บันทึกข้อความ

ส่วนราชการ งานเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านคา โทร ๐ ๓๒๒๐ ๖๘๗๙

ที่ รบ.๐๐๓๓.๓/๗.๙.๓/ **วันที่** กันยายน ๒๕๖๖

เรื่อง แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ICT RISK MANAGEMNT โรงพยาบาลบ้านคา

เรียน ผู้อำนวยการโรงพยาบาลบ้านคา

เนื่องด้วย โรงพยาบาลบ้านคา ให้ความสำคัญต่อแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดให้มีการปรับเปลี่ยนบริการของภาครัฐ เพื่อตอบสนองการบริการประชาชน ผู้ประกอบการทุกภาคส่วน ให้มีความสะดวก รวดเร็ว และแม่นยำ มีโครงสร้างการจัดเก็บและบริหารฐานข้อมูลที่บูรณาการไม่ซ้ำซ้อน การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๕๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุวัตถุประสงค์ตามภารกิจที่ตั้งไว้ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่อาจมีผลกระทบต่อการดำเนินงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของโรงพยาบาลบ้านคา แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น นำไปสู่การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

ในการนี้ งานเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านคา จึงขออนุมัติใช้แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ICT RISK MANAGEMENT เพื่อให้บุคลากรในหน่วยงานใช้เป็นแนวทางในการดำเนินงานต่อไป

จึงเรียนมาเพื่อโปรดทราบและพิจารณาอนุมัติ

เรียน ผู้อำนวยการโรงพยาบาลบ้านคา

.....

(นายสุริยา บุญเลิศฟ้า)

นักวิชาการคอมพิวเตอร์ปฏิบัติการ

คำสั่ง – อนุมัติให้ดำเนินการ

.....

(นายสุรฤทธิ์ เจริญศรี)

นายแพทย์ชำนาญการ

รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลบ้านคา

แผนบริหารจัดการความเสี่ยง

ดานเทคโนโลยีสารสนเทศ

ICT RISK MANAGEMENT

หลักการและเหตุผล

สืบเนื่องจากแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดให้มีการปรับเปลี่ยนบริการของภาครัฐ เพื่อตอบสนองการบริการประชาชน ผู้ประกอบการ ทุกภาคส่วนให้มีความสะดวก รวดเร็ว และแม่นยำ มีโครงสร้างการจัดเก็บและบริหารฐานข้อมูลที่บูรณการ ไม่ซ้ำซ้อน สามารถรองรับการเชื่อมโยงการทำงานระหว่างหน่วยงาน และ ให้บริการประชาชนได้อย่างทั่วถึงและมีประสิทธิภาพ การบริหารจัดการความเสี่ยงจึงมีบทบาทสำคัญในการปกป้องข้อมูล และ ระบบเครือข่ายคอมพิวเตอร์ ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้องงานตามภารกิจของหน่วยงานให้รอดพ้นจากความเสี่ยง ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และ การสื่อสารอีกด้วย ซึ่งขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้ อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็น ผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน มีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยี สารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้ จากความเสี่ยง และเพื่อให้การดำเนินตามภารกิจของหน่วยงานบรรลุผลตามวัตถุประสงค์ ไม่ใช่แค่เพียง การปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเท่านั้น การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่ง ผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่า ด้วยการบริหารกิจการบ้านเมืองที่ดีพ.ศ. ๒๕๕๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการ บริหารเชิงกลยุทธเป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุวัตถุประสงค์ตามภารกิจที่ตั้งไว้และเป็นการ พัฒนาการปฏิบัติงานของหน่วยงาน เพื่อนำไปสู่การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

วัตถุประสงค์

๑. เพื่อให้การจัดการภายในหน่วยงานมีประสิทธิภาพ และ มีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลบ้านค่า

๒. เพื่อให้มีการวางแผน การควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม

๓. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และ การเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ การสื่อสารภายในโรงพยาบาลบ้านค่า ผลที่คาดว่าจะได้รับ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยง และ ความเสี่ยงในด้านต่างๆ ที่อาจมี ผลกระทบต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และ การสื่อสารของโรงพยาบาลบ้านค่า แล้วพิจารณาหา แนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานตามแผน

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์ สารสนเทศของหน่วยงาน เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ความเสี่ยง ที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง และ พบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างาน หรือ ผู้บังคับบัญชา

แผนการลดความเสี่ยง (Treatment Plan) หมายถึง แผนการจัดการกับเหตุการณความเสี่ยง สำหรับ กรณีที่ผูประเมินความเสี่ยงไดประเมินเหตุการณความเสี่ยงหนึ่ง และ พบวามีความเสี่ยงเกินกวาระดับความเสี่ยง ที่ยอมรับไดผูประเมินความเสี่ยงจะตองนำเสนอแผนการจัดการดังกลาวตอหัวหนางาน หรือ ผูบังคับบัญชาเพื่อพิจารณาอนุมัติดำเนินการ

ปจจัยเสี่ยง (Risk Factor) หมายถึง ตนเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำใหวัตถุประสงคที่ กำหนดไว โดยตองระบุไดดวยวาเหตุการณนั้นจะเกิดที่ไหน เมื่อใด และ จะเกิดขึ้นไดอยางไร และ ทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเปนสาเหตุที่แทจริง เพื่อจะไดวิเคราะห และ กำหนดมาตรการความเสี่ยงใน ภายหลังได อยางถูกตอง

ขอบเขตการดำเนินการ

เปนการบริหารจัดการความเสี่ยงดานระบบเทคโนโลยีสารสนเทศ และ การสื่อสาร ภายในความรับผิดชอบของโรงพยาบาลบ้านคา

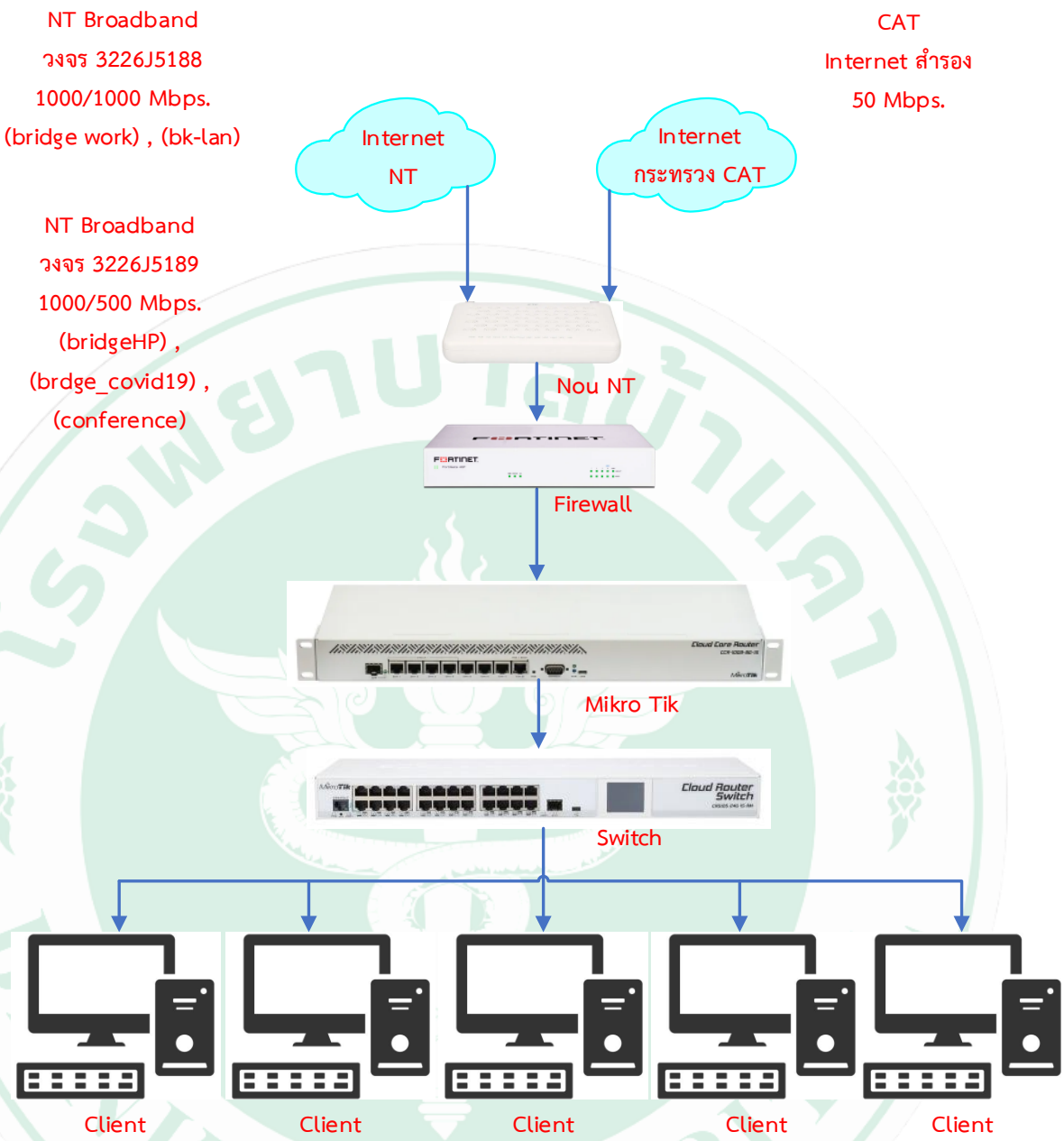
สถานภาพเทคโนโลยีสารสนเทศ และ การบริหารจัดการในปจจุบันของ โรงพยาบาลบ้านคา

ระบบเครือขายคอมพิวเตอร

ระบบเครือขายของ โรงพยาบาลบ้านคา ประกอบไปดวยสองสวนหลัก คือ ระบบเครือขายที่ใชสาย (Wire Network) และ ระบบเครือขายไรสาย (Wireless Network) โดยระบบเครือขายทั้งสองแยกการบริหารจัดการออกจากกัน โดยเครือขายใชสาย (Wire Network) โรงพยาบาลบ้านคา จะเปนผูบริหารจัดการสวนระบบเครือขายไรสาย (Wireless Network) จะเปนการใชบริการจากผูใหบริการอินเทอรเน็ต (Internet service provider: ISP) โดยมีรายละเอียดของระบบเครือขายทั้ง ๒ ประเภท ดังตอไปนี้

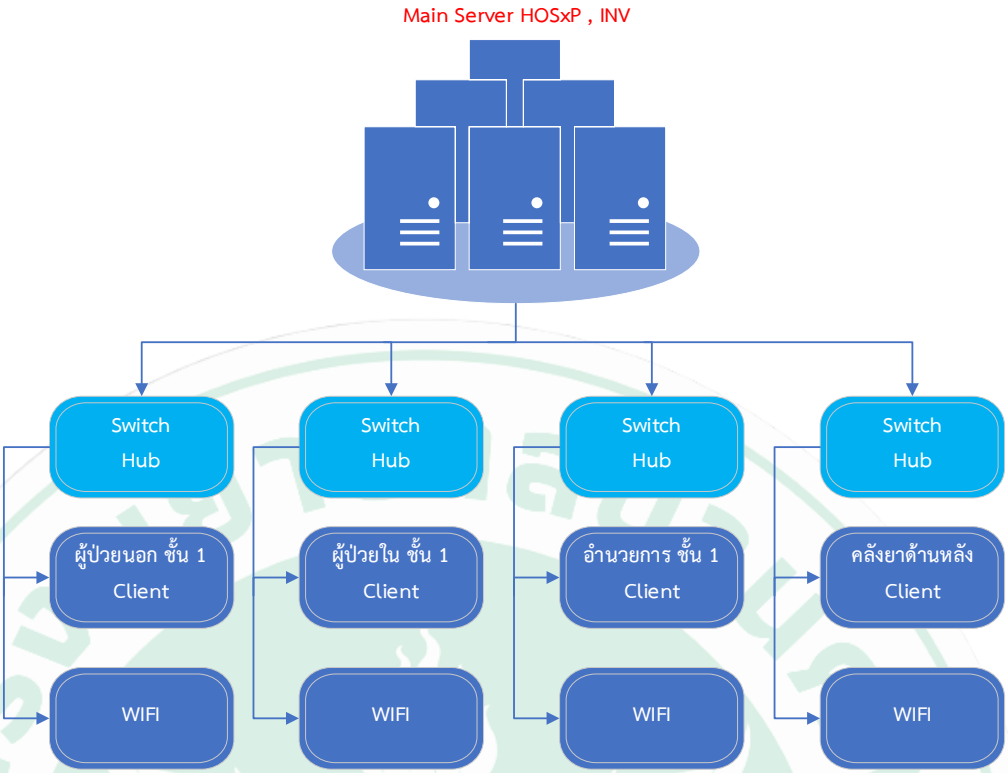
๑. ระบบเครือข่ายใช้สาย (Wire Network) โรงพยาบาลบ้านคา ใช้เครือข่ายผู้ให้บริการ Internet ๒ ผู้ให้บริการ NT กับ CAT ใช้ในการออกสู่อินเทอร์เน็ต โรงพยาบาลบ้านคา มีโครงข่าย Internet ให้บริการแก่เจ้าหน้าที่ ประกอบด้วย ๒ วงจรหลักๆ

๑. ผู้ให้บริการ NT Broadband เลขที่วงจร 3226J5188 (Fix Public IP Address 4 IP) ความเร็ว
   ช่วงเวลา 06.00 น. - 18.00 น. ความเร็ว 1000 Mbps. / 1000 Mbps.
   ช่วงเวลา 18.01 น. - 05.59 น. ความเร็ว 500 Mbps. / 500 Mbps.
   (bridge work) , (bk-lan)
๒. ผู้ให้บริการ NT Broadband เลขที่วงจร 3226J5189 (Fix Public IP Address 1 IP) ความเร็ว
   ทุกช่วงเวลา 1000 Mbps. / 500 Mbps.
   บริการเสริม IP Phone 1 หมายเลข (032-206879) โทรฟรี 1200 บาท / เดือน
   (bridgeHP) , (brdge_covid19) , (conference)
๓. ผู้ให้บริการ CAT เลขที่วงจร 3050001974
   ทุกช่วงเวลา 50 Mbps.



รูปที่ ๑ แสดงการเชื่อมโยงระบบเครือข่าย Internet

โดยระบบเครือข่ายใช้สายภายในโรงพยาบาลบ้านคา จะทำการเชื่อมโยงระบบเครือข่ายเข้ากับอุปกรณ์เครือข่ายของผู้ให้บริการอินเทอร์เน็ต (Internet Service provider: ISP) และเชื่อมต่อมายังอุปกรณ์รักษาความมั่นคงปลอดภัยในระบบเครือข่ายโรงพยาบาลบ้านคา จากนั้นจะทำการต่อเข้ากับอุปกรณ์เครือข่ายหลัก (Core Switch) ก่อนจะทำการกระจายไปยังลูกข่าย ตั้งแต่ชั้น ที่ ๑ ถึงชั้นที่ ๒ และตึก IPD , คลังยาด้านหลัง เพื่อใช้การดำเนินงานของโรงพยาบาลบ้านคา



รูปที่ ๒ แสดงระบบเครือข่ายโรงพยาบาลบ้านคา

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานสามารถแยกประเภทความเสี่ยงเป็น **๗ ประเภท** ดังนี้

๑. **ความเสี่ยงจากผู้ปฏิบัติงาน** (People ware) เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการบริหารจัดการสิทธิ์ในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือ ใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ หรือ อนุญาตให้ผู้อื่นใช้สิทธิ์ในการเข้าถึงระบบ อาจทำให้เกิดความเสียหายต่อระบบ และ ข้อมูลสารสนเทศได้

๒. **ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิด ขึ้นจากระบบคอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์เทคโนโลยีสนับสนุน ถูกโจมตีจากไวรัส หรือ โปรแกรมไม่ประสงค์ดีถูกก่อกวนจาก Hacker หรือ ถูกเจาะ ทำลายระบบจาก Cracker

๓. **ความเสี่ยงด้านอุปกรณ์ (Hardware)** เป็นความเสี่ยงที่อาจเกิดขึ้นจากอุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย ทำหน้าที่สนับสนุนการทำงานของคอมพิวเตอร์ในลักษณะต่าง ๆ เช่น External Hard disk , Flash Drive , Switch , Router , SD Card เป็นต้น

๔. **ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software)** ระบบงาน การใช้โปรแกรมละเมิดลิขสิทธิ์ซึ่งขัดต่อระบบ กฎหมายที่เกี่ยวข้อง และ อาจส่งผลให้ไม่สามารถใช้งานโปรแกรมได้เต็มประสิทธิภาพ

๕. **ความเสี่ยงด้านสถานการณ์ฉุกเฉิน** คือ ความเสี่ยงที่เกิดจากภัยพิบัติตามธรรมชาติ เช่น ไฟฟ้าดับ ไฟกระชาก ไฟไหม้ น้ำท่วม การชุมนุมประท้วง เป็นต้น

๖. **ความเสี่ยงด้านการบริหารจัดการ** เป็นความเสี่ยงจากการเปลี่ยนแปลงแนวนโยบายในการบริหารจัดการอาจส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ และ การสื่อสาร

๗. **ลักษณะรายละเอียดของความเสี่ยง (Description of risk)**

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
๑. ความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงด้านเทคนิค	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบ หรือ ใช้งานแทนถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ขาดการกำหนดนโยบายในการให้บริการ Web Service	- การสวมรอยผู้ใช้การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตการเปิดช่องให้มีการเข้าถึงระบบได้จากภายนอก - เปิดให้บริการ Web Service โดยไม่กำหนดช่วงเวลา	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงด้านเทคนิค	ผู้ใช้ขาดความระมัดระวังในการใช้ ระบบเครือข่าย เช่น การนำ **Wireless Router** หรือ **Switch/Hub** มาเชื่อมต่อกับ ระบบเครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาต และ มีการกำหนดค่า **(Configuration)** ที่ไม่ถูกต้อง ทำให้อุปกรณ์หรือ เครื่องคอมพิวเตอร์อื่น ใน ระบบเครือข่ายไม่สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของหน่วยงาน	- การนำอุปกรณ์อื่นมาเชื่อต่อเข้าระบบ - ความล้มเหลวทางเทคนิค - การใช้อุปกรณ์ในการถ่ายโอนข้อมูล	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
๓. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี / การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจส่งผลให้โปรแกรมไม่มีประสิทธิภาพ อาจก่อให้เกิดการบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น **Hacker/Cracker** เป็นค้นการดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส Malware , Worm ต่าง ๆ	- การใช้โปรแกรมลิขสิทธิ์	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย / อุปกรณ์เครือข่าย
๔. ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับไฟกระชาก	ความเสี่ยงด้านเทคนิค / ความเสี่ยงสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือ เกิดไฟกระชาก ทำให้เครื่องคอมพิวเตอร์ และอุปกรณ์ ต่าง ๆ อาจได้รับความเสียหายจากแรงดันไฟฟ้าไม่คงที่ หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย หรือ ไม่สามารถให้บริการได้ เช่น ระบบงานภายในโรงพยาบาลบ้านคา	- การเกิดภัยพิบัติ ต่าง ๆ - การชำรุดเสียหายของอุปกรณ์ หรือความพร้อมของอุปกรณ์ในการรับมือต่อสถานการณ์ฉุกเฉิน ต่าง ๆ	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย / อุปกรณ์เครือข่าย
๕. ความเสี่ยงจากการขาดทักษะความชำนาญเฉพาะด้านของบุคลากรผู้ปฏิบัติงาน/ บุคลากรไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดทักษะความชำนาญเฉพาะ ด้านทำให้การทำงานอาจเกิดข้อผิดพลาด และ จำนวนบุคลากร ที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศ ที่เพิ่มขึ้นส่งผลกระทบต่อการควบคุมดูแลระบบ	- บุคลากรไม่เพียงพอ / บุคลากรไม่พัฒนาศักยภาพให้เกิดความชำนาญเฉพาะด้าน	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา/เปลี่ยนแปลงผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชาอาจทำให้นโยบายการบริหารจัดการเทคโนโลยีสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- การเปลี่ยนแปลงนโยบายผู้บริหารทำให้ขาดความต่อเนื่อง	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย / อุปกรณ์เครือข่าย
๗. ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุนการปฏิบัติงานทำให้ไม่สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายใน และ ภายนอกองค์กร หรือ ไม่สามารถเข้ากันได้กลับเทคโนโลยีสมัยใหม่	- การเปลี่ยนแปลงทางด้านเทคโนโลยีเพื่อตอบสนองภารกิจงานตามนโยบายภาครัฐ - ระยะเวลาในการตั้งงบประมาณ	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย / อุปกรณ์เครือข่าย

การประเมินความเสี่ยง

โดยโรงพยาบาลบ้านคา กำหนดเกณฑ์ที่จะใช้การประเมินความเสี่ยง ได้แก่ ระดับความรุนแรง โอกาสที่จะเกิดความเสี่ยง ระดับความเสี่ยง ดังนี้

ระดับ และ โอกาสในการเกิดเหตุการณ์ ต่าง ๆ			ระดับความรุนแรง (๕ คะแนน)	
ระดับ	โอกาสที่จะเกิด	คำอธิบาย	ต่อระบบงาน	ต่อพันธกิจ
๕	สูงมาก	๕ ครั้ง / ปี	๕	๕
๔	สูง	๔ ครั้ง / ปี	๔	๔
๓	ปานกลาง	๓ ครั้ง / ปี	๓	๓
๒	น้อย	๒ ครั้ง / ปี	๒	๒
๑	น้อยมาก	๑ ครั้ง / ปี	๑	๑

ตารางแสดงการประเมินความเสี่ยง

ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง
๑. ความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยด้านเทคนิค	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบ หรือ ใช้งานแทน ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ขาดการกำหนด นโยบายในการให้บริการ Web Service	๒	๕
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยด้านอุปกรณ์	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ **Wireless Router** หรือ **Switch/Hub** มาเชื่อมต่อ กับระบบเครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาต และ มีการกำหนดค่า **(Configuration)** ที่ไม่ถูกต้อง ทำให้อุปกรณ์ หรือ เครื่องคอมพิวเตอร์อื่น ใน ระบบเครือข่ายไม่ สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของหน่วยงาน การใช้อุปกรณ์ในการถ่ายโอนข้อมูล	๒	๓
๓. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี / การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจส่งผลให้โปรแกรมไม่มีประสิทธิภาพ อาจก่อให้เกิดการบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น **Hacker/Cracker** เป็นค้นการดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส Malware , Worm ต่าง ๆ	๒	๔

ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง
๔. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟฟ้ากระชาก	ความเสี่ยงด้านเทคนิค / ความเสี่ยงสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดไฟกระชาก ทำให้เครื่องคอมพิวเตอร์ และ อุปกรณ์ ต่าง ๆ อาจได้รับความเสียหายจากแรงดันไฟฟ้าไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย หรือ ไม่สามารถให้บริการได้ เช่น ระบบงานภายใน โรงพยาบาลบ้านคา	๔	๔
๕. ความเสี่ยงจากการขาดทักษะความชำนาญเฉพาะด้านของบุคลากรผู้ปฏิบัติงาน/บุคลากรไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดทักษะความชำนาญเฉพาะด้านทำให้การทำงานอาจเกิดข้อผิดพลาด และ จำนวนบุคลากร ที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศ ที่เพิ่มขึ้นส่งผลกระทบต่อการควบคุมดูแลระบบ	๓	๓
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชาอาจทำให้นโยบายการบริหารจัดการเทคโนโลยีสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๓	๓
๗. ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุนการปฏิบัติงานทำให้ไม่สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายใน และ ภายนอกองค์กร หรือ ไม่สามารถเข้ากันได้กลับเทคโนโลยีสมัยใหม่	๑	๓

การประเมินค่าความเสี่ยง

ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑. ความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้งานระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบ หรือใช้งานแทน การตั้งค่าให้ระบบจำรหัสผ่านในการเข้าใช้งาน	๒	๕	๑๐
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยด้านอุปกรณ์	ผู้ใช้ขาดความระมัดระวังในการใช้ ระบบเครือข่าย เช่น การนำ **Wireless Router** หรือ **Switch/Hub** มาเชื่อมต่อ กับ ระบบเครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาต และ มีการกำหนดค่า **(Configuration)** ที่ไม่ถูกต้อง ทำให้อุปกรณ์ หรือเครื่องคอมพิวเตอร์อื่น ในระบบเครือข่ายไม่ สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของหน่วยงาน การใช้อุปกรณ์ในการถ่ายโอนข้อมูล	๒	๓	๖
๓. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี / การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน / ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจส่งผลให้โปรแกรมไม่มีประสิทธิภาพ อาจก่อให้เกิดการบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น **Hacker/Cracker** เป็นค้นการดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส Malware , Worm ต่าง ๆ	๒	๔	๘

	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๔.	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟฟ้ากระชาก	ความเสี่ยงด้านเทคนิค / ความเสี่ยงสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือ เกิดไฟกระชาก ทำให้เครื่องคอมพิวเตอร์ และอุปกรณ์ ต่าง ๆ อาจได้รับความเสียหายจากแรงดันไฟฟ้าไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย หรือ ไม่สามารถให้บริการได้ เช่น ระบบงานภายใน โรงพยาบาลบ้านคา	๔	๔	๑๖
๕.	ความเสี่ยงจากการขาดทักษะความชำนาญเฉพาะด้านของบุคลากรผู้ปฏิบัติงาน/บุคลากรไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดทักษะความชำนาญเฉพาะ ด้านทำให้การทำงานอาจเกิดข้อผิดพลาด และจำนวนบุคลากร ที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศ ที่เพิ่มขึ้นส่งผลกระทบต่อการควบคุมดูแลระบบ	๓	๓	๙
๖.	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา/เปลี่ยนแปลงผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชาอาจทำให้นโยบายการบริหารจัดการเทคโนโลยีสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๓	๓	๙
๗.	ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุนการปฏิบัติงานทำให้ไม่สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายใน และภายนอกองค์กร หรือ ไม่สามารถเข้ากันได้กลับเทคโนโลยีสมัยใหม่	๑	๓	๓

การจัดการความเสี่ยง

หน่วยงานกำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๐ ขึ้นไป ส่วนความเสี่ยงที่มีระดับต่ำกว่า ๑๐ ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยง หรือ ไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๑	ความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลอื่น	๑๐	- ยอมรับความเสี่ยง (ลงแผนจัดการความเสี่ยง)	- สร้างความตะหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล	ผู้ใช้ในหน่วยงาน / งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗
๒	ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๖	- ยอมรับความเสี่ยง (ลงแผนจัดการความเสี่ยง)	- จัดหาเครื่อง และอุปกรณ์ สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสารมารถปฏิบัติงานได้จัดทำแผนการตรวจสอบ และจัดจ้างบำรุงรักษาอย่างสม่ำเสมอ / ดำเนินการเพิ่มจุดเชื่อมต่อสัญญาณอินเตอร์เน็ตให้ครอบคลุม	ผู้ใช้ในหน่วยงาน / งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗
๓	ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี / การใช้โปรแกรมละเมิดลิขสิทธิ์	๘	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดฝึกอบรมเพื่อสร้างความตระหนักในเรื่อง นโยบาย และ แนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย - จัดหาโปรแกรมลิขสิทธิ์ เพื่อใช้ในการปฏิบัติงาน	ผู้ใช้ในหน่วยงาน / งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๔	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟฟ้ากระชาก	๑๖	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดหาเครื่องปกกันไฟฟ้ากระชาก - ประสานงานกับฝ่ายงานบริหารเรื่องเครื่องกำเนิดไฟฟ้าให้สามารถใช้งานได้ตอนที่ไฟฟ้าดับ	ฝ่ายงานบริหาร / งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗
๕	ความเสี่ยงจากการขาดทักษะความชำนาญเฉพาะด้านของบุคลากรผู้ปฏิบัติงาน/บุคลากรไม่เพียงพอ	๙	- ยอมรับความเสี่ยง (ลงแผนจัดการความเสี่ยง)	- จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม - จัดทำคู่มือปฏิบัติงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณ์ที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้	ผู้ใช้ในหน่วยงาน / งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗
๖	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา/เปลี่ยนแปลงผู้บังคับบัญชา	๙	- ยอมรับความเสี่ยง (ลงแผนจัดการความเสี่ยง)	แต่งตั้งคณะทำงานเทคโนโลยีสารสนเทศตามวาระของทีมความเสี่ยงที่เปลี่ยนแปลง	งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗
๗	ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	๓	- ยอมรับความเสี่ยง (ลงแผนจัดการความเสี่ยง)	จัดทำโครงการเพื่อจัดหาเทคโนโลยีทันสมัย เพื่อสนับสนุนการปฏิบัติงานตามภารกิจ และยุทธศาสตร์	งาน (IT) เทคโนโลยีสารสนเทศ	เฝ้าระวังตลอดปีงบประมาณ ๒๕๖๗

แผนบริหารการจัดการความเสี่ยงเทคโนโลยีสารสนเทศ ฉบับนี้ ได้ผ่านการพิจารณาจาก คณะทำงานบริหาร และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลเพื่อให้เจ้าหน้าที่ โรงพยาบาลบ้านคา ได้ใช้เป็นแนวทางปฏิบัติในการดำเนิน เพื่อ จัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต่อไป

(นายสุรฤทธิ์ เจริญศรี)
ผู้อำนวยการโรงพยาบาลบ้านคา
วันที่.....พฤศจิกายน พ.ศ. ๒๕๖๖