แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโรงพยาบาลบ่อพลอย

งานเทคโนโลยีสารสนเทศ โรงพยาบาลบ่อพลอย

ระดับความเสี่ยงที่จัดทำแผนการบริหารความเสี่ยง : ปานกลาง - สูง

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ่อพลอย บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ผู้รับผิดชอบ : งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
1. Data Loss Error ประเมินระบบงานที่ทำให้ข้อมูลผู้ใช้ไม่เกิดความผิดพลาด	- พัฒนาศักยภาพเจ้าหน้าที่ ให้มีความรู้ความเข้าใจในการบันทึกข้อมูลให้ถูกต้องครบถ้วน สมบูรณ์ และประเมินความรู้ความเข้าใจ			↔				↔				↔				ระดับความเสี่ยง 25 (สูงมาก)
	- พัฒนาระบบ IPD paperless ให้สะดวกต่อการใช้งาน		←	—	—	→	←	—	—	→	←	—	—	→		
	- พัฒนาระบบ HIS ให้เป็นปัจจุบัน และสามารถนำข้อมูลไปใช้งานได้อย่างถูกต้อง		↔		↔		↔		↔		↔		↔			
	- ติดตั้งอุปกรณ์กระจายสัญญาณ Wifi ทุกจุดบริการ		↔		←	→					↔				ปี 69 = 50000 บ.	
	- ปรับปรุงคู่มือการใช้งานระบบ IPD paperless				↔		↔		↔		↔		↔			

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
	- ควบคุม กำกับ ติดตาม Audit โดยหัวหน้างานทุกวัน		↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔		
2. Criminal – Break-ins ทรัพย์สิน IT อาจเสียหายจากการงัดเงะหรือย่องเบา	- ติดตั้งกล้องวงจรปิดเพิ่ม ครอบคลุมพื้นที่/จุดเสี่ยง ใน รพ.				↔			↔				↔				ระดับความเสี่ยง 12 (สูง)
	- จัดทำทะเบียนทรัพย์สิน IT ของหน่วยงานและโรงพยาบาล										↔					
	- ตรวจสอบความพร้อมใช้ของกล้องวงจรปิด โดย จนท.IT ทุกวัน		↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔	↔		
	- สำรองข้อมูลกล้องวงจรปิด 30 วัน				↔		↔		↔		↔		↔			
3. Fire – Internal เกิดเหตุอัคคีภัยในห้อง Data center	- มีแผนเผชิญเหตุอัคคีภัยในห้อง Data center กำหนดหน้าที่ความรับผิดชอบชัดเจน ทั้งใน – นอกเวลาราชการ		↔				↔				↔					ระดับความเสี่ยง 5 (ปานกลาง)
	- ซักซ้อมการเผชิญเหตุอัคคีภัยในห้อง Data center ปีละ 1 ครั้ง			↔				↔				↔				
	- จัดทำแผน BCP : รองรับสถานการณ์อัคคีภัยในห้อง Data center เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง		↔				↔				↔					

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
	- เจ้าหน้าที่ IT ตรวจสอบด้านความปลอดภัย พร้อมใช้ทุกวัน (Checklist)		←	—	—	→	←	—	—	→	←	—	—	→		
	- มีระบบแจ้งเตือน อุณหภูมิ, ความชื้น , ไฟไหม้ ผ่าน App.ทางมือถือ		←	—	—	→	←	—	—	→	←	—	—	→		
	- ติดตั้งอุปกรณ์ป้องกันอัคคีภัย ตรวจสอบความพร้อมใช้ ทุกเดือน		←	—	—	→	←	—	—	→	←	—	—	→		
	- สำรองข้อมูลแบบ Real time ณ อาคารอำนวยการ		←	—	—	→	←	—	—	→	←	—	—	→		
	- ซักซ้อมการกู้คืนข้อมูล ทุก 3 เดือน			↔		↔		↔		↔		↔		↔		
4. Criminal – Theft ทรัพย์สิน IT อาจเสียหายจากโจรกรรม	- จัดทำนโยบาย ระเบียบปฏิบัติเพื่อรักษาความมั่นคงปลอดภัย ความเสียหายอันเกิดจากการโจรกรรม พร้อมประเมินความพร้อมของบุคลากรโรงพยาบาลบ่อพลอย		↔				↔				↔					ระดับความเสี่ยงลดลง จาก 25 (สูงมาก) เหลือ 8 (ปานกลาง)
	- จัดทำแผนรองรับสถานการณ์ เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)		↔				↔				↔					

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
	- ร่วมกับทีม ENV ประเมินจุดเสี่ยงในโรงพยาบาล เพื่อติดตั้งกล้องวงจรปิดเพิ่มเติม		↔				↔				↔					
	- ตรวจสอบความพร้อมใช้ของกล้องวงจรปิดทุกวัน โดย จนท.IT		→	→	→	→	→	→	→	→	→	→	→	→		
5. Internet ระบบเครือข่ายเชื่อมต่ออินเทอร์เน็ตของโรงพยาบาลล่ม, ไม่สามารถใช้งานได้	- กำหนดการเข้าถึงการใช้งาน Internet ด้วย Username และ Password ส่วนบุคคล		→	→	→	→	→	→	→	→	→	→	→	→	122,000 บาท/ปี	ระดับความเสี่ยง 9 (ปานกลาง)
	- ตรวจสอบการใช้ Traffic < 50%		→	→	→	→	→	→	→	→	→	→	→	→		
	- มีเครือข่าย Internet สำรอง เมื่อผู้ให้บริการหลักขัดข้อง ให้สามารถใช้งานได้อย่างต่อเนื่อง		→	→	→	→	→	→	→	→	→	→	→	→		
	- ประกาศใช้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ พร้อมทั้งประเมินการรับรู้ใน จนท. 100%		↔				↔				↔					
	- ตรวจสอบสัญญาณ Internet ทุกวัน		→	→	→	→	→	→	→	→	→	→	→	→		

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	ปีงบ 2567				ปีงบ 2568				ปีงบ 2569				งบประมาณ	ผลลัพธ์ความก้าวหน้า
			ไตรมาส				ไตรมาส				ไตรมาส					
			1	2	3	4	1	2	3	4	1	2	3	4		
6. Data Protection Policy and Regulations (การป้องกันความลับและความเป็นส่วนตัวของข้อมูล) ข้อมูลผู้ป่วยถูกเปิดเผย	- กำหนดการเข้าถึงข้อมูลด้วย Username และ Password ของตนเอง		←	—	—	→	←	—	—	→	←	—	—	→		ระดับความเสี่ยง 8 (ปานกลาง) เท่าเดิม
	- กำหนดสิทธิ์การเข้าถึงข้อมูลของแต่ละบุคคล : แพทย์, พยาบาล, ฯลฯ		←	—	—	→	←	—	—	→	←	—	—	→		
	- จัดทำประเภทข้อมูลสำคัญที่ต้องปกปิด		↔				↔				↔					
	- กำกับ ดูแลระบบข้อมูล โดยผู้อำนวยการและเจ้าหน้าที่ IT ที่ได้รับมอบหมาย		←	—	—	→	←	—	—	→	←	—	—	→		
	- ประกาศใช้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ พร้อมทั้งประเมินการรับรู้ใน จนท. 100%		←	—	—	→	←	—	—	→	←	—	—	→		