การดำเนินการบริหารจัดการความเสี่ยง
ทีมสารสนเทศโรงพยาบาลเขาคิชฌกูฏ ปีงบประมาณ 2566

ประเภทความเสี่ยง	แนวทางการควบคุม	ปีงบ 2566				มาตรการควบคุม
		Q1	Q2	Q3	Q4	
1.ความเสี่ยงจาก การเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ตรวจสอบความพร้อมใช้ของอุปกรณ์ดับเพลิง		✓			1.ตรวจสอบอุปกรณ์ดับเพลิงถังสีเขียวชนิดฮาโลตรอน ให้เกจความดันพร้อมใช้ ติดตั้งไว้หน้าห้องศูนย์คอมพิวเอร์ 2.ติดตั้งเบรคเกอร์ในการตัดไฟฟ้าของระบบ เมื่อไฟฟ้าเกิน รั่ว หรือขัดข้อง
	จัดทำแผนในการ เคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ				✓	1.ทบทวนลำดับความสำคัญ ในการเคลื่อนย้าย 2.จัดระบบให้ง่ายต่อการเคลื่อนย้าย สามารถถอดสายสัญญาณต่างๆได้อย่างสะดวกรวดเร็ว
	จัดทำแผนรับสถานการ เพื่อให้สามารถดำเนินการได้อย่าง ต่อเนื่อง	←			→	1.ตรวจสอบสำรวจเส้นทางสม่ำเสมอ และจัดทำเส้นทางสำรอง 2.ทบทวนกระบวนการ หาวิทยาการและแนวทางใหม่ๆ
2. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาด ความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้าน เทคโนโลยีสารสนเทศ	ฝึกอบรม เผยแพร่ และประชาสัมพันธ์ เรื่องความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ	←			→	1.จัดทำเอกสารประชาสัมพันธ์ ความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ แจกให้ทุกหน่วยงานได้รับทราบ
	กำกับดูแลการ ปฏิบัติตามแนว ปฏิบัติด้านการรักษาความมั่งคงปลอดภัย ด้านเทคโนโลยีสารสนเทศอย่าง เคร่งครัด	←			→	1.การออกระเบียบมาตรฐานการเข้าถึง การใช้ข้อมูล การรักษาความลับ ของการใช้เทคโนโลยีสารสนเทศ ตามระเบียบหรือ พรบ. กฎหมายที่กำหนด 2.การกำหนดการเข้าถึงข้อมูลสารสนเทศที่จำเป็น
3. ความเสี่ยงจาก กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที	แจ้งดำเนินการปรับปรุงของระบบไฟฟ้าสำรองอัตโนมัติ				✓	1.เมื่อเครื่อง SERVER ปิดลงโดยเครื่องสำรองไฟฟ้าของโรงพยาบาลไม่ทำงาน แจ้งบริหารดำเนินการ
	ตรวจสอบความพร้อมของระบบสำรองไฟฟ้า	←			→	1.วางแผน จัดซื้อ จัดหาเครื่องสำรองไฟฟ้าให้พอเพียงพ้อมใช้ 2.ระบบบำรุงรักษาเครื่องสำรองไฟฟ้า บันทึกอายุการใช้งาน และความคุ้มค่า

ประเภทความเสี่ยง	แนวทางการควบคุม	ปีงบ 2566				มาตรการควบคุม
		Q1	Q2	Q3	Q4	
4.ความเสี่ยงจากการ การถูกบุกรุกโดยผู้ไม่ประสงค์ดี	ตรวจสอบการตั้งค่า ของ Firewall, PS อย่างสม่ำเสมอ	←			→	1.ศึกษา ตั้งค่า ตรวจสอบการทำงานของระบบ fire wall สม่ำเสมอ 2.อัพเดทการตั้งค่าตามความจำเป็น
	บริหารจัดการระบบ ตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ	←			→	1.ศึกษาเทคโนโลยี การปรับปรุง ความเหมาะสมของอุปกรณ์ fire wall 2.ตรวจสอบการบุกรุก และหาทางป้องกันอย่างสม่ำเสมอ
	จัดทำแผนจัดซื้อ Firewall ทดแทน				✓	1.จัดซื้อตามความเหมาะสม คุ้มค่า ตามอายุการใช้งาน
	อัพเดท Firmware content ของระบบ Firewall		✓			1.อัพเดทเฟิร์มแวร์ ของระบบ Firewall ให้ทันสมัยอยู่เสมอ
5.ความเสี่ยงจากการ เชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลว หรือไม่สามารถใช้งานได้	สำรวจและจัดหาระบบ เครือข่ายอินเทอร์เน็ต สำรองเพื่อเป็นช่องทางให้ระบบอินเทอร์เน็ตใช้ งานได้อย่างต่อเนื่อง	←			→	1.จัดทำระบบ Internet สำรอง ด้วยวิธี Load balance 2.ตรวจสอบการอัพเดทแพกเกจอินเตอร์เน็ต เพื่อให้องค์กรใช้ได้อย่างคุ้มค่า 3.กรณีอินเตอร์เน็ตขัดข้องทั้ง 2 เส้น จำเป็นต้องยอมรับความเสี่ยง
	ตรวจสอบการเชื่อมต่อเครือข่ายอินเทอร์เน็ต	←			→	1.สร้างมาตรฐาน ตรวจสอบการเชื่อมต่อ ความเร็ว ของอินเตอร์เน็ตอยู่เสมอ
6. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉินร้ายแรงมากที่สุด	จัดทำแผน ขั้นตอนการอนุมัติ การติดตั้งเพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง				✓	1.จัดทำแผนจัดซื้อไปอย่างสม่ำเสมอ เพื่อสามารถจัดหาได้อย่างทันเวลา 2.จัดทำระบบสำรองอุปกร์อย่างเพียงพอ เหมาะสม
	จัดทำคู่มือแผนบริหารความต่อเนื่อง (BCP)และแผนกู้คืนระบบ DRP				✓	1.จัดทำคู่มือ และสามารถเรียกใช้ได้ทันที

ประเภทความเสี่ยง	แนวทางการควบคุม	ปีงบ 2566				มาตรการควบคุม
		Q1	Q2	Q3	Q4	
7. ความเสี่ยงจาก การไม่ได้รับงบประมาณในการบำรุงรักษาระบบสารสนเทศและระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	มีการสำรวจและ รวบรวมความต้องการอย่างต่อเนื่อง เพื่อการจัดทำงบประมาณในแต่ละปี		←	→		1.รวบรวมความต้องการ จัดทำแผนล่วงหน้าในการพิจารณาตามลำดับความสำคัญ 2.ชี้แจงแนวทางการจัดซื้อ อธิบายการไม่อนุมัติแก่เจ้าหน้าที่ และวางแผนการดำเนินงานในคราวถัดไป
	มีการหารือ ชี้แจ้งและทำความเข้าใจกับผู้บังคับบัญชาในเรื่องงบประมาณที่ต้องการใช้ อย่างชัดเจน			✓		1.มีการวางแผนจัดซื้อ ปรึกษา ทำความเข้าใจ สรุปการจัดซื้อและทิศทางที่จะเป็นไป 2.ออกแบบแผนงาน ให้สอดคล้องกับนโยบายของผู้บังคับบัญชา
8. ความเสี่ยงระบบเทคโนโลยีอาจทำให้ เกิดความบกพร่องในการดูแลผู้ป่วย	เมื่อพบเหตุอุบัติการณ์ให้รายงานทุกครั้ง	←			→	1.บันทึกอุบัติการณ์ ไว้เป็นข้อมูลปรับปรุง พัฒนา ของฝ่ายสารสนเทศ
	ควบคุม ติดตาม ดูแล โดยคณะกรรการความเสี่ยงรพ.เขาคิชฌกูฏ	←			→	1.ติดตามข้อมูล เก็บประวัติและสถิติ ไว้ปรับปรุงแก้ไข ทุกๆปี 2.เมื่อมีเหตุระดับรุนแรงให้วางแผนแก้ไขทันที
9. ความเสี่ยง ด้านการการเปิดเผยข้อมูลผู้ป่วย	จัดทำแผนโครงการกระตุ้นผู้ใช้งานให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูลหรือแชร์ข้อมูลในสื่อสังคม ออนไลน์ ทุกชนิด	←			→	1.จัดทำสื่อ กระตุ้นเตือน ให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูลหรือแชร์ข้อมูลในสื่อสังคม ออนไลน์ทุกปี
	ปรับปรุงระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของ รพ.				✓	1.ปรับปรุงระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศทุกปี 2.ศึกษาระเบียบต่างๆอยู่เสมอ เพื่อสร้างมาตรฐานตามหลักสากล
	ประกาศใช้นโยบายเรื่องระเบียบปฏิบัติในการปฏิบัติการส่งข้อมูลผู้ป่วยทางโปรแกรม LINE	✓				1.จัดทำนโยบายเรื่องระเบียบปฏิบัติในการปฏิบัติการส่งข้อมูลผู้ป่วยทางด้านต่างๆ และประกาศใช้ในโรงพยาบาล
	เพิ่มกระบวนการให้ผู้ป่วยยินยอมให้เปิดเผยข้อมูลเพื่อ การวินิจฉัยและรักษาในช่องทางต่าง ๆ (*ผู้ป่วยในใช้แบบฟอร์ม Informed Consent,ผู้ป่วยนอกใช้ตรายาง)	✓				1.ประชุมหาข้อตกลง ในการออกแบบฟอร์มให้ผู้รับบริการยินยอมเปิดเผยข้อมูล