9.2.5 มีการนำผลการประเมินหรือความสี่ยงที่ยังคงเหลืออยู่ มาปรับปรุงแผนการจัดการความเสี่ยงอย่างต่อเนื่อง

จากการประเมินผลได้นำมาปรับปรุงแผนการจัดการความเสี่ยง ดังนี้

กลยุทธ์ในการแก้ไขความเสี่ยง

โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 จึงจัดทำแผนกลยุทธ์จัดการความเสี่ยงทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

IT - Hardware

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1.1 Server and Main Switches Crash or Failure	10			
		อุปกรณ์ในเครื่องแม่ข่ายเสียหาย	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีการรักษาความเย็นในห้อง Server ให้อยู่ใน 24 องศา ซึ่งยอมรับได้ถึง 26 องศา ถ้าเกินกว่านั้น ต้องรีบหาทางแก้ไข 2. หมั่นตรวจสอบเครื่องสำรองไฟ และเปลี่ยนแบตเตอรี่ทุก 2 ปี 3. จัดหาระบบมอนิเตอร์สถานะ Server
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. จัดทำระบบ DR-Site 2. มีเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันที 3. จัดทำแผนกู้คืนระบบ
1.2 Network Switches Crash or Failure	4			
		อุปกรณ์กระจายสัญญาณเสียหรือมีปัญหา	ลดโอกาสที่จะเกิดเหตุการณ์	1.จัดหาเครื่องสำรองไฟ
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.มีครุภัณฑ์สำรองอย่างน้อย 2 ตัว 2.ดำเนินการตามแผน BCP
		สาย CAT5, CAT6 ที่เชื่อมต่อภายภายในมีปัญหา	ลดโอกาสที่จะเกิดเหตุการณ์	1.จัดทำระบบสายสำรอง
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.จัดหาอุปกรณ์สำรองสำหรับซ่อมแซม 2.ดำเนินการตามแผน BCP
		สาย Fiber Optic เครือข่ายภายในขาดหรือใช้งานไม่ได้	ย้ายกระบวนการซ่อมไปอยู่ในความรับผิดชอบบริษัท	1. จัดทำระบบสายสำรอง 2. ทำสัญญากับบริษัทที่ดำเนินการติดตั้งสาย Fiber Optic ให้โรงพยาบาลดำเนินการแก้ไขภายใน 24 ชั่วโมง หรือน้อยกว่านั้น
			ลดโอกาสที่จะเกิดเหตุการณ์	1.จัดทำระบบสายสัญญาณสำรอง (Link Backup)
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.ดำเนินการตามแผน BCP

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1.3 Workstation and Printers Failure	3			
		เครื่องคอมพิวเตอร์	ลดโอกาสเกิดปัญหา	1. มีแผนการตรวจเช็คอุปกรณ์ ทำความสะอาดคอมพิวเตอร์อย่างน้อย 6 เดือนครั้ง 2. มีทดแทนอุปกรณ์เครื่องเก่าที่ใช้งานมานานเกิน 7 ปี 3. มีเครื่องสำรองไฟใช้กับเครื่องคอมพิวเตอร์ในห้องตรวจทุกเครื่อง
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องคอมพิวเตอร์สำรองพร้อมใช้งาน 2. มีอะไหล่สำรองแต่ละชนิดอย่างน้อย 3-5 ชิ้น
		อุปกรณ์ต่อพ่วงคอมพิวเตอร์ เช่น เครื่องพิมพ์	ลดผลเสียหายที่เกิดย้ายความเสี่ยงไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1.ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดต้องมีการสำรองเครื่องพิมพ์อย่างน้อย 10% ของจำนวนที่ทำสัญญาเช่า
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดให้มีการตรวจสอบเครื่องพิมพ์อย่างน้อย 1 เดือนครั้ง

IT – System Software

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
2.1 Operating System Failure	2			
		OS ในเครื่อง Server มีปัญหา	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันที 2. ดำเนินการ Veeam Restore 3. มีการดำเนินตามแผน DRP 4. มีการดำเนินการตามแผน BCP 5. พัฒนาศักยภาพของบุคลากรในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
		OS ในเครื่อง Client มีปัญหา	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องคอมพิวเตอร์สำรองพร้อมใช้งาน 2.มีอะไหล่สำรองแต่ละชนิดอย่างน้อย 3-5 ชิ้น

IT- Applications

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
3.2 Back Offices	4			
		โปรแกรม Back Offices มีปัญหา	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ดำเนินการตามแผน Backup & Restore 2. ดำเนินการทดสอบ Restore ข้อมูลทุกทุก 1 เดือน 3. มีการดำเนินตามแผน BCP

IT- Communication, Connectivity

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
4.1 Intranet	5			
		ระบบนำเสนอข้อมูลข่าวสารผ่านระบบอินทราเน็ตไม่สามารถใช้งานได้	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ดำเนินการตามแผน Backup & Restore 2. ดำเนินการทดสอบ Restore ข้อมูลทุกทุก 1 เดือน 3. มีการดำเนินตามแผน BCP
4.2 Internet	10			
		ระบบการสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ตไม่สามารถใช้งานได้	ลดโอกาสเกิดความเสียหาย	1. มีผู้ให้บริการอินเตอร์เน็ต อย่างน้อย 2 บริษัทที่ให้บริการในโรงพยาบาล
			ย้ายความเสี่ยงไปยังผู้ให้บริการอินเตอร์เน็ต	1. แจ้งผู้ให้บริการเพื่อดำเนินการแก้ไข

IT – Operational (Human) Error

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
5.1 Backup Error	6			
		ไม่ได้สำรองข้อมูล	ลดโอกาสเกิดเหตุการณ์	แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูล
		สำรองข้อมูลไม่สำเร็จ	ลดโอกาสเกิดเหตุการณ์	แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูลจัดทำระบบ ย้ายไฟล์อัตโนมัติ
		สำรองข้อมูลไม่ได้คุณภาพ	ยอมรับความเสี่ยงเหตุการณ์	มีการสุ่มตรวจสอบข้อมูลที่สำรองไว้ เดือนละ 1 ครั้ง
		พื้นที่ที่สำรองข้อมูลเต็ม	ลดโอกาสเกิดเหตุการณ์	แผนจัดทำระบบแจ้งเตือนอัตโนมัติเมื่อฮาร์ดดิสก์ใกล้เต็ม
5.2 Data Loss Error	2			
		การเข้าถึงข้อมูลและการเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ลดโอกาสเกิดเหตุการณ์	1.กำหนดสิทธิการใช้งาน
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.พัฒนาให้โปรแกรมสามารถเก็บประวัติการใช้งานได้ 2. แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูล 3. มีการเก็บข้อมูลทั้งในระบบเวชระเบียนและในระบบ HIS

Data Loss and Privacy Breach

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
6.2 Data Protection Policy and Regulations	6			
		การเข้าถึงข้อมูลที่บุคลากรไม่มีส่วนเกี่ยวข้อง	ลดโอกาสเกิดเหตุการณ์	1. กำหนดสิทธิการเขาถึงข้อมูลแยกตามหน่วยงาน
6.3 PDPA Implementation	10			
		การเข้าถึงข้อมูลส่วนบุคคล	ลดโอกาสเกิดเหตุการณ์	1. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบายระเบียบ และแนวปฏิบัติแก่บุคลากร ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล

				2. จัดทำนโยบายระเบียบและแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการ และแนวปฏิบัติ

IT – Hacking Unauthorized Intrusions

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
9.1 Hacking Unauthorized Intrusions	15			
		การสวมรอยของผู้ใช้งาน	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีระเบียบปฏิบัติในการห้ามเผยแพร่รหัสผ่านของตนเอง และต้องออกจากระบบเมื่อเลิกใช้งาน 2. มีระบบ Auto logout 5 นาที เมื่อไม่มีการใช้งาน
		การเปิดช่องให้มีการเข้าถึงระบบได้จากภายนอก	ลดโอกาสเกิดเหตุการณ์	1. มีการยืนยันตัวตน หรือการใช้ Token เพื่อเป็นรหัสผ่านในการเข้าถึงข้อมูล 2. การเปิดช่องทางเฉพาะที่ต้องการใช้งานเท่านั้น 3. เปิดให้บริการ Web Service โดยกำหนดเวลา
		เครื่องคอมพิวเตอร์ติดไวรัส	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีการติดตั้ง Antivirus ที่ไม่มีวันหมดอายุ และสามารถอัพเดต และจับไวรัสได้จริง 2. มี Firewall
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. แนะนำให้ผู้ใช้เก็บข้อมูลที่สำคัญในไดร์ฟอื่น

Environment Factors

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
10.1 Flooding – Internal	5			
		โอกาสเกิดน้ำรั่วในห้อง Server	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งพื้นยก (Raised Floor) เหนือจากพื้น 15 ซม.
10.2 Flooding – External	5			
		อำเภอสองพี่น้องเป็นพื้นที่มีโอกาสเกิดน้ำท่วม	ลดผลเสียหายเมื่อเกิดเหตุการณ์	วางแผนรับมือน้ำท่วมโดยทำการย้ายอุปกรณ์มายังจุดที่น้ำท่วมไม่ถึง
10.3 Fire – Internal	5			
		ไฟไหม้เครื่องแม่ข่าย และ ไฟไหม้อุปกรณ์กระจายสัญญาณ	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งอุปกรณ์ดักจับควัน 2. มีป้ายห้ามสูบบุหรี่ ห้ามนำวัสดุติดไฟง่ายเข้าใกล้เครื่องแม่ข่าย

			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีถังดับเพลิงติดตั้งภานในห้อง Server 2. จัดทำระบบ DR-Site 3. ดำเนินการตามแผน DRP 4. ดำเนินการตามแผน BCP
10.4 Fire – External	5			
		การเกิดไฟไหม้ในพื้นที่	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.
10.5 Utilities – Electricity	5			
		ไฟดับ ไฟกระชากทำให้ระบบ Server และระบบ Network ทำงานไม่ได้	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องสำรองไฟสำหรับ server, switch, และ client ที่สำคัญ 2. หมั่นตรวจสอบเครื่องสำรองไฟ และเปลี่ยนแบตเตอรี่ทุก 2 ปี 3. จัดทำระบบ DR-Site 4. ดำเนินการตามแผน DRP 5. ดำเนินการตามแผน BCP
			ย้ายความเสี่ยงไปยังแผนกช่างไฟฟ้า	ระบบไฟฟ้าโรงพยาบาล สามารถทำงานเมื่อเกิดไฟฟ้าดับ ภายใน 10 วินาที
10.6 Criminal – Theft	5			
		การลักขโมย หรือโจรกรรม	ลดโอกาสที่จะเกิดเหตุการณ์	1. ล็อคประตูเมื่อไม่มีเจ้าหน้าที่อยู่ห้อง 2. มีระบบแสกนลายนิ้วมือเพื่อเปิดเข้าห้อง Server 3. มีการติดตั้งกล้องวงจรปิด
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. จัดทำระบบ DR-Site 2. ดำเนินการตามแผน DRP 3. ดำเนินการตามแผน BCP
10.7 Criminal – Break-ins	5			
		การงัดแงะหรือย่องเบา	ลดโอกาสที่จะเกิดเหตุการณ์	1. ล็อคประตูเมื่อไม่มีเจ้าหน้าที่อยู่ห้อง 2. มีระบบแสกนลายนิ้วมือเพื่อเปิดเข้าห้อง Server 3. มีการติดตั้งกล้องวงจรปิด
10.8 Civil Unrest – Protest, Mob	25			
		เมื่อมีการชุมนุมหรือเหตุจลาจล	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. จัดทำระบบ DR-Site 2. ดำเนินการตามแผน DRP 3. ดำเนินการตามแผน BCP

Patient Risks due to IT Errors/Misuse

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
	4			

11.1 Patient Risks due to IT Errors/Misuse		จุดอ่อนการใช้เทคโนโลยีที่ทำให้เกิดอันตรายต่อผู้ป่วย	ลดโอกาสที่จะเกิดเหตุการณ์	1. อบรมเจ้าหน้าที่ให้มีความรู้ด้านเทคโนโลยีสารสนเทศ นิยามและความสำคัญของการรู้สารสนเทศ

ตารางการจัดการความเสี่ยง (Risk Treatment Table)

ลำดับ	ความเสี่ยง (Risk)	ความรุนแรง (Impact)	โอกาสเกิด (Likelihood)	ระดับความเสี่ยง	วิธีการจัดการ (Treatment)	ผู้รับผิดชอบ	ระยะเวลา
1.	ระบบ HIS ล่ม	สูง	กลาง	สูง	จัดทำ DR Site และสำรองข้อมูลอัตโนมัติ	หัวหน้า IT	ภายใน 2570
2.	มัลแวร์/ไวรัสโจมตี	สูง	สูง	สูง	ติดตั้ง Endpoint Protection, อัปเดต Patch ระบบ	IT Support	ต่อเนื่อง
3.	การเข้าถึงข้อมูลผู้ป่วยโดยไม่ได้รับอนุญาต	สูง	กลาง	สูง	จำกัดสิทธิ์ผู้ใช้ตามบทบาท, Audit Log	Admin & Security	ต่อเนื่อง
4	ข้อมูลสูญหายจากฮาร์ดแวร์ชำรุด	กลาง	กลาง	กลาง	สำรองข้อมูลรายวัน, ตรวจสอบ Hardware	จพ.เครื่องคอมพิวเตอร์	รายวัน
5	ไฟฟ้าดับกระทันหัน	กลาง	สูง	กลาง	ติดตั้ง UPS และเครื่องปั่นไฟ	งานอาคารสถานที่	เสร็จแล้ว
6	การโจมตีจากภายนอก (DDoS)	สูง	ต่ำ	กลาง	ใช้ Firewall/IPS และระบบเฝ้าระวัง	Network Admin	2569
7	ความรู้ไม่เพียงพอของเจ้าหน้าที่	กลาง	สูง	กลาง	จัดอบรมความรู้ด้าน IT Security เป็นประจำ	HR ร่วมกับ IT	2569

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ชื่อกลุ่มงาน กลุ่มงานเทคโนโลยีสารสนเทศ **วันที่จัดทำ** 1 กุมภาพันธ์ 2568

เรื่อง	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
เครื่องแม่ข่าย (Server) ล่มหรือมีปัญหา	- อุปกรณ์ในเครื่องแม่ข่ายเสียหาย	1. จัดทำ DR-Site ภายในโรงพยาบาล 2. จัดทำ DR-Site ต่างโรงพยาบาล 3. จัดหาระบบมอนิเตอร์สถานะ Server	กง.เทคโนโลยีสารสนเทศ	500,000 2,000,000 -	ปีงบประมาณ 2569 ปีงบประมาณ 2570 ปีงบประมาณ 2568
ระบบเครือข่ายล่มหรือมีปัญหา	- อุปกรณ์กระจายสัญญาณเสียหรือมีปัญหา - สาย Lan ที่เชื่อมต่อภายภายในมีปัญหา	1.จัดหา Switch สำรอง 2.ปรับปรุงระบบเครือข่าย (Main Switch) 3. ปรับปรุงสาย CAT5 เป็น CAT6 ทั้งหมด	กง.เทคโนโลยีสารสนเทศ	500,000 500,000	ปีงบประมาณ 2568 ปีงบประมาณ 2569
เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงในหน่วยงานมีปัญหา	- เครื่องคอมพิวเตอร์มีปัญหา - เครื่องพิมพ์มีปัญหา	1. จัดหาคอมพิวเตอร์ทดแทนเครื่องที่ใช้งานเกิน 5 ปี และจัดหาเครื่องสำรองอย่างน้อย 5 ตัว 2. ทำแผนจัดหาอะไหล่สำรอง * อยู่ในแผนจัดหาวัสดุ ปี 2568 1.มีสำรอง 10 เครื่องจากการเช่า	กง.เทคโนโลยีสารสนเทศ	128,800 458,120	ปีงบประมาณ 2568 ปีงบประมาณ 2568

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ชื่อกลุ่มงาน กลุ่มงานเทคโนโลยีสารสนเทศ **วันที่จัดทำ** 1 กุมภาพันธ์ 2568

เรื่อง	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
ระบบปฏิบัติการมีปัญหา	- OS ในเครื่อง Server มีปัญหา - OS ในเครื่อง Client มีปัญหา	1. พัฒนาศักยภาพของบุคคลากรในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อดูแลและแก้ไขปัญหาได้ 2. ทำแผนจัดหาอะไหล่สำรอง * อยู่ในแผนจัดหาวัสดุ ปี 2568	กง.เทคโนโลยีสารสนเทศ	- 458,120	ปีงบประมาณ 2568 ปีงบประมาณ 2569
โปรแกรมสำหรับให้บริการทางการแพทย์ โปรแกรม HIS	- โปรแกรม HIS มีปัญหา ไม่สามารถใช้งานได้	1. พัฒนาศักยภาพของบุคลากรในกง.เทคโนโลยีสารสนเทศโดยการส่งไปอบรมเกี่ยวกับกำกับดูแลเครื่องแม่ข่าย (Server)	กง.เทคโนโลยีสารสนเทศ	30,000	ปีงบประมาณ 2569
การสำรองข้อมูลผิดพลาด	- ไม่ได้สำรองข้อมูล - พื้นที่ที่สำรองข้อมูลเต็ม - ข้อมูลมีการสูญหายหรือข้อผิดพลาด	1. แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูล 2. มีการสุ่มตรวจสอบข้อมูลที่สำรองไว้ ทุก 1 เดือน 3. แผนจัดทำระบบแจ้งเตือนอัตโนมัติเมื่อฮาร์ดดิสก์ที่ใช้งานมาก 90%	กง.เทคโนโลยีสารสนเทศ	-	ปีงบประมาณ 2569
ระบบการสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ตไม่สามารถใช้งานได้	- อุปกรณ์กระจายสัญญาณเสียหรือมีปัญหา - สาย Fiber Optic เครือข่ายขาดหรือใช้งานไม่ได้	1. มีผู้ให้บริการอินเตอร์เน็ต อย่างน้อย 2 บริษัทที่ให้บริการในโรงพยาบาล	กง.เทคโนโลยีสารสนเทศ	15,600	ดำเนินการแล้ว
ผู้ให้บริการหยุด ให้บริการ	- ผู้ให้บริการระบบ Server หรือ Network หยุดให้การบริการ	1. พัฒนาศักยภาพของบุคคลากรในศูนย์คอมพิวเตอร์ให้สามารถดูแลระบบได้	กง.เทคโนโลยีสารสนเทศ	-	ปีงบประมาณ 2570

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ชื่อกลุ่มงาน กง.เทคโนโลยีสารสนเทศ **วันที่จัดทำ** 1 กุมภาพันธ์ 2568

เรื่อง	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
การเข้าถึงข้อมูลส่วนบุคคล	- ข้อมูลส่วนบุคคลรั่วไหล	1. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบายระเบียบ และแนวปฏิบัติแก่บุคลากรตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล 2.จัดทำนโยบายระเบียบและแนวปฏิบัติ ในการจัดการข้อมูลส่วนบุคคลรวมถึงทบทวนมาตรการและแนวปฏิบัติ	กง.เทคโนโลยีสารสนเทศ		ปีงบประมาณ 2568
การถูกโจมตีจากภายนอก	- เครื่องคอมพิวเตอร์ติดไวรัส	1. จัดหาโปรแกรมป้องกันไวรัส	กง.เทคโนโลยีสารสนเทศ	280,000	ดำเนินการแล้ว
อัคคีภัย	- ไฟไหม้เครื่องแม่ข่าย และ ไฟไหม้อุปกรณ์กระจายสัญญาณ	1. แผนอัคคีภัยของโรงยาบาล 2. จัดทำ DR-Site ภายในโรงพยาบาล 3. จัดทำ DR-Site ต่างโรงพยาบาล	กง.เทคโนโลยีสารสนเทศ	500,000 2,000,000 2,000,000	ปีงบประมาณ 2568 ปีงบประมาณ 2568 ปีงบประมาณ 2570
โจรกรรม – ลักขโมย	- การลักขโมย	1. จัดทำ DR-Site ภายในโรงพยาบาล 2. จัดทำ DR-Site ต่างโรงพยาบาล	กง.เทคโนโลยีสารสนเทศ	2,000,000 2,000,000	ปีงบประมาณ 2568 ปีงบประมาณ 2570