รายงานผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านสารสนเทศโรงพยาบาลบ้านด่าน

ตารางที่ ๑ การติดตามกิจกรรมการจัดการความเสี่ยง

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงดานการใชเทคโนโลยี

ประเภทความเสี่ยง/ กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีงบประมาณ ๒๕๖๙												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑. ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ															
๑.๑ ระบบฐานข้อมูล/ โปรแกรมที่ให้บริการเกิดความเสียหาย	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ	- ทุกวัน/ทุกสัปดาห์													
	- จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	- ทุก สัปดาห์เดือนละ ๔ ครั้ง	←											→	
	- ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุก สัปดาห์ เดือนละ ๔ ครั้ง													
๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ	- ทุกวัน/ทุกสัปดาห์													
	- จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	- ทุก สัปดาห์เดือนละ ๔ ครั้ง	←											→	
	- ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุก สัปดาห์ เดือนละ ๔ ครั้ง													

ตารางที่ ๑ การติดตามกิจกรรมการจัดการความเสี่ยง(ต่อ)

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงดานการใชเทคโนโลยี

ประเภทความเสี่ยง/ กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีงบประมาณ ๒๕๖๙												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๒. ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ															
๒.๑ ไฟไหม้ห้อง Server	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- ทุกวันที่ ๓๐ ก.ย.ของทุกปี												√	
๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก	- ทุก ๓ เดือน			√			√			√			√	
๒.๓ ฝนฟ้าคะนอง อุปกรณ์ต่อพ่วงเสียหาย	- ตรวจสอบความพร้อมของระบบป้องกันไฟกรรโชก กราวป้องกันฟ้าผ่า ทำแผนซื้ออุปกรณ์ป้องกันเพิ่ม	- ช่วงฤดูฝน								←	—	—	—	→	
๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล															
๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	- ทุกวันที่ ๓๐ ก.ย.ของทุกปี												√	
๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←	—	—	—	—	—	—	—	—	—	—	→	
๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←	—	—	—	—	—	—	—	—	—	—	→	

ตารางที่ ๑ การติดตามกิจกรรมการจัดการความเสี่ยง(ต่อ)

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงดานการใชเทคโนโลยี

ประเภทความเสี่ยง/ กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/ สิ้นสุด	ปีงบประมาณ ๒๕๖๙												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๓.๔ ขาดเครื่องมือป้องกันหรือตรวจจับไวรัส	- มีโปรแกรมป้องกันไวรัสและ Update ฐานข้อมูลไวรัส	- สัปดาห์ละ ๑ ครั้ง	←											→	
๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ															
๔.๑ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์การโดยไม่ได้รับอนุญาต	- กำหนดสิทธิในการเข้าถึงข้อมูล	- เมื่อแต่งตั้ง/โยกย้าย /ลาออก / เกษียณอายุราชการ	←											→	
๕. อุปกรณ์คอมพิวเตอร์เสียหาย	- บำรุงรักษาคอมพิวเตอร์ เช่น เป่าฝุ่น สแกนฮาร์ดดิสค์ disk cleanup และ disk defragmenter	- สัปดาห์ละ ๑ ครั้ง													
๕.๑ คอมพิวเตอร์ไม่สามารถใช้งานได้			←											→	

ผู้รับผิดชอบ.....

(นางสาวดวงจันทร์ ชะงักรัมย์)

นักวิชาการคอมพิวเตอร์ปฏิบัติการ

วันที่...30 เมษายน 2569...