศอย่างต่อเนื่อง

๑๐.๒ ทบทวนทะเบียนทรัพย์สินสารสนเทศและผลการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสำคัญ

๑๐.๓ รายงานความเสี่ยงสำคัญต่อผู้บริหารและคณะกรรมการที่เกี่ยวข้อง

๑๐.๔ บันทึกเหตุการณ์ความเสี่ยงในระบบ HRMS หรือระบบที่โรงพยาบาลกำหนด

๑๐.๕ ติดตามผลการแก้ไข ป้องกัน และลดความเสี่ยงจนกว่าจะอยู่ในระดับที่ยอมรับได้

๑๐.๖ ใช้ผลการประเมินความเสี่ยงประกอบการวางแผนด้านงบประมาณ การจัดซื้อครุภัณฑ์ การพัฒนาระบบ และการอบรมบุคลากร

๑๑. สรุปความสอดคล้องกับ HS๔ หัวข้อ ๙.๒.๑

โรงพยาบาลสองแควมีแนวทางการดำเนินงานด้านการจัดการความเสี่ยงของระบบสารสนเทศ โดยมีองค์ประกอบสำคัญ ได้แก่

๑๑.๑ มีการกำหนดกระบวนการประเมินความเสี่ยงอย่างเป็นระบบ

๑๑.๒ มีการจัดทำหรือทบทวนทรัพย์สินสารสนเทศที่อยู่ภายใต้การให้บริการของโรงพยาบาล

๑๑.๓ มีการวิเคราะห์โอกาสเกิดและผลกระทบของความเสี่ยง

๑๑.๔ มีการให้คะแนนและจัดลำดับความสำคัญของความเสี่ยง

๑๑.๕ มีการกำหนดมาตรการควบคุมและกลยุทธ์ในการจัดการความเสี่ยง

๑๑.๖ มีการใช้ระบบ HRMS ในการบันทึก ติดตาม และรายงานข้อมูลความเสี่ยง

๑๑.๗ มีการมีส่วนร่วมของผู้บริหาร หน่วยงานสารสนเทศ และหน่วยงานผู้ใช้งาน

๑๑.๘ มีการติดตาม ทบทวน และรายงานผลอย่างต่อเนื่อง

จัดทำโดย .....

(นางสาวตรีรัตน์ ทนันชัย)

ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

วันที่ ๒๖ เดือน เมษายน พ.ศ. ๒๕๖๙

อนุมัติโดย .....

(นายกุลพล ตั้งรัตนาพิบูล)

ตำแหน่ง ผู้อำนวยการโรงพยาบาลสองแคว

วันที่ ๒๖ เดือน เมษายน พ.ศ. ๒๕๖๙