การประเมินความเสี่ยงที่มีผลต่อข้อมูลการให้บริการลูกค้า (Risk Assessment Report)

พื้นที่/หน่วยงาน			วันที่จัดทำ						ผู้จัดทำ		ผู้อนุมัติ			
Asset / Process	Threats	Vulnerability	Impact			Evaluate		Risk Level ระดับความเสี่ยง	Existing Control (ระบุมาตรการควบคุมที่มี)	Related Risk Treatement Plan แผนจัดการความเสี่ยง	Plan Status สถานะ	Residual		Risk Level ระดับความเสี่ยง
			Confidentiality	Integrity	Availability	Probability	Impact					Probability	Impact	
Computer PC / Lab top	Virus	บุคลากรนำอุปกรณ์ภายนอกมาเชื่อมต่อ เช่น Flash drive, External harddisk เป็นต้น	x	x	x	2	2	Low(4)	1.แสกนไวรัสทุกอุปกรณ์ทุกวันก่อนใช้งาน 2. ก่อนใช้งานทุกครั้งต้องสแกนไวรัสทุกอุปกรณ์ที่นำมาเชื่อมต่อ	1.ตั้งค่าใช้งานเครื่องคอมพิวเตอร์ไม่ให้ใช้ Port Storage ใน Registry ได้ ในเครื่องที่เก็บข้อมูลสำคัญ				
		บุคลากรดาวน์โหลดไฟล์หรือซอฟต์แวร์หรือเข้าเว็บไซต์ที่ไม่ปลอดภัย	x	x	x	3	2	Medium(6)	1.อุปกรณ์ทุกตัวมี firewall ป้องกัน 2.บุคลากรต้องตรวจสอบไฟล์หรือลิงค์ก่อนดาวน์โหลดข้อมูล	1.ฝึกอบรมการกำหนดค่าการใช้งาน Firewall ได้เอง				
		เครื่องคอมพิวเตอร์ลูกข่ายติดไวรัส	x	x	x	2	3	Medium(6)	1.มีการทำ VLAN แต่ไม่ครบ ทุกหน่วย 2.ใช้ Firewall	1.พัฒนา VLAN ให้ครอบคลุมทั้ง รพ.				
		ไม่อัพเดตซอฟต์แวร์อย่างสม่ำเสมอ	x	x	x	1	2	Low(2)	ยังไม่มีแนวทางป้องกันสำหรับเครื่องที่ไม่ได้ต่อ Net	กำหนดค่าใน Firewall / ติดตั้ง Server Update ภายใน				
	อุปกรณ์สูญหาย	1.บุคลากรนำอุปกรณ์ออกไปจากพื้นที่โดยไม่ได้รับอนุญาตและไม่สามารถตรวจสอบได้(อาจจะตัดออกเนื่องจากไม่เคยเกิด และเสี่ยงต่ำ)	x			1	4	Low(4)	1.ยังไม่มีแนวทางป้องกันและตรวจสอบ	1.กำหนดผู้รับผิดชอบที่มีสิทธิ์ในการนำอุปกรณ์ออกจากพื้นที่ 2. ติดตั้งกล้องวงจรปิดที่สามารถมองเห็นอุปกรณ์ทุกตัว 3.ตรวจสอบอุปกรณ์ตามความถี่ที่กำหนด				

External hard disk	ติด Virus	นำไปใช้กับเครื่องอื่นที่ไม่ปลอดภัย	x	x	x	1	1	Low(1)	แผน Scan Virus สม่ำเสมอ	กำหนดให้ใช้งานเฉพาะงานอัพแบ็คอัพ Server เท่านั้น				
	Hardware เสื่อมประสิทธิภาพและตกรุ่น	การเปลี่ยนแปลงของเทคโนโลยีและระยะเวลาในการใช้งาน		x	x	1	1	Low(1)	1.ขอซื้อสำรอง 2.กำหนดการบำรุงรักษาเชิงป้องกัน					
	ข้อมูลสูญหาย	ถูกขโมย	x	x	x	1	5	Medium(5)	มีการเข้ารหัสข้อมูลสำคัญ	จัดเก็บในที่ๆปลอดภัย เช่น ตู้นิรภัย				
บุคลากรหรือบุคคลภายนอก	1.นำข้อมูลไปเปิดเผยสู่ภายนอก เช่น -แผนผัง,ที่ตั้งห้อง server -อุปกรณ์ ยี่ห้อ สเปค ของอุปกรณ์ -ข้อมูลการรักษาของผู้ป่วย	ขาดความตระหนัก ขาดความรู้ ในเรื่องความปลอดภัยของข้อมูลสารสนเทศ	x	x	x	1	5	Medium(5)	1.ชี้แจงการรักษาความลับ ทำสัญญารักษาความลับสำหรับบุคคลภายนอก 2.อบรม security awareness ให้บุคลากรทุกปี	จัดทำแผนตั้งรับในกรณีถูกนำข้อมูลไปเปิดเผย				
	2.ทำอุปกรณ์ชำรุดเสียหาย เช่น -ช่างเข้ามาซ่อมแอร์แล้วทำน้ำหยอดใส่อุปกรณ์ -ช่างดูแลอินเตอร์เน็ต เข้ามาให้บริการ อาจจะต่อสายผิด -ช่างที่มาให้บริการเดินหนอุปกรณ์อื่น ๆ ในห้อง server	ขาดความระมัดระวังในการปฏิบัติงาน	x	x	x	2	3	Medium(6)	1.มีผู้สังเกตการด้วยตลอดเวลา	1.จัดทำข้อมูลลดกลงในการปฏิบัติงาน 2.ติดตั้งกล้องวงจรปิด				