การประเมินผลการจัดการความเสี่ยงด้านสารสนเทศโรงพยาบาลบ้านด่าน

การประเมินความเสี่ยง

ตารางที่ ๑ การประเมินผลการจัดการความเสี่ยง แยกตามประเภทความเสี่ยง ๕ ด้าน

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ	รายละเอียดการจัดการ	โอกาสที่จะ เกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยง คงเหลือ (๑) X (๒)
๑.	**ความเสี่ยงด้าน Hardware**						
	๑.๑ อุปกรณ์คอมพิวเตอร์เสียหาย	- หมดอายุการใช้งาน - มีการใช้งานหนัก - สภาวะแวดล้อม (ไฟฟ้า ,อากาศ)	ไม่สามารถทำงานต่อไปได้	- มีแผนจัดซื้อทดแทนทุกปี - จุดไหนไม่ใช้งานปิดการใช้งาน - มีเครื่องสำรองไฟ	๑	๑	๑
	๑.๒ ระบบเครือข่ายมีปัญหา	- อุปกรณ์เครือข่ายเสียหาย - ผู้ให้บริการเครือข่ายขัดข้อง	ไม่สามารถใช้บริการผ่านเครือข่ายได้	- มีระบบสำรองเครือข่าย ๓ เครือข่าย CAT(๒)/๓BB(๑)	๑	๑	๑
๒.	**ความเสี่ยงด้าน Software**						
	๒.๑ Software ไม่สามารถทำงานได้	- ระบบปฏิบัติการเสียหาย - Software มีการทำงานผิดพลาด	ไม่สามารถให้บริการได้	- มีระบบปฏิบัติ/ Software ถูกลิขสิทธิ์	๑	๑	๑
		- Virus /Hacker /Spyware		- มี antivirus ถูกลิขสิทธิ์ Update ได้	๑	๑	๑
๓.	**ความเสี่ยงด้านบุคลากร**						
	๓.๑ ขาดทักษะในการทำงาน	- ไม่เข้าใจระบบงานนั้นๆ อย่างถี่ถ้วน - ปรับเปลี่ยนตำแหน่ง	งานที่ได้ไม่มี ประสิทธิภาพเท่าที่ควร	- จัดอบรมเจ้าหน้าที่ที่เกี่ยวข้องเฉพาะงาน	๑	๒	๒
	๓.๒ ไม่ใช่หน้าที่หลักที่รับผิดชอบ	- ทำงานที่ไม่ใช่หน้าที่ของตน	งานอาจผิดพลาด	- แบ่งภาระงานให้รับผิดชอบตามตำแหน่งหน้าที่	๑	๑	๑

การประเมินความเสี่ยง(ต่อ)

ตารางที่ ๑ การประเมินผลการจัดการความเสี่ยง แยกตามประเภทความเสี่ยง ๕ ด้าน

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ	รายละเอียดการจัดการ	โอกาสที่จะ เกิดหลังจัดการความเสี่ยง (๑)	ผลกระทบเสียหายหลังจัดการความเสี่ยง (๒)	ระดับความเสี่ยง คงเหลือ (๑) X (๒)
๔.	**ความเสี่ยงด้านข้อมูล**						
	๔.๑ ข้อมูลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี	ไม่มีข้อมูลเพื่อนำไปใช้งาน	- ตรวจสอบดูแลอุปกรณ์ Hardware ให้พร้อมใช้ - มีระบบการสำรองข้อมูลแบบ real time	๑	๒	๒
	๔.๒ ข้อมูลผิดพลาด	- เนื่องจากการปฏิบัติงานผิดพลาด - โปรแกรมทำงานผิดพลาด	ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้	-	๑	๑	๑
	๔.๓ ความปลอดภัยของข้อมูล	- ขาดอุปกรณ์ป้องกันข้อมูลที่ดี - ขาดการตรวจสอบ - ขาดบุคลากรที่มีความรู้อย่างแท้จริง	อาจทำให้ข้อมูลเสียหาย ข้อมูลรั่วไหล	- มีอุปกรณ์ป้องกันข้อมูลที่ดี (Firewall - Fortinet FortiGate ๑๐๐E) - ต่ออายุอุปกรณ์ป้องกันข้อมูลทุกๆ ๓ปี - เข้าประชุม/อบรมด้านความปลอดภัยของข้อมูล	๑	๓	๓
๕.	**ความเสี่ยงด้านหน้าที่การปฏิบัติ**						
	๕.๑ ปฏิบัติหน้าที่ไม่ถูกต้อง	- ไม่เข้าใจในขั้นตอนปฏิบัติ	ไม่สามารถทำงานได้หรืองานมีความผิดพลาด	- จัดอบรมเจ้าหน้าที่ที่เกี่ยวข้องเฉพาะงาน	๑	๑	๑
	๕.๒ ละเลยการปฏิบัติ	- ไม่เอาใจใส่ในงาน	งานไม่มีประสิทธิภาพ	- ตระหนักในหน้าที่ที่ได้รับมอบหมาย	๑	๑	๑

(นางสาวดวงจันทร์ ชะงักรัมย์)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ผู้จัดทำรายงาน

(นายศาสตรา เข็มบุบผา)
ผู้อำนวยการโรงพยาบาลบ้านด่าน