รับเรื่องจาก
เลขที่รับ 2856
วันที่ ๒๕ มี.ค. ๒๕๖๙

บันทึกข้อความ

ส่วนราชการ กลุ่มงานเทคโนโลยีสารสนเทศ โรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ โทร ๘๒๐๗
ที่ สพ ๐๐๓๓.๐๕/๐๒๘๕๖ **วันที่** ๒๓ มีนาคม ๒๕๖๙
เรื่อง ขอพิจารณาเห็นชอบและประกาศใช้คู่มือการปฏิบัติงาน (SOP) กระบวนงานการสำรองข้อมูลสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

เรียน ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗

ด้วย กลุ่มงานเทคโนโลยีสารสนเทศ ได้จัดทำคู่มือการปฏิบัติงาน (Standard Operating Procedure : SOP) กระบวนงานการสำรองข้อมูลสารสนเทศ ของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ เพื่อกำหนดแนวทางและมาตรฐานในการดำเนินงานด้านการสำรองข้อมูลสารสนเทศของโรงพยาบาล ให้สามารถป้องกันการสูญหายของข้อมูลและรองรับการกู้คืนข้อมูลเมื่อเกิดเหตุขัดข้องของระบบสารสนเทศ ซึ่งอาจส่งผลกระทบต่อการให้บริการของโรงพยาบาล ทั้งนี้ โรงพยาบาลได้กำหนดแนวทางการสำรองข้อมูลตามหลัก ๓-๒-๑ Backup Rule โดยให้มีการสำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง และสามารถกู้คืนข้อมูลย้อนหลังได้ไม่น้อยกว่า ๗ วัน เพื่อให้การบริหารจัดการข้อมูลสารสนเทศของโรงพยาบาลมีความมั่นคงปลอดภัยและสนับสนุนความต่อเนื่องในการให้บริการ

ในการนี้ เพื่อให้การดำเนินงานด้านการสำรองข้อมูลสารสนเทศของโรงพยาบาลเป็นไปอย่างมีมาตรฐานและเป็นแนวทางปฏิบัติเดียวกัน จึงเห็นควรเสนอเพื่อโปรดพิจารณาเห็นชอบ คู่มือการปฏิบัติงาน (SOP) กระบวนงานการสำรองข้อมูลสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗ และอนุมัติให้ประกาศใช้เป็นแนวทางปฏิบัติภายในโรงพยาบาล พร้อมทั้งมอบหมายให้กลุ่มงานเทคโนโลยีสารสนเทศดำเนินการตามคู่มือดังกล่าวและติดตามรายงานผลการสำรองข้อมูลอย่างต่อเนื่องต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา

(นางปาริชาติ กลั่นแกล้ว)
หัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

(นายปวริศ สังขันธ์)
รองผู้อำนวยการด้านภารกิจสุขภาพดิจิทัล

เรียน ผอก.ร.พ.สมเด็จพระสังฆราช องค์ที่ ๑๗
☐ เพื่อโปรดทราบ
☑ เพื่อพิจารณาและสั่งการ
☑ เห็นสมควรมอบ IT
๒๕ มี.ค ๖๙

ทราบ/ชอบ

(นายจิรภัทร กัลยาณพจน์พร)
ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราช องค์ที่ ๑๗
๒๕ มี.ค. ๒๕๖๙

คู่มือการปฏิบัติงาน (SOP) กระบวนงานการสำรองข้อมูลสารสนเทศ
กลุ่มงานเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อกำหนดแนวทางในการปฏิบัติงานด้านการสำรองข้อมูลสารสนเทศของโรงพยาบาลให้เป็นไปตามมาตรฐานที่กำหนด สามารถป้องกันการสูญหายของข้อมูล และรองรับการกู้คืนข้อมูลเมื่อเกิดเหตุขัดข้องของระบบสารสนเทศ ซึ่งอาจส่งผลกระทบต่อการให้บริการของโรงพยาบาล

โรงพยาบาลดำเนินการสำรองข้อมูลตามหลัก ๓-๒-๑ Backup Rule โดยกำหนดให้มีการสำรองข้อมูลอย่างน้อย วันละ ๑ ครั้ง และสามารถย้อนหลังข้อมูลได้อย่างน้อย ๗ วัน

๒. ขอบเขต

คู่มือนี้ใช้เป็นแนวทางในการดำเนินการสำรองข้อมูลของระบบสารสนเทศที่อยู่ภายใต้ความรับผิดชอบของกลุ่มงานเทคโนโลยีสารสนเทศ โดยครอบคลุมระบบและอุปกรณ์ที่เกี่ยวข้อง ดังนี้

(๑) ระบบสารสนเทศโรงพยาบาล (Hospital Information System : HIS)

(๒) เครื่องแม่ข่ายระบบสารสนเทศ (Server)

(๓) ระบบเครื่องเสมือน (Virtual Machine : VM)

(๔) ระบบจัดเก็บข้อมูลบนเครือข่าย (Network Attached Storage : NAS)

(๕) อุปกรณ์จัดเก็บข้อมูลสำรองภายนอก (External Storage Drive)

ทั้งนี้ กำหนดให้มีการสำรองข้อมูลอย่างน้อย วันละ ๑ ครั้ง และจัดเก็บข้อมูลสำรองย้อนหลังได้อย่างน้อย ๗ วัน เพื่อรองรับการกู้คืนข้อมูลในกรณีที่เกิดเหตุขัดข้องของระบบสารสนเทศ

๓. กระบวนงานการสำรองข้อมูลสารสนเทศ

กระบวนงานการสำรองข้อมูลสารสนเทศ ประกอบด้วยองค์ประกอบและอุปกรณ์ที่ใช้ในการดำเนินการ ดังนี้

(๑) เครื่องแม่ข่าย (Server) สำหรับจัดเก็บและประมวลผลข้อมูลของระบบสารสนเทศ

(๒) อุปกรณ์จัดเก็บข้อมูลบนเครือข่าย (Network Attached Storage : NAS) สำหรับใช้เป็นพื้นที่จัดเก็บข้อมูลสำรองผ่านระบบเครือข่าย

(๓) อุปกรณ์จัดเก็บข้อมูลภายนอก (External Storage Drive) สำหรับใช้ในการสำรองข้อมูลแบบหมุนเวียนรายวัน

รายละเอียดกระบวนงานการสำรองข้อมูลสารสนเทศตามเอกสารแนบท้าย

๔. รายละเอียดขั้นตอนการปฏิบัติงาน

ขั้นตอนที่ ๑ ตรวจสอบสถานะเครื่องแม่ข่ายระบบสารสนเทศ

เจ้าหน้าที่ผู้ดูแลระบบดำเนินการตรวจสอบสถานะของเครื่องแม่ข่ายระบบสารสนเทศภายในห้อง Data Center เพื่อให้มั่นใจว่าระบบมีความพร้อมสำหรับการสำรองข้อมูล โดยตรวจสอบรายการ ดังนี้

(๑) สถานะการทำงานของระบบ Server

(๒) พื้นที่จัดเก็บข้อมูลของระบบ

(๓) สถานะการเชื่อมต่อของระบบเครือข่าย

(๔) สถานะการทำงานของระบบ Virtual Machine (VM)

ขั้นตอนที่ ๒ ดำเนินการสำรองข้อมูลจากเครื่องแม่ข่ายหลัก

ดำเนินการสำรองข้อมูลจากเครื่องแม่ข่ายหลัก (Server) ไปยังระบบสำรองข้อมูลตามรอบเวลาที่กำหนด โดยกำหนดให้มีการสำรองข้อมูลอย่างน้อย **วันละ ๑ ครั้ง** ครอบคลุมข้อมูลที่สำคัญของระบบสารสนเทศ ได้แก่

(๑) ฐานข้อมูลของระบบ Hospital Information System (HIS)

(๒) ระบบเครื่องเสมือน Virtual Machine (VM)

(๓) ไฟล์ระบบสารสนเทศและข้อมูลสำคัญของระบบงาน

ขั้นตอนที่ ๓ การสำรองข้อมูลไปยัง NAS Storage (Online Backup)

ระบบดำเนินการสำรองข้อมูลไปยัง Network Attached Storage (NAS) ภายในองค์กร เพื่อใช้เป็นพื้นที่จัดเก็บข้อมูลสำรองแบบ Online Backup โดยมีการจัดเก็บข้อมูลในอุปกรณ์ ดังต่อไปนี้

(๑) NAS เครื่องที่ ๑

(๒) NAS เครื่องที่ ๒

ทั้งนี้ อุปกรณ์ NAS ทั้งสองเครื่องตั้งอยู่ในตำแหน่งที่แตกต่างกัน เพื่อลดความเสี่ยงจากเหตุการณ์ความเสียหายที่อาจเกิดขึ้นในสถานที่เดียวกัน และรองรับการกู้คืนข้อมูลได้อย่างรวดเร็ว

ขั้นตอนที่ ๔ การสำรองข้อมูลลง External Storage Drive (Offline Backup)

ดำเนินการสำรองข้อมูลลง External Storage Drive เพื่อจัดเก็บข้อมูลสำรองแบบ Offline Backup โดยใช้อุปกรณ์จำนวน **๗ ชุด** หมุนเวียนตามวันในสัปดาห์ ได้แก่

(๑) วันจันทร์

(๒) วันอังคาร

(๓) วันพุธ

(๔) วันพฤหัสบดี

(๕) วันศุกร์

(๖) วันเสาร์

(๗) วันอาทิตย์

ภายหลังจากดำเนินการสำรองข้อมูลแล้ว ให้ถอดอุปกรณ์ออกจากระบบและจัดเก็บไว้ในสถานที่ที่มีความปลอดภัย เพื่อป้องกันความเสียหายที่อาจเกิดจาก Malware Ransomware และ ความเสียหายของระบบหลัก

ขั้นตอนที่ ๕ การตรวจสอบความสมบูรณ์ของข้อมูลสำรอง

เจ้าหน้าที่ผู้ดูแลระบบดำเนินการตรวจสอบความสมบูรณ์ของข้อมูลสำรอง เพื่อยืนยันว่าการสำรองข้อมูลดำเนินการสำเร็จและไม่มีข้อผิดพลาด (error) โดยตรวจสอบรายการ ดังนี้

(๑) บันทึกเหตุการณ์การสำรองข้อมูล (Backup Log)

(๒) ขนาดไฟล์ข้อมูลสำรอง (Backup File Size)

(๓) สถานะการคัดลอกข้อมูล (Copy Status)

ขั้นตอนที่ ๖ การบันทึกผลการดำเนินงาน

ดำเนินการบันทึกผลการสำรองข้อมูลประจำวัน เพื่อใช้เป็นหลักฐานในการตรวจสอบตามหลักธรรมาภิบาลข้อมูลและการกำกับดูแลด้านเทคโนโลยีสารสนเทศ โดยระบบจะแจ้งเตือน (Notify Alert) ผลการสำรองข้อมูลให้ผู้รับผิดชอบทราบโดยอัตโนมัติดังนี้

(๑) รายงานผลการสำรองข้อมูลประจำวัน พร้อมการแจ้งเตือนผ่านระบบ Notify Alert

๕. รูปแบบการสำรองข้อมูล (๓-๒-๑ Backup)

โรงพยาบาลดำเนินการสำรองข้อมูลสารสนเทศตามหลัก **๓-๒-๑ Backup Rule** เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูลและรองรับการกู้คืนระบบในกรณีเกิดเหตุขัดข้อง โดยมีรายละเอียด ดังนี้

๕.๑ การจัดเก็บข้อมูลสำรองจำนวน ๓ ชุด

(๑) ข้อมูลต้นฉบับ จัดเก็บใน เครื่องแม่ข่ายหลัก (Server)

(๒) ข้อมูลสำรองชุดที่ ๑ จัดเก็บใน NAS Storage

(๓) ข้อมูลสำรองชุดที่ ๒ จัดเก็บใน External Storage Drive

๕.๒ การจัดเก็บข้อมูลบนสื่ออย่างน้อย ๒ ประเภท

ข้อมูลสำรองถูกจัดเก็บในสื่อจัดเก็บข้อมูลอย่างน้อย ๒ ประเภท ได้แก่

(๑) NAS Storage

(๒) External Storage Drive

๕.๓ การจัดเก็บข้อมูลสำรองแบบ Offline อย่างน้อย ๑ ชุด

กำหนดให้มีข้อมูลสำรองแบบ Offline Backup อย่างน้อย ๑ ชุด โดยจัดเก็บใน External Storage Drive และถอดการเชื่อมต่อจากระบบเมื่อไม่ใช้งาน

๖. โครงสร้างอุปกรณ์สำรองข้อมูล

โรงพยาบาลมีอุปกรณ์สำหรับการสำรองข้อมูลสารสนเทศ ดังนี้

(๑) NAS Storage จำนวน ๒ เครื่อง : สำหรับจัดเก็บข้อมูลสำรองภายในเครือข่ายขององค์กร (Online Backup) เพื่อรองรับการกู้คืนข้อมูลได้อย่างรวดเร็ว

(๒) External Storage Drive จำนวน ๗ ชุด : สำหรับสำรองข้อมูลแบบหมุนเวียนรายวันตามวันในสัปดาห์ เพื่อให้สามารถกู้คืนข้อมูลย้อนหลังได้ ไม่น้อยกว่า ๗ วัน

๗. การกำหนดค่า RPO และ RTO

(๑) Recovery Point Objective (RPO) : กำหนดระยะเวลาการสูญหายของข้อมูลที่ยอมรับได้ไม่เกิน ๒๔ ชั่วโมง (สามารถกู้คืนข้อมูลย้อนหลังได้ไม่เกิน ๑ วัน)

(๒) Recovery Time Objective (RTO) : กำหนดระยะเวลาในการกู้คืนระบบให้กลับมาใช้งานได้ไม่เกิน ๒๔ ชั่วโมง ภายหลังเกิดเหตุขัดข้องของระบบสารสนเทศ

กระบวนงานการสำรองข้อมูลสารสนเทศ
กลุ่มงานเทคโนโลยีสารสนเทศ

วัตถุประสงค์ : เพื่อเป็นแนวทางในการปฏิบัติตามขั้นตอนของการสำรองข้อมูลสำคัญขององค์กรให้เป็นไปตามมาตรฐานที่กำหนด

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	จุดควบคุมความเสี่ยง	ระยะเวลา
นายศิลา กลั่นแกล้ว นายสมเจตน์ บุญยิ้ม	ตรวจสอบสถานะ Server และระบบเครือข่าย	ต้องไม่มี Error ของระบบ	๕ นาที / ครั้ง
นายศิลา กลั่นแกล้ว นายสมเจตน์ บุญยิ้ม	สำรองข้อมูลจาก Server หลัก	ระบบ Backup ต้องทำงานตามเวลาที่กำหนด	อัตโนมัติ
นายศิลา กลั่นแกล้ว นายสมเจตน์ บุญยิ้ม	สำรองข้อมูลไปยัง NAS	ตรวจสอบไฟล์ Backup	๑-๒ ชั่วโมง/ครั้ง
นายศิลา กลั่นแกล้ว นายสมเจตน์ บุญยิ้ม	สำรองข้อมูลลง External Drive	ต้องถอดอุปกรณ์หลังใช้งาน	๖-๘ ชั่วโมง/ครั้ง
นายศิลา กลั่นแกล้ว นายสมเจตน์ บุญยิ้ม	ตรวจสอบ Log การสำรองข้อมูลทุกระบบ เพื่อยืนยันว่าไม่มี Error และข้อมูลสำรองครบถ้วน	ไม่พบ Error Log และ Sync ต้องสมบูรณ์	๑๐ นาที / ครั้ง
นายศิลา กลั่นแกล้ว นายสมเจตน์ บุญยิ้ม	การบันทึกผลการดำเนินงาน	มีหลักฐานบันทึกการดำเนินงาน	๕ นาที / ครั้ง
รวมระยะเวลาในการดำเนินการประมาณ *(ไม่รวมกระบวนการสำรองข้อมูลแบบอัตโนมัติและแบบ Real-time ที่ระบบดำเนินการต่อเนื่องตลอดเวลา)			๑๑ ชั่วโมงต่อครั้ง

ตารางวิเคราะห์ระดับความเสี่ยง
กระบวนงานการสำรองข้อมูลสารสนเทศ
กลุ่มงานเทคโนโลยีสารสนเทศ

ภารกิจตามกฎหมาย/ แผนงาน/ ภารกิจอื่น ที่สำคัญ/ขั้นตอน	วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง				ลำดับความเสี่ยง
				โอกาส	ผลกระทบ	ระดับความเสี่ยง		
						คะแนน	ระดับ	
๑.Backup Server	ป้องกันข้อมูลสูญหาย	Backup ไม่สำเร็จ	ระบบตั้งเวลาไม่ทำงาน	๒	๔	๘	ปานกลาง	๑
๒. NAS Backup	ข้อมูลต่อเนื่อง	NAS เสียหาย	Hardware Failure	๒	๔	๘	ปานกลาง	๒
๓. External Backup	ป้องกัน Ransomware	ไม่ถอด HDD	Human Error	๒	๔	๘	ปานกลาง	๔
๔. Monitoring	ตรวจสอบความถูกต้อง	ไม่ตรวจ Log	ขาดการติดตาม	๓	๓	๙	ปานกลาง	๓
๕. Storage	ตรวจสอบความถูกต้อง	HDD เสีย	อายุการใช้งาน	๒	๔	๘	ปานกลาง	๕

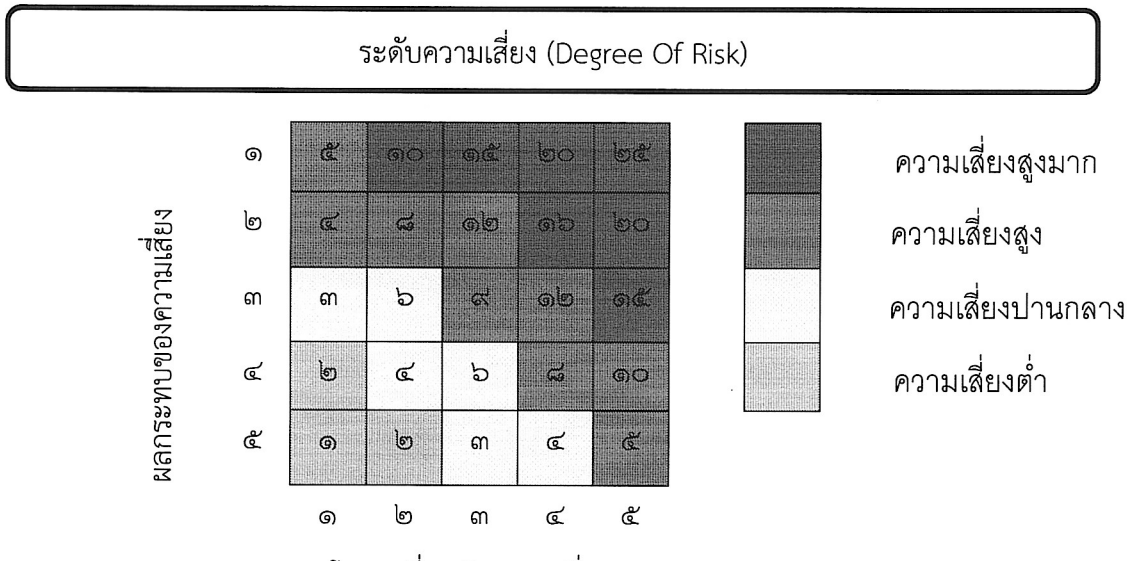
ตารางวิเคราะห์ระดับความเสี่ยง
เกณฑ์การประเมินระดับโอกาสของความถี่ที่จะเกิดขึ้น

๑. ผลกระทบต่อการให้บริการของโรงพยาบาล

ผลกระทบที่เกิดขึ้น	ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง
ระบบ HIS ไม่สามารถใช้งานได้ ส่งผลให้การรักษาพยาบาลหยุดชะงักทั้งโรงพยาบาล	๕	สูงมาก
ระบบสารสนเทศหลักใช้งานไม่ได้บางส่วน ต้องใช้ระบบสำรองหรือทำงาน Manual	๔	สูง
ระบบล่าช้า หรือเข้าถึงข้อมูลผู้ป่วยไม่ได้ชั่วคราว	๓	ปานกลาง
ระบบมีปัญหาเล็กน้อย ไม่กระทบการรักษา	๒	น้อย
ไม่มีผลกระทบต่อการให้บริการ	๑	น้อยมาก

๒. ผลกระทบต่อข้อมูลและความต่อเนื่องของระบบสารสนเทศ

ผลกระทบที่เกิดขึ้น	ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง
สูญหายข้อมูลผู้ป่วยจำนวนมากไม่สามารถกู้คืนได้	๕	สูงมาก
สูญหายข้อมูลบางช่วงเวลา ต้องกู้คืนจาก Backup ก่อนหน้า	๔	สูง
ข้อมูลไม่สมบูรณ์ ต้องตรวจสอบและปรับปรุงข้อมูล	๓	ปานกลาง
สูญหายข้อมูลเล็กน้อย สามารถกู้คืนได้ทันที	๒	น้อย
ไม่มีข้อมูลสูญหาย	๑	น้อยมาก



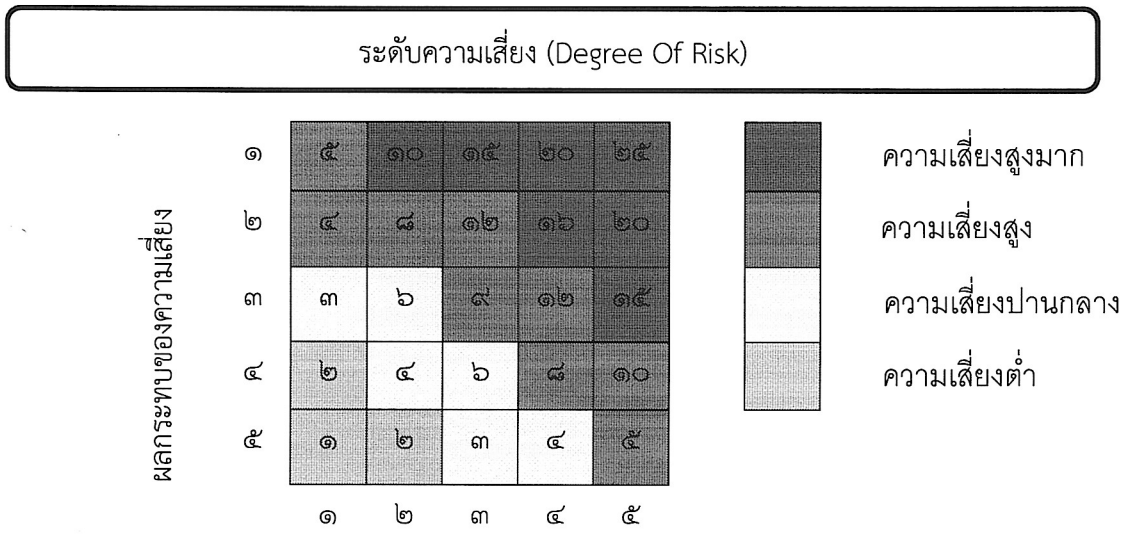
ตารางวิเคราะห์ระดับความเสี่ยง
เกณฑ์การประเมินระดับผลกระทบความเสี่ยงที่จะเกิดขึ้น

๓. ผลกระทบต่อการให้บริการของโรงพยาบาล

ผลกระทบที่เกิดขึ้น	ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง
ระบบ HIS ไม่สามารถใช้งานได้ ส่งผลให้การรักษาพยาบาลหยุดชะงักทั้งโรงพยาบาล	๕	สูงมาก
ระบบสารสนเทศหลักใช้งานไม่ได้บางส่วน ต้องใช้ระบบสำรองหรือทำงาน Manual	๔	สูง
ระบบล่าช้า หรือเข้าถึงข้อมูลผู้ป่วยไม่ได้ชั่วคราว	๓	ปานกลาง
ระบบมีปัญหาเล็กน้อย ไม่กระทบการรักษา	๒	น้อย
ไม่มีผลกระทบต่อการให้บริการ	๑	น้อยมาก

๔. ผลกระทบต่อข้อมูลและความต่อเนื่องของระบบสารสนเทศ

ผลกระทบที่เกิดขึ้น	ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง
สูญหายข้อมูลผู้ป่วยจำนวนมากไม่สามารถกู้คืนได้	๕	สูงมาก
สูญหายข้อมูลบางช่วงเวลา ต้องกู้คืนจาก Backup ก่อนหน้า	๔	สูง
ข้อมูลไม่สมบูรณ์ ต้องตรวจสอบและปรับปรุงข้อมูล	๓	ปานกลาง
สูญหายข้อมูลเล็กน้อย สามารถกู้คืนได้ทันที	๒	น้อย
ไม่มีข้อมูลสูญหาย	๑	น้อยมาก



แบบสอบถามการประเมินกระบวนงานการสำรองข้อมูลสารสนเทศ
กลุ่มงานเทคโนโลยีสารสนเทศ

แบบสอบถามฉบับนี้จัดทำขึ้นเพื่อใช้ในการประเมินการดำเนินงานด้านการสำรองข้อมูลสารสนเทศของโรงพยาบาลให้เป็นไปตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงรองรับการตรวจสอบและประเมินผลจากหน่วยงานกำกับดูแล

แบบสอบถามด้านกระบวนงานการสำรองข้อมูลสารสนเทศ

คำถาม	มี/ใช่	ไม่มี/ไม่ใช่	คำอธิบาย/คำตอบ
การตรวจสอบก่อนสำรองข้อมูล			
๑. มีการสำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง			
๒. สามารถกู้คืนข้อมูลย้อนหลังได้อย่างน้อย ๗ วัน			
๓. มีการสำรองข้อมูลไปยัง NAS Storage			
๔. มีการสำรองข้อมูลลง External Storage Drive			
๕. มีการถอด External Drive หลัง Backup			
๖. มีการตรวจสอบ Log Backup			
๗. มีรายงานสรุปผล Backup			
๘. มีการกำหนดค่า RPO และ RTO			

สรุป ด้านงานกระบวนงานการสำรองข้อมูลสารสนเทศเป็นไปตามมาตรฐานวิชาชีพ

ชื่อ ผู้รายงาน นางปาริชาติ กลั่นแกล้ว
หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
วันที่.....