ประเมินแนวทางการพัฒนาระบบเทคโนโลยีสารสนเทศโรงพยาบาล (HAIT)

บทที่ 3 การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล

แนวคิดสำคัญระบบเทคโนโลยีสารสนเทศโรงพยาบาล

1.เข้าใจความเสี่ยง (Risk) and อุบัติการณ์ (Incident)

2.การจัดการความเสี่ยง (Risk Management) และการจัดการอุบัติการณ์

3.ค้นหาความเสี่ยง ประเมินความเสี่ยง วางกลยุทธ์จัดการความเสี่ยง ปฏิบัติการจัดการความเสี่ยง

4.ประเมินผลการจัดการความเสี่ยงที่ผ่านมา วิเคราะห์ผลการประเมิน และนำผลการวิเคราะห์มาปรับปรุงแผนการจัดการความเสี่ยงในปีถัดไป (PDCA)

5.ให้ค้นหาความเสี่ยงใหม่ๆ นำมาประเมิน วางกลยุทธ์และจัดการความเสี่ยงทุกปี

สิ่งที่หน่วยงานต้องทราบ

1.ความเข้าใจ คำว่า “ความเสี่ยง” และ “อุบัติการณ์”

2.ทราบความเสี่ยง 3 ลำดับแรกของโรงพยาบาลและมาตรการควบคุม ระบบเทคโนโลยีสารสนเทศโรงพยาบาล

3.ทราบอุบัติการณ์ 3 ลำดับแรกที่เกิดของโรงพยาบาล และมาตรการควบคุมอุบัติการณ์ ปี2567 ระบบเทคโนโลยีสารสนเทศโรงพยาบาล

4.ทราบอุบัติการณ์หน่วยงานตนเองที่เกิดบ่อย และแนวทางป้องกันแก้ไข ระบบเทคโนโลยีสารสนเทศโรงพยาบาล

ความเสี่ยง (Risk)

จุดอ่อน(ยังไม่เกิด)ที่มีอยู่ในระบบทั้งหมด จะเป็นช่องโหว่ที่จะกระทำความเสียหายให้เกิดขึ้นในระบบได้

อุบัติการณ์ (Incident)

เหตุการณ์ที่เกิดขึ้นแล้ว ทำให้เกิดความเสียหายแก่ระบบ โดยสาเหตุส่วนใหญ่สามารถป้องกันได้ ถ้ามีการปิดจุดอ่อน(ปิดความเสี่ยง)

การจัดการความเสี่ยง(Risk Management)ระบบสารสนเทศเวชระเบียน

Risk Profile ปี 2566

จำ! สไลด์นี้

หัวข้อความเสี่ยง	โอกาสเกิด	ผลกระทบ	คะแนนความเสี่ยง	ลำดับการแก้ไข	มาตรการควบคุม (ปีงบประมาณ 2566)
ไฟตก	5	4	20	1	1.ตรวจสอบและดูแลรักษาอุปกรณ์ไฟฟ้าอย่างสม่ำเสมอ 2.จัดทำแผนตรวจสอบเครื่องสำรองไฟระดับหน่วยงานตามแผนซ่อมบำรุงประจำปี 3. ตรวจสอบระบบไฟฟ้าเพื่อตระหนักถึงความสมบูรณ์และความปลอดภัยของสายไฟ ตรวจสอบการติดตั้งและการใช้งานของสายไฟเพื่อให้มั่นใจว่ามันอยู่ในสภาพที่ดีและไม่มีการชำรุดหรือสายไฟที่ลากอยู่ซ้อนกัน 4.มีระบบสำรองไฟฟ้า
ไวรัสโจมตีเครื่องคอมพิวเตอร์	3	4	12	2	1.ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่น่าเชื่อถือ 2.อัปเดตระบบปฏิบัติการ Windows และซอฟต์แวร์ที่ใช้งานบนเครื่องคอมพิวเตอร์ของ 3.ติดตั้ง firewall 4.ระมัดระวังไม่คลิกลิงก์หรือเปิดไฟล์แนบในอีเมลที่ไม่น่าเชื่อถือ และหลีกเลี่ยงเข้าชมเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มีระบบความปลอดภัย
โปรแกรม hos-xp ขัดข้อง	3	4	12	3	1.อัพเดท hos xp ให้เป็นเวอร์ชันปัจจุบัน 2.แนะนำการใช้งานโปรแกรมที่หน้างาน 3.เปลี่ยนสายสัญญาณ LAN ใหม่/เปลี่ยนหัว RJ45 ใหม่ 4.เมื่อมีการติดตั้งอุปกรณเกี่ยวกับคอมพิวเตอร์ใหม่ต้องมีเจ้าหน้าที่ไอทีทุกครั้ง

Risk Profile ปี 2566

หัวข้อความเสี่ยง	โอกาสเกิด	ผลกระทบ	คะแนนความเสี่ยง	ลำดับการแก้ไข	มาตรการควบคุม (ปีงบประมาณ 2566)
เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงขัดข้อง/ชำรุดใช้การไม่ได้	2	4	6	4	1.จัดทำแผนจัดซื้อเครื่องคอมพิวเตอร์ทดแทนมีมีอายุเกิน 5 ปี 2. อัพเกรดอุปกรณ์ให้มีประสิทธิภาพยิ่งขึ้น 3.ปฏิบัติตามแผนการตรวจสอบเครื่องอุปกรณ์คอมพิวเตอร์
swith เสีย	3	2	6	4	1.ให้กำหนดสิทธิ์การเข้าถึงในระดับผู้ใช้หรือกลุ่มผู้ใช้เพื่อควบคุมการเข้าถึงและการใช้งานสวิตช์ โดยใช้ระบบรหัสผ่านหรือระบบตรวจสอบตัวตนอื่นๆ 2.ใช้การกำหนดค่าความปลอดภัยบนสวิตช์เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการโจมตีจากภายนอก เช่นการเปิดใช้งานความปลอดภัยแบบ 8-2.1X หรือการกำหนดค่า ACL (Access Control List) เพื่อจำกัดการเข้าถึงแบบละเอียด 3.ปรับแต่งการทำงานของสวิตช์เพื่อให้เหมาะสมกับความต้องการของเครือข่าย เช่น การกำหนดค่า VLAN (Virtual Local Area Network) เพื่อแยกแยะและควบคุมการสื่อสารระหว่างอุปกรณ์ในเครือข่าย
บริษัทไม่รับประกันการแก้ไขตามสัญญา	2	4	6	4	1.อ่านสัญญาที่ได้ทำกับบริษัทเพื่อตรวจสอบข้อกำหนดและเงื่อนไขที่เกี่ยวข้องกับการแก้ไขปัญหา ตรวจสอบว่ามีข้อกำหนดหรือข้อความที่อ้างถึงการรับประกันหรือไม่ 2.ติดต่อบริษัทเพื่อแสดงความเห็นเกี่ยวกับปัญหาที่เกิดขึ้นและขอให้แก้ไขตามสัญญา อธิบายว่าคุณคาดหวังจากการแก้ไขอย่างไร และระบุข้อเท็จจริงที่เกี่ยวข้องกับสัญญา 3.หากมีคำสั่งซ่อมแซมที่ระบุในสัญญา ตรวจสอบว่าคุณได้ปฏิบัติตามขั้นตอนที่

Risk Profile ปี 2566

หัวข้อความเสี่ยง	โอกาสเกิด	ผลกระทบ	คะแนนความเสี่ยง	ลำดับการแก้ไข	มาตรการควบคุม (ปีงบประมาณ 2566)
ฟ้าผ่า	2	4	6	5	1.การติดตั้งระบบป้องกันฟ้าผา เช่นกำแพงคั้นหรือแผ่นคั้นดินเชื่อมต่อ เป็นต้นสามารถช่วยในการยับยั้งการเคลื่อนไหวของดินและลดความเสี่ยงจากฟ้าผา 2.การเตรียมความพร้อมและการตรวจสอบเป็นสิ่งสำคัญเพื่อรักษาสภาพอยู่ในสภาวะที่ดี ควรมีการตรวจสอบและบำรุงรักษาระบบป้องกันฟ้าผาอย่างสม่ำเสมอ รวมถึงการตรวจสอบสภาพ สายล่อฟ้าผ่าในพื้นที่
server ขัดข้อง	1	5	5	5	1.ทำการตรวจสอบและวางแผนความต้องการของเซิร์ฟเวอร์ให้เหมาะสมกับการใช้งาน 2.เลือกฮาร์ดแวร์ที่มีความเหมาะสมกับความต้องการมีความเสถียร 3.ติดตั้งระบบปฏิบัติการที่เหมาะสม เช่น Windows Server, Linux, หรือ Unix 4.การตั้งค่าระบบไฟร์วอลล์ และการกำหนดสิทธิ์การเข้าถึงข้อมูล 5.ติดตั้งโปรแกรมป้องกันไวรัส 6.สำรองข้อมูลเป็นระยะเพื่อป้องกันการสูญหายของข้อมูล
เครื่องแม่ข่าย router เสีย	1	5	5	5	1.ปรับแต่งการตั้งค่าเครื่องแม่ข่ายเพื่อป้องกันการโจมตี เช่นการปิดการใช้งานเซอร์วิสที่ไม่จำเป็น การกำหนดค่าเราท์เตอร์เฟิร์มแวร์เพื่อป้องกันช่องโหว่ที่รู้จัก 2.ตรวจสอบและกำหนดเส้นทางการส่งข้อมูลที่เหมาะสมเพื่อให้เครือข่ายทำงานได้อย่างมีประสิทธิภาพ รวมถึงการกำหนดเส้นทางที่ปลอดภัยและที่มีการสำรอง 3.ตรวจสอบและอัปเกรดซอฟต์แวร์ของเครื่องแม่ข่ายเพื่อให้ได้รับความเสถียรและประสิทธิภาพที่ดีที่สุด รวมถึงการดำเนินการแก้ไขช่องโหว่ที่รู้จัก 4.ใช้การเข้ารหัสข้อมูลที่ส่งผ่านเครือข่ายเพื่อปกป้องความลับและความปลอดภัยของข้อมูล

Risk Profile ปี 2566

หัวข้อความเสี่ยง	โอกาสเกิด	ผลกระทบ	คะแนนความเสี่ยง	ลำดับการแก้ไข	มาตรการควบคุม (ปีงบประมาณ 2566)
windows 10 ขัดข้อง	1	5	5	5	1.การอัปเดตระบบปฏิบัติการ และใช้ licent ที่ถูกลิขสิทที่ถูกลิขสิทธิ์ 2.กำหนดค่ากฎระเบียบการใช้งานเพื่อควบคุมการใช้งานของผู้ใช้ และสร้างนโยบายที่เข้มงวดเกี่ยวกับความปลอดภัย
ไฟไหม้	1	5	5	5	1.ติดตั้งระบบดับเพลิงที่เหมาะสมในห้องเซิร์ฟเวอร์ เช่น ระบบสเปรย์น้ำดับเพลิง หรือระบบดับเพลิงแบบสารเคมี 2. ตรวจสอบและบำรุงรักษาระบบระบายความร้อนให้มีประสิทธิภาพ 3.ติดตั้งระบบตรวจจับควันในห้องเซิร์ฟเวอร์ 4.รักษาความสะอาดทั้งภายในและภายนอกห้องเซิร์ฟเวอร์ ล้างอุปกรณ์และระบบเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ 5.จำกัดการเข้าถึงห้องเซิร์ฟเวอร์เฉพาะบุคคลที่มีสิทธิ์ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ใช้ระบบการระบุตัวตนและการควบคุมการเข้าถึงเช่น รหัสผ่าน การสแกนลายนิ้วมือ หรือการใช้บัตรพนักงาน 6.สำรองข้อมูลในห้องเซิร์ฟเวอร์อย่างสม่ำเสมอ เก็บข้อมูลในตำแหน่งที่ปลอดภัยและทำการทดสอบสำรองข้อมูลเป็นประจำ

ผังการกำกับการดำเนินงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ปีงบประมาณ 2566

ประเด็นความเสี่ยง	แผนปฏิบัติงาน	ระยะเวลา	ต.ค	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ผู้รับผิดชอบ
เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงขัดข้อง/ชำรุด ใช้การไม่ได้	1.จัดทำแผนจัดซื่อเครื่องคอมพิวเตอร์ ทดแทนมีมีอายุเกิน 5 ปี	ปีละ 1 ครั้ง													ทีม IT
	2.อัพเกรดอุปกรณ์ให้มีประสิทธิภาพยิ่งขึ้น	ปีละ 1 ครั้ง													ทีม IT
โปรแกรม hos xp ใช้งานไม่ได้	1.อัพเดท hos xp ให้เป็นเวอร์ชันล่าสุด 2.อบรมเจ้าหน้าที่ใช้งานโปรแกรมเบื้องต้น														ทีม IT
ไวรัสโจมตีเครื่องคอมพิวเตอร์	1.ติดตั้ง firewall 100 F														ทีม IT
	2.อัพเดทระบบปฏิบัติการอย่างสม่ำเสมอ														ทีม IT
ไฟตก ทำให้ระบบ IT ใช้งานไม่ได้	1.จัดทำแผนเครื่อง สำรองไฟระดับหน่วยงานตามแผนซ่อมบำรุงประจำปี	ปีละ 1 ครั้ง													ทีม IT
	2.ตรวจสอบและดูแลรักษาอุปกรณ์ไฟฟ้าอย่างสม่ำเสมอ	ปีละ 1 ครั้ง													ทีมซ่อมบำรุง
	3.ตรวจสอบเครื่องปันไฟ	ทุกวัน													ทีมซ่อมบำรุง

อุบัติการณ์ (Incident) ปี 2566

จำ! สไลด์นี้

ความเสี่ยง	ระดับความเสี่ยง	สาเหตุ	จำนวนอุบัติการณ์ (ต.ค.65-มี.ค.66)	จำนวนอุบัติการณ์ (เม.ย-ก.ย.66)
โปรแกรม hos xp ขัดข้อง	12	-มีปัญหาเกี่ยวกับเครื่องแม่ข่าย -สายสัญญาณ Lan มีปัญหา -เข้าสู่ hos xp ไม่ได้ลืมรหัสพาสเวิร์ด	56	54
ไฟตก	20	-เกิดจากทำงานผิดพลาดของกระแสไฟฟ้าจากข้างนอก -การโหลดเกินกำลัง: การใช้งานอุปกรณ์ไฟฟ้ามากเกินไปโดยที่ระบบไฟฟ้าไม่สามารถรองรับได้ อาจทำให้เกิดการตกไฟฟ้า ตัวอย่างเช่น การเชื่อมต่อเครื่องใช้ไฟฟ้าที่มีกำลังการใช้งานสูงเกินกว่าความจุของวงจรไฟฟ้า	25	10
เครื่องคอมพิวเตอร์และ อุปกรณ์ต่อพ่วง ขัดข้อง/ชำรุด ใช้การไม่ได้	6	-ฮาร์ดดิสก์มีปัญหา -เมนบอร์ดเสีย -เครื่องคอมพิวเตอร์เกินอายุการใช้งาน -Ram เสีย -ไฟพาเวอร์ซัพพลายของเครื่องคอมพิวเตอร์ไม่ทำงาน	17	14

อุบัติการณ์ (Incident) ปี 2566

ความเสี่ยง	ระดับความเสี่ยง	สาเหตุ	จำนวนอุบัติการณ์ (ต.ค.65-มี.ค.66)	จำนวนอุบัติการณ์ (เม.ย-ก.ย.66)
ไวรัสโจมตีเครื่องคอมพิวเตอร์	12	-USB ติดไวรัส -การเปิดเว็บไซต์หรือ URL ที่ไม่ปลอดภัย	5	1
โปรแกรม hos office ใช้งานไม่ได้	4		11	4
ปริ้นเตอร์ใช้งานไม่ได้	4	ฮาร์ดแวร์: เครื่องปริ้นเตอร์อาจมีปัญหาฮาร์ดแวร์ เช่น หัวพิมพ์เสีย ลูกกลิ้งดูดกระดาษเสีย ตัวปริ้นเตอร์ชำรุด หรืออุปกรณ์ภายในที่มีปัญหา เพื่อแก้ไขปัญหานี้ อาจต้องติดต่อศูนย์บริการหรือช่างซ่อมเพื่อเปลี่ยนหรือซ่อมแซมอะไหล่	5	1
windows 10 ขัดข้อง	5	การอัปเดตไม่สมบูรณ์: การอัปเดตระบบปฏิบัติการ Windows 10 อาจไม่สมบูรณ์หรือไม่เสร็จสิ้น อาจเกิดข้อผิดพลาดในระหว่างการดาวน์โหลดและติดตั้งอัปเดต นอกจากนี้ การติดตั้งแพตช์หรืออัปเดตที่ไม่เข้ากันกับระบบอาจเป็นสาเหตุของปัญหา	3	3

มาตรการควบคุมอุบัติการณ์ที่เกิดขึ้น (ปีงบประมาณ 2567)

จำ! สไลด์นี้

หัวข้อความเสี่ยง	มาตรการควบคุม (ปีงบประมาณ 2567)
โปรแกรม hos-xp ขัดข้อง	1.ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัย 5do 7 Don't 2.อัพเดท HOSXP ให้เป็นปัจจุบัน 3.1.ปฏิบัติตามมาตรการ SLA
เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงขัดข้อง/ชำรุด ใช้การไม่ได้	1.ตรวจสอบอุปกรณ์เครือข่ายระดับหน่วยงานตามแผนซ่อมบำรุงประจำปี 2.แผนจัดซื้ออุปกรณ์เครือข่ายทดแทน 3.มีอุปกรณ์ทดแทนกรณีซ่อมไม่ได้
ไฟตก	1.ตรวจสอบการทำงานของเครื่องปั่นไฟของโรงพยาบาล 2.จัดทำแผนตรวจสอบเครื่องสำรองไฟระดับหน่วยงานตามแผนซ่อมบำรุงประจำปี 3.ติดตั้งเครื่องสำรองไฟ (UPS) เครื่องคอมพิวเตอร์และเครื่อง Server