คู่มือวิเคราะห์ความเสี่ยง
ระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลสองแคว จังหวัดน่าน

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ฉบับสรุปความเสี่ยงด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

งานเทคโนโลยีสารสนเทศ / กลุ่มงานสุขภาพดิจิทัล

โรงพยาบาลสองแคว

คำนำ

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการวิเคราะห์ ประเมิน จัดลำดับและบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลสองแคว ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ โดยรวบรวมตัวอย่างประเด็นความเสี่ยงที่เคยใช้ประกอบการประเมิน ได้แก่ ระบบ HOSxP/HIS ใช้งานไม่ได้ ระบบสำรองข้อมูล การป้องกันมัลแวร์ การควบคุมสิทธิ์ การเปิดเผยข้อมูลผู้รับบริการ ระบบไฟฟ้า/UPS BCP/DRP, OS Patching, WAF, Log Management/SIEM, Software Patching, Network Segmentation, Licensed Software และการพัฒนาศักยภาพบุคลากรด้าน Cybersecurity/PDPA

การจัดทำเอกสารนี้ใช้กรณีอุบัติการณ์รหัส ๒๕๐๗๐๐๐๑๐๙ กรณี HOSxP ใช้งานไม่ได้ เป็นหลักฐานอ้างอิงสำคัญในการทบทวนความเสี่ยงจริง และเชื่อมโยงไปสู่การกำหนดมาตรการควบคุมเชิงป้องกัน การตอบสนองเหตุการณ์ และการติดตามผลอย่างต่อเนื่อง เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีความพร้อมใช้ ปลอดภัย และสนับสนุนการให้บริการผู้ป่วยได้อย่างมีประสิทธิภาพ

งานเทคโนโลยีสารสนเทศ/กลุ่มงานสุขภาพดิจิทัล โรงพยาบาลสองแคว หวังว่าเอกสารฉบับนี้จะเป็นหลักฐานประกอบการบริหารความเสี่ยงด้านสารสนเทศ และใช้เป็นแนวทางสำหรับการดำเนินงาน ติดตาม และทบทวนปรับปรุงแผนบริหารความเสี่ยงของโรงพยาบาลต่อไป

งานเทคโนโลยีสารสนเทศ / กลุ่มงานสุขภาพดิจิทัล

โรงพยาบาลสองแคว

สารบัญ

บทที่ ๑ การบริหารความเสี่ยง

๑.๑ ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และอาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของโรงพยาบาล ทั้งด้านการให้บริการผู้ป่วย ความพร้อมใช้ของระบบสารสนเทศ ความถูกต้องครบถ้วนของข้อมูล การรักษาความลับของข้อมูล และภาพลักษณ์ของหน่วยงาน

การประเมินความเสี่ยง (Risk Assessment) เป็นกระบวนการระบุความเสี่ยง วิเคราะห์โอกาสเกิดและผลกระทบ จัดระดับและจัดลำดับความสำคัญของความเสี่ยง เพื่อใช้กำหนดแผนควบคุม ลด หรือเฝ้าระวังความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้กำหนดมาตรการเพื่อลดโอกาสเกิดเหตุการณ์ หรือลดผลกระทบจากเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่โรงพยาบาลสามารถยอมรับได้ โดยมีการติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง

๑.๒ วัตถุประสงค์ของการบริหารจัดการความเสี่ยง

๑. เพื่อให้ระบบสารสนเทศหลักของโรงพยาบาล เช่น HOSxP, ระบบฐานข้อมูล, ระบบเครือข่าย และระบบสำรองข้อมูล มีความพร้อมใช้และสนับสนุนบริการผู้ป่วยได้ต่อเนื่อง

๒. เพื่อระบุ วิเคราะห์ และจัดลำดับความเสี่ยงด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลอย่างเป็นระบบ

๓. เพื่อกำหนดมาตรการควบคุม ลดความเสี่ยง ป้องกันอุบัติการณ์ซ้ำ และเตรียมความพร้อมเมื่อเกิดเหตุฉุกเฉิน

๔. เพื่อสนับสนุนการปฏิบัติตามมาตรฐาน HS๔/CTAM+ นโยบาย Cybersecurity และ PDPA

๕. เพื่อใช้เป็นหลักฐานประกอบการติดตาม รายงานผู้บริหาร และทบทวนปรับปรุงแผนประจำปี

๑.๓ ทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ทรัพยากร	รายละเอียด
ระบบงาน (Application System)	เช่น HOSxP/HIS, LIS, ระบบรายงาน, ระบบบริการออนไลน์ และระบบสนับสนุนงานบริหาร
เทคโนโลยี (Technology)	เครื่องแม่ข่าย เครื่องลูกข่าย ระบบปฏิบัติการ ฐานข้อมูล ระบบเครือข่าย Firewall, Switch, Wireless และอุปกรณ์สำรองไฟ
สถานที่และสิ่งอำนวยความสะดวก (Facilities)	ห้อง Server ห้อง IT ระบบไฟฟ้า เครื่องปรับอากาศ ระบบสำรองไฟ และพื้นที่จัดเก็บอุปกรณ์
บุคลากร (People)	เจ้าหน้าที่ IT ผู้ดูแลระบบ ผู้ใช้งานระบบ ผู้บริหาร และผู้เกี่ยวข้องกับข้อมูลสุขภาพ
ข้อมูล (Data)	ฐานข้อมูลผู้รับบริการ เวชระเบียน ข้อมูลการเงิน ข้อมูลบุคลากร เอกสารราชการ และ Log การใช้งานระบบ

๑.๔ ประเภทความเสี่ยงด้านสารสนเทศ

๑. ความเสี่ยงด้านเทคนิค

เกิดจากระบบคอมพิวเตอร์ โปรแกรม ฐานข้อมูล เครือข่าย อุปกรณ์ หรือภัยคุกคามไซเบอร์ เช่น Malware, ช่องโหว่, ระบบล่ม

๒. ความเสี่ยงด้านผู้ปฏิบัติงาน

เกิดจากการใช้งานระบบผิดวิธี การใช้สิทธิ์เกินหน้าที่ การเปิดเผยข้อมูล หรือขาดความตระหนักด้าน Cybersecurity/PDPA

๓. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน

เกิดจากไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อุปกรณ์เสียหาย เหตุขัดข้องร้ายแรง หรือเหตุการณ์ที่ทำให้ระบบหยุดชะงัก

๔. ความเสี่ยงด้านการบริหารจัดการ

เกิดจากนโยบาย แผนงาน งบประมาณ บุคลากร สัญญาบริการ หรือการกำกับติดตามที่ไม่เพียงพอ

บทที่ ๒ การวิเคราะห์ความเสี่ยง

๒.๑ เกณฑ์ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) เชิงคุณภาพ

ระดับ	โอกาสที่เกิด	คำอธิบาย
๕	สูงมาก	มีโอกาสเกิดขึ้นเป็นประจำ หรือเกิดซ้ำหลายครั้งในรอบปี
๔	สูง	มีโอกาสเกิดขึ้นบ่อยครั้ง
๓	ปานกลาง	มีโอกาสเกิดขึ้นบางครั้ง หรือเคยเกิดขึ้นจริงในหน่วยงาน/ระบบใกล้เคียง
๒	น้อย	มีโอกาสเกิดขึ้นน้อยครั้ง
๑	น้อยมาก	มีโอกาสเกิดขึ้นยาก หรือมีมาตรการควบคุมที่มั่นคง

๒.๒ เกณฑ์ระดับความรุนแรงของผลกระทบ (Impact) เชิงคุณภาพ

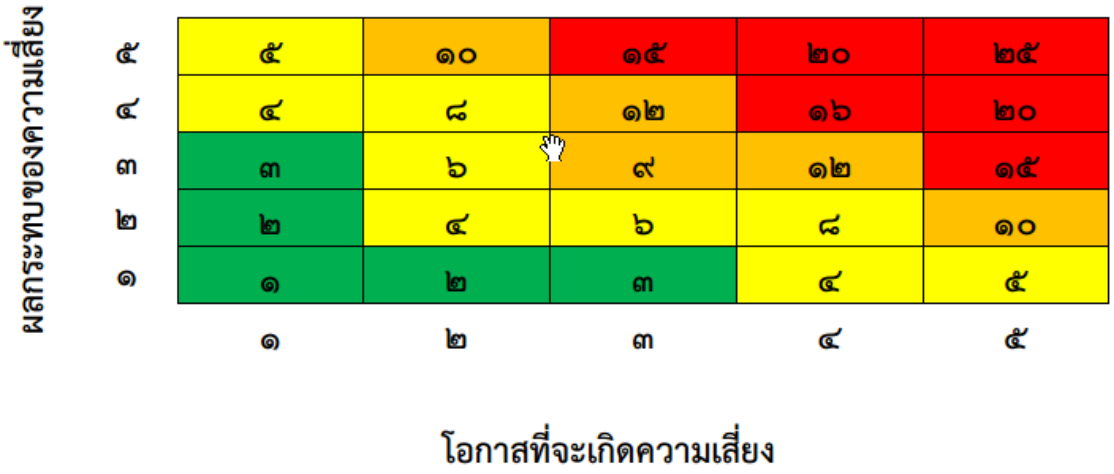
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	กระทบต่อบริการผู้ป่วย ระบบหลักหยุดชะงัก ข้อมูลสูญหาย/รั่วไหลรุนแรง หรือกระทบชื่อเสียงอย่างมาก
๔	สูง	กระทบหลายหน่วยงานหรือบริการสำคัญ ต้องใช้เวลาฟื้นฟู มีความเสียหายชัดเจน
๓	ปานกลาง	กระทบการทำงานบางส่วน มีงานล่าช้า แต่ยังมีวิธีสำรองหรือแก้ไขได้
๒	น้อย	กระทบเฉพาะจุด แก้ไขได้เร็ว ความเสียหายจำกัด
๑	น้อยมาก	กระทบน้อยมาก ไม่กระทบผู้รับบริการหรือระบบสำคัญ

๒.๓ ระดับของความเสี่ยง (Degree of Risk)

ระดับความเสี่ยงคำนวณจากผลคูณของระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) กับระดับความรุนแรงของผลกระทบ (Impact) โดยกำหนดเกณฑ์ ๔ ระดับ ดังนี้

ลำดับ	ระดับความเสี่ยง	ช่วงคะแนน	มาตรการกำหนด
๑	สูงมาก (Extreme Risk : E)	๑๕-๒๕ คะแนน	มีมาตรการลดและประเมินซ้ำ หรือถ่ายโอนความเสี่ยง
๒	สูง (High Risk : H)	๙-๑๔ คะแนน	มีมาตรการลดความเสี่ยงและติดตามใกล้ชิด
๓	ปานกลาง (Moderate Risk : M)	๔-๘ คะแนน	ยอมรับได้โดยมีมาตรการควบคุมและติดตาม
๔	น้อย (Low Risk : L)	๑-๓ คะแนน	ยอมรับความเสี่ยงและเฝ้าระวังตามปกติ

๒.๔ ตารางระดับความเสี่ยง (Degree of Risk)



๒.๕ ตารางที่ ๑ วิเคราะห์ความเสี่ยงระบบสารสนเทศ โรงพยาบาลสองแคว

สรุปประเด็นความเสี่ยงจากตัวอย่างที่เคยจัดทำและปรับเป็นรายการประเมินรวม โดยใช้อุบัติการณ์รหัส ๒๕๐๗๐๐๐๑๐๙ กรณี HOSxP ใช้งานไม่ได้ เป็นหลักฐานอ้างอิงหลักของความเสี่ยงด้านความพร้อมใช้ของระบบสารสนเทศ

ลำดับ	ประเด็นความเสี่ยง	ประเภท/สาเหตุสำคัญ	หลักฐาน/เหตุการณ์อ้างอิง	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับความเสี่ยง
๑	ระบบ HOSxP/HIS ไม่สามารถใช้งานได้เกิน ๓๐ นาที หรือข้อมูลให้บริการไม่พร้อมใช้	เทคนิค/บริการสำคัญ สาเหตุ: Server, Database, Network หรือโปรแกรม HOSxP ขัดข้อง ส่งผลต่อ OPD/IPD/ER/Lab/การเงิน	อุบัติการณ์รหัส ๒๕๐๗๐๐๐๑๐๙ กรณี HOSxP ใช้งานไม่ได้	๓	๕	๑๕ สูงมาก (E)	๑
๒	ระบบสำรองข้อมูลไม่ครอบคลุม หรือไม่สามารถกู้คืนข้อมูลได้ทันเวลา	เทคนิค/ข้อมูล สาเหตุ: Backup ไม่ครบจุด, ไม่มีการทดสอบ Restore, สื่อสำรองข้อมูลเสียหายหรือจัดเก็บไม่ปลอดภัย	รายการความเสี่ยง Backup ในชุด CTAM+/แผน IT	๓	๕	๑๕ สูงมาก (E)	๒
๓	การติดมัลแวร์/ไวรัส/คริปโตไมเนอร์ในเครื่องลูกข่ายหรือเครื่องแม่ข่าย	เทคนิค/ภัยคุกคามไซเบอร์ สาเหตุ: เครื่องไม่ได้อัปเดต Antivirus/EDR, เปิดไฟล์แนบ/เว็บเสี่ยง, ระบบปฏิบัติการเก่า	ตัวอย่าง Incident จาก CSM/NT Cyfence เช่น Ramnit, Sality, Monero Cryptocurrency Miner	๓	๔	๑๒ สูง (H)	๓
๔	การควบคุมสิทธิ์เข้าถึงระบบไม่เหมาะสม ทั้งเครือข่ายภายในและเครือข่ายสาธารณะ	ผู้ปฏิบัติงาน/การบริหารจัดการ สาเหตุ: User ใช้สิทธิ์เกินหน้าที่, ใช้รหัสผ่านร่วมกัน, ไม่ทบทวนสิทธิ์เมื่อย้ายงาน/ลาออก	รายการความเสี่ยง Access Control (Public และ Private)	๓	๔	๑๒ สูง (H)	๔

ลำดับ	ประเด็นความเสี่ยง	ประเภท/สาเหตุสำคัญ	หลักฐาน/เหตุการณ์อ้างอิง	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับความเสี่ยง
๕	การเปิดเผยข้อมูลผู้รับบริการหรือข้อมูลสุขภาพโดยไม่ได้รับอนุญาต	ข้อมูล/PDPA สาเหตุ: การเข้าถึงเวชระเบียนโดยไม่จำเป็น, ส่งข้อมูลผิดช่องทาง, เอกสารค้างบนโต๊ะ/เครื่องพิมพ์	รายการความเสี่ยงการเปิดเผยข้อมูลผู้รับบริการ/PDPA	๒	๕	๑๐ สูง (H)	๖
๖	กระแสไฟฟ้าขัดข้องหรือ UPS ไม่พร้อมใช้ ส่งผลให้อุปกรณ์ IT เสียหาย/ระบบหยุดชะงัก	ภัย/สถานการณ์ฉุกเฉิน สาเหตุ: ไฟตก ไฟดับ เครื่องสำรองไฟเสื่อม แบตเตอรี่หมดอายุ หรือเครื่องปั่นไฟไม่พร้อม	รายการความเสี่ยงระบบไฟฟ้า/UPS	๓	๔	๑๒ สูง (H)	๕
๗	แผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (BCP/DRP) ไม่พร้อมใช้งานจริง	บริหารจัดการ/สถานการณ์ฉุกเฉิน สาเหตุ: ไม่มีแผนลายลักษณ์อักษร ไม่กำหนด RTO/RPO ไม่เคยซ้อมแผน	รายการความเสี่ยง BCP/DRP ในชุด CTAM+	๒	๕	๑๐ สูง (H)	๗
๘	ระบบปฏิบัติการและเครื่องแม่ข่ายไม่ได้รับการ Patch ตามรอบ	เทคนิค สาเหตุ: OS หมดอายุ/ไม่มีแผน Patch/กลัวกระทบระบบงาน ทำให้มีช่องโหว่คงค้าง	รายการความเสี่ยง OS Patching	๓	๓	๙ สูง (H)	๙
๙	ระบบบันทึกเหตุการณ์ (Log Management/SIEM) ไม่ครอบคลุมหรือไม่ถูกติดตาม	เทคนิค/ตรวจจับเหตุการณ์ สาเหตุ: ไม่ได้รวบรวม Log จากอุปกรณ์สำคัญ หรือไม่มีผู้ติดตามแจ้งเตือนอย่างต่อเนื่อง	รายการความเสี่ยง Log Management/SIEM และรายงาน CSM	๓	๓	๙ สูง (H)	๑๐
๑๐	ระบบเว็บ/บริการสาธารณะไม่มีการป้องกัน Web Application ที่เพียงพอ	เทคนิค/Public Service สาเหตุ: เว็บไซต์หรือระบบออนไลน์ถูกสแกนช่องโหว่ โจมตี หรือถูกแก้ไขหน้าเว็บ	รายการความเสี่ยง WAF/Public-facing system	๒	๔	๘ ปานกลาง (M)	๑๑

ลำดับ	ประเด็นความเสี่ยง	ประเภท/สาเหตุสำคัญ	หลักฐาน/เหตุการณ์อ้างอิง	โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับความเสี่ยง
๑๑	Software/Application ไม่ได้รับการอัปเดตหรือ Patch ตามรอบ	เทคนิค สาเหตุ: โปรแกรมใช้งานเก่า ไม่มีผู้รับผิดชอบเวอร์ชัน หรือไม่ได้ติดตามประกาศช่องโหว่	รายการความเสี่ยง Software Update/Software Patching	๒	๓	๖ ปานกลาง (M)	๑๓
๑๒	โครงข่ายภายในไม่มีการแยกส่วนที่เหมาะสม (Network Segmentation)	เทคนิค/เครือข่าย สาเหตุ: เครื่องผู้ใช้ อุปกรณ์สำคัญ Server กล้องวงจรปิด/IoT อยู่ในเครือข่ายเดียวกัน ทำให้ลุกลามได้ง่าย	รายการความเสี่ยง Network Segmentation	๒	๔	๘ ปานกลาง (M)	๑๒
๑๓	การใช้ซอฟต์แวร์ไม่มีลิขสิทธิ์หรือไม่ถูกต้องตามเงื่อนไข	บริหารจัดการ/กฎหมาย สาเหตุ: จัดซื้อไม่ครอบคลุม ใช้งานโปรแกรมไม่ทราบแหล่งที่มา หรือไม่มีทะเบียน License	รายการความเสี่ยง Licensed Software	๒	๓	๖ ปานกลาง (M)	๑๔
๑๔	บุคลากร IT มีจำกัดหรือขาดทักษะเฉพาะด้าน ทำให้แก้ไขเหตุขัดข้องได้ล่าช้า	บุคลากร/บริหารจัดการ สาเหตุ: บุคลากรน้อย ภาระงานหลายระบบ และไม่มีผู้แทนสำรองในบางระบบ	รายการความเสี่ยงเจ้าหน้าที่ IT มีจำกัด/ขาดความรู้เฉพาะด้าน	๓	๓	๙ สูง (H)	๘
๑๕	บุคลากรทั่วไปขาดความตระหนักด้าน Cybersecurity และ PDPA	ผู้ปฏิบัติงาน/วัฒนธรรมความปลอดภัย สาเหตุ: ไม่เข้าใจการใช้รหัสผ่าน การเปิดเผยข้อมูล การคลิกลิงก์/ไฟล์แนบ และแนวทางแจ้งเหตุ	รายการความเสี่ยง Cybersecurity & PDPA Policy and Personnel Development	๒	๓	๖ ปานกลาง (M)	๑๕

๒.๖ ตารางที่ ๒ แผนบริหารความเสี่ยงด้านสารสนเทศ ประจำปีงบประมาณ ๒๕๖๙

ความเสี่ยงด้านการดำเนินงาน (ด้านเทคโนโลยีสารสนเทศ)

วัตถุประสงค์: เพื่อให้ระบบสารสนเทศของโรงพยาบาลพร้อมใช้งาน ปลอดภัย และสนับสนุนการให้บริการผู้ป่วยได้อย่างต่อเนื่อง

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ โอกาส x ผลกระทบ	แผนงาน/โครงการ/กิจกรรมรองรับการบริหารความเสี่ยง	ระยะเวลาดำเนินการ	หน่วยงานรับผิดชอบ	งบประมาณ
ระบบ HOSxP/HIS ไม่สามารถใช้งานได้เกิน ๓๐ นาที หรือข้อมูลให้บริการไม่พร้อมใช้	๓ x ๕ = ๑๕ สูงมาก (E)	๑. จัดทำแผนรองรับระบบ HOSxP ขัดข้องและแบบฟอร์มสำรองการให้บริการ ๒. ตรวจสอบสถานะ Server/Database/Network ทุกวันราชการ และเมื่อมีแจ้งเตือน ๓. กำหนดขั้นตอนแจ้งเหตุ แยกระดับความรุนแรง และรายงานผู้บริหารเมื่อหยุดชะงักเกิน ๓๐ นาที ๔. ทบทวนอุบัติการณ์ ๒๕๐๗๐๐๐๑๐๙ และกำหนด Corrective/Preventive Action ๕. ซ้อมใช้งานระบบ/เอกสารสำรองอย่างน้อยปีละ ๑ ครั้ง	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ
ระบบสำรองข้อมูลไม่ครอบคลุม หรือไม่สามารถกู้คืนข้อมูลได้ทันเวลา	๓ x ๕ = ๑๕ สูงมาก (E)	๑. กำหนดตารางสำรองข้อมูลฐานข้อมูล HOSxP และระบบสำคัญแบบรายวัน/รายเดือน ๒. ตรวจสอบผล Backup ทุกวันราชการและบันทึกผล ๓. สำรองข้อมูลอย่างน้อย ๒ สื่อ/๒ ตำแหน่ง รวมถึง External/Cloud ตามความเหมาะสม ๔. ทดสอบ Restore อย่างน้อยไตรมาสละ ๑ ครั้ง ๕. จำกัดสิทธิ์เข้าถึงไฟล์สำรองและจัดเก็บในพื้นที่ปลอดภัย	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ โอกาส x ผลกระทบ	แผนงาน/โครงการ/กิจกรรมรองรับการบริหารความเสี่ยง	ระยะเวลาดำเนินการ	หน่วยงานรับผิดชอบ	งบประมาณ
การติดมัลแวร์/ไวรัส/คริปโตไมเนอร์ในเครื่องลูกข่ายหรือเครื่องแม่ข่าย	๓ x ๔ = ๑๒ สูง (H)	๑. ติดตั้งและอัปเดต Antivirus/Endpoint Protection ในเครื่องที่ให้บริการ ๒. สแกนเครื่องที่ถูกแจ้งเตือน แยกเครื่องออกจากเครือข่ายเมื่อพบความเสี่ยง ๓. กำหนดแนวทาง Reimage/Upgrade เครื่อง Windows เก่าเป็น Windows ที่รองรับ ๔. บล็อก IOC/URL/Port ที่เกี่ยวข้องผ่าน Firewall ตามรายงาน CSM ๕. อบรมผู้ใช้งานเรื่องอีเมล ไฟล์แนบ และเว็บเสี่ยง	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ
การควบคุมสิทธิ์เข้าถึงระบบไม่เหมาะสมทั้งเครือข่ายภายในและเครือข่ายสาธารณะ	๓ x ๔ = ๑๒ สูง (H)	๑. กำหนดสิทธิ์ตามหน้าที่ Least Privilege และแยก Admin/User ทั่วไป ๒. ทบทวนสิทธิ์ผู้ใช้งาน HOSxP/ระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง ๓. ยกเลิกบัญชีผู้พ้นสภาพ/ย้ายงานทันทีที่ได้รับแจ้ง ๔. กำหนดนโยบายรหัสผ่านและห้ามใช้บัญชีร่วมกัน ๕. บันทึกการขอเพิ่ม/ลด/ยกเลิกสิทธิ์เป็นลายลักษณ์อักษร	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/หัวหน้าหน่วยงาน	ไม่ใช้งบประมาณ
การเปิดเผยข้อมูลผู้รับบริการหรือข้อมูลสุขภาพโดยไม่ได้รับอนุญาต	๒ x ๕ = ๑๐ สูง (H)	๑. กำหนดแนวปฏิบัติการใช้และเปิดเผยข้อมูลสุขภาพตามหน้าที่ ๒. ใช้บัญชีผู้ใช้งานรายบุคคลและออกจากระบบหลังใช้งาน ๓. จำกัดสิทธิ์แฟ้ม/รายงานที่มีข้อมูลส่วนบุคคล ๔. จัดทำแนวทางการขอประวัติการรักษาและการส่งต่อข้อมูล	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/เวชระเบียน/ทุกหน่วยงาน	ไม่ใช้งบประมาณ

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ โอกาส x ผลกระทบ	แผนงาน/โครงการ/กิจกรรมรองรับการบริหารความเสี่ยง	ระยะเวลาดำเนินการ	หน่วยงานรับผิดชอบ	งบประมาณ
		๕. สื่อสาร/ทบทวน PDPA และวินัยข้อมูลแก่เจ้าหน้าที่ทุกปี			
กระแสไฟฟ้าขัดข้องหรือ UPS ไม่พร้อมใช้ ส่งผลให้อุปกรณ์ IT เสียหาย/ระบบหยุดชะงัก	๓ x ๔ = ๑๒ สูง (H)	๑. สำรวจจุดบริการสำคัญที่ต้องมี UPS เช่น Server, ER, Ward, ANC, Lab, X-ray ๒. ตรวจสอบ UPS และแบตเตอรี่ตามรอบอย่างน้อยเดือนละ ๑ ครั้ง ๓. บำรุงรักษาเครื่องปั่นไฟและทดสอบตามแผน ๔. เปลี่ยนแบตเตอรี่ UPS ตามอายุการใช้งาน/ผลทดสอบ ๕. จัดลำดับจุดสำคัญสำหรับขอจัดซื้อ UPS เพิ่ม	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งาน ENV/งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ
แผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (BCP/DRP) ไม่พร้อมใช้งานจริง	๒ x ๕ = ๑๐ สูง (H)	๑. จัดทำ BCP/DRP ระบบสารสนเทศ ครอบคลุม HOSxP, Network, Internet, Backup, ช่องทางสื่อสาร ๒. กำหนด RTO/RPO ของระบบสำคัญ ๓. กำหนดผู้รับผิดชอบและช่องทางติดต่อฉุกเฉิน ๔. ซ้อมแผนอย่างน้อยปีละ ๑ ครั้ง และสรุปผลปรับปรุงแผน ๕. เชื่อมโยงแผนกับระบบเอกสารสำรองการให้บริการผู้ป่วย	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	คณะกรรมการสารสนเทศ/งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ
ระบบปฏิบัติการและเครื่องแม่ข่ายไม่ได้รับการ Patch ตามรอบ	๓ x ๓ = ๙ สูง (H)	๑. จัดทำทะเบียน Server/PC พร้อมเวอร์ชัน OS และสถานะสนับสนุน ๒. กำหนดรอบ Patch รายเดือนหรือรายไตรมาสตามความสำคัญ ๓. ทดสอบ Patch กับเครื่องสำรอง/ช่วงเวลานอกบริการก่อนใช้งานจริง ๔. สำรองข้อมูลก่อน Patch ระบบสำคัญ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ โอกาส x ผลกระทบ	แผนงาน/โครงการ/กิจกรรมรองรับการบริหารความเสี่ยง	ระยะเวลาดำเนินการ	หน่วยงานรับผิดชอบ	งบประมาณ
		๕. จัดทำรายงาน Patch Compliance รายไตรมาส			
ระบบบันทึกเหตุการณ์ (Log Management/SIEM) ไม่ครอบคลุมหรือไม่ถูกติดตาม	๓ x ๓ = ๙ สูง (H)	๑. กำหนดแหล่ง Log สำคัญ เช่น Firewall, Server, HIS, AD, Network Device ๒. ตรวจสอบรายงาน CSM/SIEM รายเดือน ๓. กำหนดขั้นตอนรับแจ้งและตอบสนองเหตุการณ์จาก Log ๔. เก็บรักษา Log ตามระยะเวลาที่เหมาะสมและจำกัดสิทธิ์เข้าถึง ๕. สรุปเหตุการณ์สำคัญเสนอต่อคณะกรรมการสารสนเทศ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/ผู้ให้บริการ CSM	ไม่ใช้งบประมาณ
ระบบเว็บ/บริการสาธารณะไม่มีการป้องกัน Web Application ที่เพียงพอ	๒ x ๔ = ๘ ปานกลาง (M)	๑. สำรวจระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ต ๒. ปิดพอร์ต/บริการที่ไม่จำเป็นและจำกัด IP ที่เข้าถึงระบบบริหารจัดการ ๓. ใช้ Firewall/WAF/Reverse Proxy ตามความเหมาะสม ๔. สำรองเว็บไซต์และไฟล์สำคัญเป็นรอบ ๕. ตรวจสอบช่องโหว่และอัปเดต CMS/Plugin อย่างสม่ำเสมอ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ
Software/Application ไม่ได้รับการอัปเดตหรือ Patch ตามรอบ	๒ x ๓ = ๖ ปานกลาง (M)	๑. จัดทำทะเบียนโปรแกรมสำคัญและผู้รับผิดชอบ ๒. กำหนดรอบตรวจสอบเวอร์ชันและ Patch อย่างน้อยรายไตรมาส ๓. สำรองข้อมูลและทดสอบก่อนอัปเดตระบบสำคัญ ๔. ยกเลิกโปรแกรมที่หมดอายุหรือไม่จำเป็น ๕. สื่อสารผู้ใช้งานเมื่อมีการอัปเดตที่กระทบการทำงาน	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/ผู้ดูแลระบบ	ไม่ใช้งบประมาณ

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ โอกาส x ผลกระทบ	แผนงาน/โครงการ/กิจกรรมรองรับการบริหารความเสี่ยง	ระยะเวลาดำเนินการ	หน่วยงานรับผิดชอบ	งบประมาณ
โครงข่ายภายในไม่มีการแยกส่วนที่เหมาะสม (Network Segmentation)	๒ x ๔ = ๘ ปานกลาง (M)	๑. จัดทำผังเครือข่ายและแบ่ง VLAN/Zone ตามประเภทการใช้งาน ๒. แยก Server/ระบบสำคัญออกจากเครื่องผู้ใช้งานทั่วไป ๓. กำหนด Firewall Rule ระหว่าง Zone เท่าที่จำเป็น ๔. แยกเครือข่าย Guest/IoT/กล้องวงจรปิดออกจากระบบบริการผู้ป่วย ๕. ทบทวน IP และอุปกรณ์ในเครือข่ายอย่างน้อยปีละ ๑ ครั้ง	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ไม่ใช้งบประมาณ
การใช้ซอฟต์แวร์ไม่มีลิขสิทธิ์หรือไม่ถูกต้องตามเงื่อนไข	๒ x ๓ = ๖ ปานกลาง (M)	๑. จัดทำทะเบียนซอฟต์แวร์และ License ของเครื่องราชการ ๒. ใช้ซอฟต์แวร์ที่ถูกลิขสิทธิ์หรือ Open Source ที่เหมาะสม ๓. กำหนดมาตรฐานเครื่องคอมพิวเตอร์ใหม่ เช่น Windows/Office ที่มี License ๔. ตรวจสอบเครื่องก่อนส่งมอบหรือซ่อมบำรุง ๕. สื่อสารห้ามติดตั้งโปรแกรมละเมิดลิขสิทธิ์	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานพัสดุ/งานสุขภาพดิจิทัล	เงินบำรุง
บุคลากร IT มีจำกัดหรือขาดทักษะเฉพาะด้าน ทำให้แก้ไขเหตุขัดข้องได้ล่าช้า	๓ x ๓ = ๙ สูง (H)	๑. กำหนดผู้รับผิดชอบหลักและผู้ช่วยในระบบสำคัญ ๒. จัดทำคู่มือแก้ไขปัญหาพื้นฐานและรายการติดต่อผู้ให้บริการ ๓. วางแผนอบรมเพิ่มพูนทักษะ Cybersecurity, Network, Database, Backup, HOSxP ๔. จัดลำดับงาน IT ตามความสำคัญของบริการผู้ป่วย	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	กลุ่มงานสุขภาพดิจิทัล /งานทรัพยากรบุคคล	ไม่ใช้งบประมาณ

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ โอกาส x ผลกระทบ	แผนงาน/โครงการ/กิจกรรมรองรับการบริหารความเสี่ยง	ระยะเวลาดำเนินการ	หน่วยงานรับผิดชอบ	งบประมาณ
		๕. รายงานข้อจำกัดกำลังคนต่อผู้บริหารเพื่อพิจารณาสนับสนุน			
บุคลากรทั่วไปขาดความตระหนักด้าน Cybersecurity และ PDPA	๒ x ๓ = ๖ ปานกลาง (M)	๑. ประกาศนโยบายและแนวปฏิบัติด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ๒. จัดทำสื่อประชาสัมพันธ์/Wallpaper/Line/บอร์ดความรู้ ๓. อบรมหรือทบทวน Cybersecurity & PDPA อย่างน้อยปีละ ๑ ครั้ง ๔. กำหนดช่องทางแจ้งเหตุผิดปกติด้านไซเบอร์และข้อมูลส่วนบุคคล ๕. ทบทวนอุบัติการณ์และสื่อสารบทเรียนโดยไม่ระบุข้อมูลผู้ป่วย	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/คณะกรรมการสารสนเทศ	ไม่ใช้งบประมาณ

บทที่ ๓ การติดตามประเมินผลการดำเนินงานจัดการความเสี่ยง

๓.๑ แบบรายงานผลการติดตามการบริหารความเสี่ยงด้านสารสนเทศ

แบบรายงานผลการติดตามการบริหารความเสี่ยงด้านสารสนเทศ โรงพยาบาลสองแคว ประจำปีงบประมาณ ๒๕๖๙

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ	กิจกรรมควบคุมหลัก	ตัวชี้วัด	ระยะเวลา	หน่วยงานรับผิดชอบ	ผลการดำเนินงาน/สถานะ
ระบบ HOSxP/HIS ไม่สามารถใช้งานได้เกิน ๓๐ นาที หรือข้อมูลให้บริการไม่พร้อมใช้	๓ x ๕ = ๑๕ สูงมาก (E)	- จัดทำแผนรองรับระบบ HOSxP ขัดข้องและแบบฟอร์มสำรองการให้บริการ - ตรวจสอบสถานะ Server/Database/Network ทุกวันราชการ และเมื่อมีแจ้งเตือน - กำหนดขั้นตอนแจ้งเหตุ แยกระดับความรุนแรง และรายงานผู้บริหารเมื่อหยุดชะงักเกิน ๓๐ นาที	ระบบสารสนเทศหลักพร้อมใช้งานไม่น้อยกว่า ๙๙%; มีบันทึกอุบัติการณ์และ RCA ครบถ้วน	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ดำเนินการ/ติดตามต่อเนื่อง
ระบบสำรองข้อมูลไม่ครอบคลุม หรือไม่สามารถกู้คืนข้อมูลได้ทันเวลา	๓ x ๕ = ๑๕ สูงมาก (E)	- กำหนดตารางสำรองข้อมูลฐานข้อมูล HOSxP และระบบสำคัญแบบรายวัน/รายเดือน - ตรวจสอบผล Backup ทุกวันราชการและบันทึกผล - สำรองข้อมูลอย่างน้อย ๒ สื่อ/๒ ตำแหน่ง รวมถึง External/Cloud ตามความเหมาะสม	Backup สำเร็จไม่น้อยกว่า ๙๕%; ทดสอบ Restore อย่างน้อยไตรมาสละ ๑ ครั้ง	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ดำเนินการ/ต้องติดตามหลักฐานรายเดือน
การติดมัลแวร์/ไวรัส/คริปโตไมเนอร์ในเครื่องลูกข่ายหรือเครื่องแม่ข่าย	๓ x ๔ = ๑๒ สูง (H)	- ติดตั้งและอัปเดต Antivirus/Endpoint Protection ในเครื่องที่ให้บริการ	เครื่องที่มี Antivirus อัปเดตไม่น้อยกว่า ๙๕%; Incident Malware	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ดำเนินการ/ติดตามจากรายงาน CSM

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ	กิจกรรมควบคุมหลัก	ตัวชี้วัด	ระยะเวลา	หน่วยงานรับผิดชอบ	ผลการดำเนินงาน/สถานะ
		- สแกนเครื่องที่ถูกแจ้งเตือน แยกเครื่องออกจากเครือข่ายเมื่อพบความเสี่ยง - กำหนดแนวทาง Reimage/Upgrade เครื่อง Windows เก่าเป็น Windows ที่รองรับ	ได้รับการแก้ไขภายใน ๑ วันทำการ			
การควบคุมสิทธิ์เข้าถึงระบบไม่เหมาะสม ทั้งเครือข่ายภายในและเครือข่ายสาธารณะ	๓ x ๔ = ๑๒ สูง (H)	- กำหนดสิทธิ์ตามหน้าที่ Least Privilege และแยก Admin/User ทั่วไป - ทบทวนสิทธิ์ผู้ใช้งาน HOSxP/ระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง - ยกเลิกบัญชีผู้พ้นสภาพ/ย้ายงานทันทีที่ได้รับแจ้ง	มีทะเบียนสิทธิ์ผู้ใช้งานและบันทึกทบทวนสิทธิ์ครบถ้วนปีละ ๑ ครั้ง	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/หัวหน้าหน่วยงาน	ดำเนินการ/รอทบทวนรอบปี
การเปิดเผยข้อมูลผู้รับบริการหรือข้อมูลสุขภาพโดยไม่ได้รับอนุญาต	๒ x ๕ = ๑๐ สูง (H)	- กำหนดแนวปฏิบัติการใช้และเปิดเผยข้อมูลสุขภาพตามหน้าที่ - ใช้บัญชีผู้ใช้งานรายบุคคลและออกจากระบบหลังใช้งาน - จำกัดสิทธิ์แฟ้ม/รายงานที่มีข้อมูลส่วนบุคคล	อุบัติการณ์ข้อมูลรั่วไหลเป็น ๐; เจ้าหน้าที่รับทราบแนวปฏิบัติไม่น้อยกว่า ๙๐%	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/เวชระเบียน/ทุกหน่วยงาน	ดำเนินการ/ติดตามอุบัติการณ์รายเดือน
กระแสไฟฟ้าขัดข้องหรือ UPS ไม่พร้อมใช้ ส่งผลให้อุปกรณ์ IT เสียหาย/ระบบหยุดชะงัก	๓ x ๔ = ๑๒ สูง (H)	- สำรวจจุดบริการสำคัญที่ต้องมี UPS เช่น Server, ER, Ward, ANC, Lab, X-ray - ตรวจสอบ UPS และแบตเตอรี่ตามรอบอย่างน้อยเดือนละ ๑ ครั้ง - บำรุงรักษาเครื่องปั่นไฟและทดสอบตามแผน	จุดบริการสำคัญมี UPS พร้อมใช้; มีบันทึกตรวจสอบ UPS/เครื่องปั่นไฟครบถ้วน	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งาน ENV/งานสุขภาพดิจิทัล	ดำเนินการ/เสนอแผนจัดซื้อเพิ่มเติม

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ	กิจกรรมควบคุมหลัก	ตัวชี้วัด	ระยะเวลา	หน่วยงานรับผิดชอบ	ผลการดำเนินงาน/สถานะ
แผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (BCP/DRP) ไม่พร้อมใช้งานจริง	๒ x ๕ = ๑๐ สูง (H)	- จัดทำ BCP/DRP ระบบสารสนเทศครอบคลุม HOSxP, Network, Internet, Backup, ช่องทางสื่อสาร - กำหนด RTO/RPO ของระบบสำคัญ - กำหนดผู้รับผิดชอบและช่องทางติดต่อฉุกเฉิน	มี BCP/DRP ฉบับอนุมัติและรายงานซ้อมแผนอย่างน้อยปีละ ๑ ครั้ง	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	คณะกรรมการสารสนเทศ/งานสุขภาพดิจิทัล	อยู่ระหว่างปรับปรุงและซ้อมแผน
ระบบปฏิบัติการและเครื่องแม่ข่ายไม่ได้รับการ Patch ตามรอบ	๓ x ๓ = ๙ สูง (H)	- จัดทำทะเบียน Server/PC พร้อมเวอร์ชัน OS และสถานะสนับสนุน - กำหนดรอบ Patch รายเดือนหรือรายไตรมาสตามความสำคัญ - ทดสอบ Patch กับเครื่องสำรอง/ช่วงเวลานอกบริการก่อนใช้งานจริง	เครื่องแม่ข่ายและเครื่องลูกข่ายสำคัญได้รับ Patch ตามรอบไม่น้อยกว่า ๘๐%	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	อยู่ระหว่างรวบรวมทะเบียนและแผน Patch
ระบบบันทึกเหตุการณ์ (Log Management/SIEM) ไม่ครอบคลุมหรือไม่ถูกติดตาม	๓ x ๓ = ๙ สูง (H)	- กำหนดแหล่ง Log สำคัญ เช่น Firewall, Server, HIS, AD, Network Device - ตรวจสอบรายงาน CSM/SIEM รายเดือน - กำหนดขั้นตอนรับแจ้งและตอบสนองเหตุการณ์จาก Log	มีรายงาน CSM/SIEM รายเดือนและมีบันทึกการติดตามเหตุการณ์สำคัญ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/ผู้ให้บริการ CSM	ดำเนินการ/ติดตามจากรายงานรายเดือน
ระบบเว็บ/บริการสาธารณะไม่มีการป้องกัน Web Application ที่เพียงพอ	๒ x ๔ = ๘ ปานกลาง (M)	- สำรวจระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ต - ปิดพอร์ต/บริการที่ไม่จำเป็นและจำกัด IP ที่เข้าถึงระบบบริหารจัดการ - ใช้ Firewall/WAF/Reverse Proxy ตามความเหมาะสม	ไม่มีบริการ Public ที่เปิดเกินความจำเป็น; เว็บไซต์สำคัญมี Backup และอัปเดตตามรอบ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ดำเนินการ/ต้องทบทวนรายการ Public Service

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ	กิจกรรมควบคุมหลัก	ตัวชี้วัด	ระยะเวลา	หน่วยงานรับผิดชอบ	ผลการดำเนินงาน/สถานะ
Software/Application ไม่ได้รับการอัปเดตหรือ Patch ตามรอบ	๒ x ๓ = ๖ ปานกลาง (M)	- จัดทำทะเบียนโปรแกรมสำคัญและผู้รับผิดชอบ - กำหนดรอบตรวจสอบเวอร์ชันและ Patch อย่างน้อยรายไตรมาส - สำรองข้อมูลและทดสอบก่อนอัปเดตระบบสำคัญ	มีทะเบียนโปรแกรมและบันทึกการอัปเดตรายไตรมาส	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/ผู้ดูแลระบบ	ดำเนินการบางส่วน/ต้องทำทะเบียนให้ครบ
โครงข่ายภายในไม่มีการแยกส่วนที่เหมาะสม (Network Segmentation)	๒ x ๔ = ๘ ปานกลาง (M)	- จัดทำผังเครือข่ายและแบ่ง VLAN/Zone ตามประเภทการใช้งาน - แยก Server/ระบบสำคัญออกจากเครื่องผู้ใช้งานทั่วไป - กำหนด Firewall Rule ระหว่าง Zone เท่าที่จำเป็น	มีผังเครือข่ายล่าสุดและมีการแบ่ง Zone สำหรับระบบสำคัญ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล	ดำเนินการเรียบร้อยแล้ว
การใช้ซอฟต์แวร์ไม่มีลิขสิทธิ์หรือไม่ถูกต้องตามเงื่อนไข	๒ x ๓ = ๖ ปานกลาง (M)	- จัดทำทะเบียนซอฟต์แวร์และ License ของเครื่องราชการ - ใช้ซอฟต์แวร์ที่ถูกลิขสิทธิ์หรือ Open Source ที่เหมาะสม - กำหนดมาตรฐานเครื่องคอมพิวเตอร์ใหม่ เช่น Windows/Office ที่มี License	เครื่องคอมพิวเตอร์ใหม่มี License ครบ; มีทะเบียน License ที่ตรวจสอบได้	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานพัสดุ/งานสุขภาพดิจิทัล	ดำเนินการ/ติดตามการจัดซื้อทดแทน
บุคลากร IT มีจำกัดหรือขาดทักษะเฉพาะด้าน ทำให้แก้ไขเหตุขัดข้องได้ล่าช้า	๓ x ๓ = ๙ สูง (H)	- กำหนดผู้รับผิดชอบหลักและผู้ช่วยในระบบสำคัญ - จัดทำคู่มือแก้ไขปัญหาพื้นฐานและรายการติดต่อผู้ให้บริการ	เจ้าหน้าที่ IT เข้ารับการอบรมอย่างน้อยปีละ ๑ เรื่อง; มีคู่มือระบบสำคัญ	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	กลุ่มงานสุขภาพดิจิทัล/งานทรัพยากรบุคคล	อยู่ระหว่างดำเนินการ

รายการความเสี่ยง	ระดับความเสี่ยงก่อนดำเนินการ	กิจกรรมควบคุมหลัก	ตัวชี้วัด	ระยะเวลา	หน่วยงานรับผิดชอบ	ผลการดำเนินงาน/สถานะ
		- วางแผนอบรมเพิ่มพูนทักษะ Cybersecurity, Network, Database, Backup, HOSxP				
บุคลากรทั่วไปขาดความตระหนักด้าน Cybersecurity และ PDPA	๒ x ๓ = ๖ ปานกลาง (M)	- ประกาศนโยบายและแนวปฏิบัติด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ - จัดทำสื่อประชาสัมพันธ์/ Wallpaper/Line/บอร์ดความรู้ - อบรมหรือทบทวน Cybersecurity & PDPA อย่างน้อยปีละ ๑ ครั้ง	เจ้าหน้าที่ได้รับการสื่อสาร/อบรมไม่น้อยกว่า ๘๐%; มีหลักฐานประชาสัมพันธ์	๑ ต.ค. ๖๘ ถึง ๓๐ ก.ย. ๖๙	งานสุขภาพดิจิทัล/คณะกรรมการสารสนเทศ	ดำเนินการ/ติดตาม หลักฐานการสื่อสาร

๓.๒ รายงานทบทวนความเสี่ยงคงเหลือและแนวทางปรับปรุงแผน

ใช้สำหรับสรุปผลหลังดำเนินมาตรการควบคุม เพื่อนำเสนอคณะกรรมการสารสนเทศและผู้บริหารโรงพยาบาล โดยประเด็นที่ยังมีระดับความเสี่ยงสูงหรือปานกลางให้กำหนดมาตรการเพิ่มเติมในรอบถัดไป

รายการความเสี่ยง	ระดับก่อนดำเนินการ	มาตรการที่ดำเนินการแล้ว/อยู่ระหว่างดำเนินการ	ความเสี่ยงคงเหลือ	ข้อเสนอปรับปรุงแผนรอบถัดไป
ระบบ HOSxP/HIS ไม่สามารถใช้งานได้เกิน ๓๐ นาที หรือข้อมูลให้บริการไม่พร้อมใช้	๓ x ๕ = ๑๕ สูงมาก (E)	- จัดทำแผนรองรับระบบ HOSxP ขัดข้องและแบบฟอร์มสำรองการให้บริการ - ตรวจสอบสถานะ Server/Database/Network ทุกวันราชการ และเมื่อมีแจ้งเตือน	๒ x ๔ = ๘ ปานกลาง	เร่งทดสอบแผนกู้คืน/ระบบสำรองและจัดทำรายงานผลเป็นหลักฐานรายไตรมาส
ระบบสำรองข้อมูลไม่ครอบคลุม หรือไม่สามารถกู้คืนข้อมูลได้ทันเวลา	๓ x ๕ = ๑๕ สูงมาก (E)	- กำหนดตารางสำรองข้อมูลฐานข้อมูล HOSxP และระบบสำคัญแบบรายวัน/รายเดือน - ตรวจสอบผล Backup ทุกวันราชการและบันทึกผล	๒ x ๔ = ๘ ปานกลาง	เร่งทดสอบแผนกู้คืน/ระบบสำรองและจัดทำรายงานผลเป็นหลักฐานรายไตรมาส
การติดมัลแวร์/ไวรัส/คริปโตไมเนอร์ในเครื่องลูกข่ายหรือเครื่องแม่ข่าย	๓ x ๔ = ๑๒ สูง (H)	- ติดตั้งและอัปเดต Antivirus/Endpoint Protection ในเครื่องที่ให้บริการ - สแกนเครื่องที่ถูกแจ้งเตือน แยกเครื่องออกจากเครือข่ายเมื่อพบความเสี่ยง	๒ x ๓ = ๖ ปานกลาง	จัดทำทะเบียนอุปกรณ์และรายงาน Patch/Antivirus/Log รายเดือน
การควบคุมสิทธิ์เข้าถึงระบบไม่เหมาะสม ทั้งเครือข่ายภายในและเครือข่ายสาธารณะ	๓ x ๔ = ๑๒ สูง (H)	- กำหนดสิทธิ์ตามหน้าที่ Least Privilege และแยก Admin/User ทั่วไป - ทบทวนสิทธิ์ผู้ใช้งาน HOSxP/ระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง	๒ x ๓ = ๖ ปานกลาง	ทบทวนสิทธิ์และจัดอบรม/สื่อสาร PDPA-Cybersecurity ให้ครอบคลุมทุกหน่วยงาน
การเปิดเผยข้อมูลผู้รับบริการหรือข้อมูลสุขภาพโดยไม่ได้รับอนุญาต	๒ x ๕ = ๑๐ สูง (H)	- กำหนดแนวปฏิบัติการใช้และเปิดเผยข้อมูลสุขภาพตามหน้าที่ -	๑ x ๔ = ๔ ปานกลาง	ทบทวนสิทธิ์และจัดอบรม/สื่อสาร PDPA-Cybersecurity ให้ครอบคลุมทุกหน่วยงาน

รายการความเสี่ยง	ระดับก่อนดำเนินการ	มาตรการที่ดำเนินการแล้ว/อยู่ระหว่างดำเนินการ	ความเสี่ยงคงเหลือ	ข้อเสนอปรับปรุงแผนรอบถัดไป
		ใช้บัญชีผู้ใช้งานรายบุคคลและออกจากระบบหลังใช้งาน		
กระแสไฟฟ้าขัดข้องหรือ UPS ไม่พร้อมใช้ ส่งผลให้อุปกรณ์ IT เสียหาย/ระบบหยุดชะงัก	๓ x ๔ = ๑๒ สูง (H)	- สำรวจจุดบริการสำคัญที่ต้องมี UPS เช่น Server, ER, Ward, ANC, Lab, X-ray - ตรวจสอบ UPS และแบตเตอรี่ตามรอบอย่างน้อยเดือนละ ๑ ครั้ง	๒ x ๓ = ๖ ปานกลาง	เสนอแผนจัดซื้อ/ปรับปรุง UPS และ Network Segmentation ตามลำดับความสำคัญ
แผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบ (BCP/DRP) ไม่พร้อมใช้งานจริง	๒ x ๕ = ๑๐ สูง (H)	- จัดทำ BCP/DRP ระบบสารสนเทศ ครอบคลุม HOSxP, Network, Internet, Backup, ช่องทางสื่อสาร - กำหนด RTO/RPO ของระบบสำคัญ	๒ x ๔ = ๘ ปานกลาง	เร่งทดสอบแผนกู้คืน/ระบบสำรองและจัดทำรายงานผลเป็นหลักฐานรายไตรมาส
ระบบปฏิบัติการและเครื่องแม่ข่ายไม่ได้รับการ Patch ตามรอบ	๓ x ๓ = ๙ สูง (H)	- จัดทำทะเบียน Server/PC พร้อมเวอร์ชัน OS และสถานะสนับสนุน - กำหนดรอบ Patch รายเดือนหรือรายไตรมาสตามความสำคัญ	๒ x ๓ = ๖ ปานกลาง	จัดทำทะเบียนอุปกรณ์และรายงาน Patch/Antivirus/Log รายเดือน
ระบบบันทึกเหตุการณ์ (Log Management/SIEM) ไม่ครอบคลุมหรือไม่ถูกติดตาม	๓ x ๓ = ๙ สูง (H)	- กำหนดแหล่ง Log สำคัญ เช่น Firewall, Server, HIS, AD, Network Device - ตรวจสอบรายงาน CSM/SIEM รายเดือน	๒ x ๒ = ๔ ปานกลาง	จัดทำทะเบียนอุปกรณ์และรายงาน Patch/Antivirus/Log รายเดือน
ระบบเว็บ/บริการสาธารณะไม่มีการป้องกัน Web Application ที่เพียงพอ	๒ x ๔ = ๘ ปานกลาง (M)	- สำรวจระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ต - ปิดพอร์ต/บริการที่ไม่จำเป็นและจำกัด IP ที่เข้าถึงระบบบริหารจัดการ	๑ x ๔ = ๔ ปานกลาง	ติดตามตามรอบและรวบรวมหลักฐานดำเนินการให้ครบถ้วน
Software/Application ไม่ได้รับการอัปเดตหรือ Patch ตามรอบ	๒ x ๓ = ๖ ปานกลาง (M)	- จัดทำทะเบียนโปรแกรมสำคัญและผู้รับผิดชอบ - กำหนดรอบตรวจสอบเวอร์ชันและ Patch อย่างน้อยรายไตรมาส	๑ x ๓ = ๓ น้อย	ติดตามตามรอบและรวบรวมหลักฐานดำเนินการให้ครบถ้วน

รายการความเสี่ยง	ระดับก่อนดำเนินการ	มาตรการที่ดำเนินการแล้ว/อยู่ระหว่างดำเนินการ	ความเสี่ยงคงเหลือ	ข้อเสนอปรับปรุงแผนรอบถัดไป
โครงข่ายภายในไม่มีการแยกส่วนที่เหมาะสม (Network Segmentation)	๒ x ๔ = ๘ ปานกลาง (M)	- จัดทำผังเครือข่ายและแบ่ง VLAN/Zone ตามประเภทการใช้งาน - แยก Server/ระบบสำคัญออกจากเครื่องผู้ใช้งานทั่วไป	๒ x ๓ = ๖ ปานกลาง	เสนอแผนจัดซื้อ/ปรับปรุง UPS และ Network Segmentation ตามลำดับความสำคัญ
การใช้ซอฟต์แวร์ไม่มีลิขสิทธิ์หรือไม่ถูกต้องตามเงื่อนไข	๒ x ๓ = ๖ ปานกลาง (M)	- จัดทำทะเบียนซอฟต์แวร์และ License ของเครื่องราชการ - ใช้ซอฟต์แวร์ที่ถูกลิขสิทธิ์หรือ Open Source ที่เหมาะสม	๑ x ๓ = ๓ น้อย	ติดตามตามรอบและรวบรวมหลักฐานดำเนินการให้ครบถ้วน
บุคลากร IT มีจำกัดหรือขาดทักษะเฉพาะด้าน ทำให้แก้ไขเหตุขัดข้องได้ล่าช้า	๓ x ๓ = ๙ สูง (H)	- กำหนดผู้รับผิดชอบหลักและผู้ช่วยในระบบสำคัญ - จัดทำคู่มือแก้ไขปัญหาพื้นฐานและรายการติดต่อผู้ให้บริการ	๒ x ๓ = ๖ ปานกลาง	ติดตามตามรอบและรวบรวมหลักฐานดำเนินการให้ครบถ้วน
บุคลากรทั่วไปขาดความตระหนักด้าน Cybersecurity และ PDPA	๒ x ๓ = ๖ ปานกลาง (M)	- ประกาศนโยบายและแนวปฏิบัติด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ - จัดทำสื่อประชาสัมพันธ์/Wallpaper/Line/บอร์ดความรู้	๑ x ๓ = ๓ น้อย	ทบทวนสิทธิ์และจัดอบรม/สื่อสาร PDPA-Cybersecurity ให้ครอบคลุมทุกหน่วยงาน

ภาคผนวก ก แบบลงนามรับรองและทบทวนเอกสาร

ชื่อเอกสาร	คู่มือวิเคราะห์ความเสี่ยงระบบเทคโนโลยีสารสนเทศ	**หน่วยงาน**	งานเทคโนโลยีสารสนเทศ/กลุ่มงานสุขภาพดิจิทัล
หน่วยงาน	โรงพยาบาลสองแคว จังหวัดน่าน	**ปีงบประมาณ**	๒๕๖๙
สถานะเอกสาร	ฉบับใช้งาน/แนบหลักฐานประเมิน	**รหัสอ้างอิง**	IT RISK ๒๕๖๙
ผู้จัดทำ/ผู้ทบทวน	งานเทคโนโลยีสารสนเทศ	**อนุมัติโดย**	ผู้อำนวยการโรงพยาบาลสองแคว
วันที่จัดทำ/ทบทวน	๑ มิถุนายน ๒๕๖๙		

สรุปการนำไปใช้เป็นหลักฐาน

๑. ใช้เป็นหลักฐานการระบุ วิเคราะห์ และจัดลำดับความเสี่ยงด้านสารสนเทศของโรงพยาบาลสองแคว

๒. ใช้ประกอบการติดตามผลการดำเนินการตามแผน และรายงานผู้บริหาร/คณะกรรมการสารสนเทศ

๓. เชื่อมโยงกับอุบัติการณ์รหัส ๒๕๐๗๐๐๐๑๐๙ กรณี HOSxP ใช้งานไม่ได้
เพื่อแสดงการนำเหตุการณ์จริงมาทบทวนและป้องกันซ้ำ

ผู้จัดทำ/ผู้ทบทวน
ลงชื่อ ..... (นางสาวตรีรัตน์ ทนันชัย) ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ วันที่ ๑ มิถุนายน ๒๕๖๙
ผู้อนุมัติ
ลงชื่อ ..... (นายกุลพล ตั้งรัตนาพิบูล) ตำแหน่ง ผู้อำนวยการโรงพยาบาลสองแคว วันที่ ๑ มิถุนายน ๒๕๖๙