การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศโรงพยาบาล Hospital IT Risk Management(ฉบับเผยแพร่)
หน่วยคอมพิวเตอร์และเทคโนโลยีสารสนเทศ โรงพยาบาลหนองบัวลำภู
ปีงบประมาณ 2560

การจัดการความเสี่ยง (Risk Management) เป็นกลไกสำคัญ สำหรับการควบคุมคุณภาพระบบงานทุกระบบ เพราะหากเราต้องการให้ระบบงานมีคุณภาพ เราต้องประเมินและตรวจสอบความเสี่ยงที่จะให้ระบบงานของเราด้อยคุณภาพให้ครอบคลุมความเสี่ยงทุกด้าน แล้วจัดการป้องกันไม่ให้ความเสี่ยงเหล่านั้นมีโอกาสมารบกวน และทำให้ระบบงานของเราด้อยคุณภาพลงไปได้

ระบบเทคโนโลยีสารสนเทศโรงพยาบาลก็เป็นระบบหนึ่งที่ต้องใช้การจัดการความเสี่ยงเป็นกลไกสำคัญในการควบคุมเพื่อให้มั่นใจว่าระบบดำเนินไปได้อย่างมีคุณภาพ ดังนั้น ผู้บริหาร และผู้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศโรงพยาบาลจึงต้องมีความเข้าใจวิธีการจัดการความเสี่ยงเป็นอย่างดี เพื่อให้สามารถดำเนินการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วยปัจจัยดังนี้

1. จุดอ่อน หรือ ช่องโหว่
2. ภัยคุกคาม

จุดอ่อน หมายถึง ข้อบกพร่องทางด้าน กายภาพ การจัดระบบ ขั้นตอนการทำงาน บุคคลากรการบริหารจัดการ ครุภัณฑ์ โปรแกรม หรือข้อมูลสารสนเทศสำคัญ ดังตัวอย่างต่อไปนี้

- ไม่มีการติดตั้งกุญแจประตูห้องเครื่องแม่ข่าย
- ไม่มีระบบดักจับควัน และระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบเครื่องแม่ข่าย
- ไม่กำหนดขั้นตอนมาตรฐานในการสำรองข้อมูล
- บุคคลากรไม่ทำตามระเบียบปฏิบัติด้านการตั้งรหัสผ่าน
- ไม่มีการดำเนินการควบคุมความมั่นคงปลอดภัย
- ไม่มีเครื่องแม่ข่ายสำรอง
- ใช้โปรแกรมระบบงานสำคัญร่วมกับโปรแกรมส่วนตัว
- ติดตั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตได้โดยอิสระ
- ไม่มีการควบคุมการเข้าถึงข้อมูล สารสนเทศที่สำคัญ

ภัยคุกคาม หมายถึง ภัยอันตรายต่างๆ ทั้งที่มีสาเหตุมาจากมนุษย์และสาเหตุอื่นๆ อันมีโอกาสจะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ดังอย่างต่อไปนี้

- ไฟไหม้
- น้ำท่วม
- ขโมย

- ไวรัสคอมพิวเตอร์
- กระแสไฟฟ้าขัดข้อง

ความเสี่ยง คือความเป็นไปได้หรือโอกาสที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบ โดยจุดอ่อนของระบบจะเพิ่มโอกาสให้ภัยคุกคามเข้ามาสร้างความเสียหายให้กับระบบเทคโนโลยีสารเทศได้ การจัดการความเสี่ยง จึงมีเป้าหมายสำคัญเพื่อ ลดโอกาส ที่ภัยคุกคามจะเข้ามาสร้างเสียหายให้กับระบบนั่นเอง

ขั้นตอนสำคัญในการจัดการความเสี่ยง

ขั้นตอนที่สำคัญในการจัดการความเสี่ยง ประกอบไปด้วย ขั้นตอนดังต่อไปนี้

1. การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)
2. การวางแผนกลยุทธ์จัดการความเสี่ยง (Risk Management Strategic Planning)
3. การดำเนินการจัดการความเสี่ยง (Risk Treatment)

1.การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทำโดยการสำรวจระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อค้นหาจุดอ่อนและภัยคุกคามที่มีโอกาสจะเข้ามาทำความเสียหายให้กับระบบ แล้วประเมินระดับคะแนนความเสี่ยง เพื่อนำมาพิจารณาวางแผนจัดการความเสี่ยงต่อไป

มาตรฐาน ISO/IEC 27001 : 2013 ซึ่งเป็นมาตรฐานนานาชาติสำหรับระบบบริหารความปลอดภัยของข้อมูล (Security Management Systems, ISMS) ได้กล่าวถึงความเสี่ยงในระบบเทคโนโลยีสารสนเทศไว้มากมาย ดังอย่างเช่น

- acts of terrorism การก่อการร้าน
- air conditioning failure ระบบปรับอากาศหยุดทำงาน
- airborne particles/dust ฝุ่นละออง
- bomb attack การวางระเบิด
- breach of legislation or regulations การละเมิดนโยบายและระเบียบปฏิบัติด้านความปลอดภัย
- breaches of contractual obligations การละเมิดข้อตกลงหรือสัญญาที่ผูกพัน
- compromise of security ความย่อหย่อนในระบบรักษาความปลอดภัย
- damage caused by penetration tests ความเสียหายจากการทดลองเจาะเข้าระบบ
- damage caused by third parties ความเสียหายจากบุคคลที่สาม
- destruction of records ข้อมูลถูกทำลาย
- destruction of the business continuity plans แผนกู้คืนถูกทำร้าย
- deterioration of media สื่อที่เก็บข้อมูลเสื่อมสภาพ
- disasters (natural of man-made) ภัยพิบัติ (จากธรรมชาติ หรือ จากมนุษย์)

- ฯลฯ

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จึงควรเริ่มจาก การตรวจสอบรายการความเสี่ยงที่อาจเกิดขึ้นได้ทั้งหมด โดยอาจใช้แบบประเมินความเสี่ยง เช่น แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่พัฒนาโดย สมาคมเวชสารสนเทศไทย โดยเมื่อคาดว่าอาจเกิดความเสี่ยงเรื่องใดแล้ว คณะผู้ประเมินจะต้องประเมินรายละเอียดเพิ่มเติม ได้แก่

1. โอกาสที่จะเกิดความเสี่ยงนั้น Probability
2. ความเสียหายที่จะเกิดขึ้น Impact

แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล พัฒนาโดยสมาคมเวชสารสนเทศไทย ปีพ.ศ. 255

TMI Risk analysis worksheet (Range of 0.0 to 1.0 for P and I)

IT Components	Probability (P)	Impact (I)	Risk = P x I
1. IT – Hardware	1 2 3 4 5	1 2 3 4 5	
1.1 Servers Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.2 Network Switches Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.3 Workstations Failure	1 2 3 4 5	1 2 3 4 5	
1.4	1 2 3 4 5	1 2 3 4 5	
2. IT – System Software	1 2 3 4 5	1 2 3 4 5	
2.1 Operating System Failure	1 2 3 4 5	1 2 3 4 5	
2.2	1 2 3 4 5	1 2 3 4 5	
3. IT – Applications	1 2 3 4 5	1 2 3 4 5	
3.1 Front Offices	1 2 3 4 5	1 2 3 4 5	
3.2 Back Offices	1 2 3 4 5	1 2 3 4 5	
3.3	1 2 3 4 5	1 2 3 4 5	
4. IT – Communications, Connectivity	1 2 3 4 5	1 2 3 4 5	
4.1 Intranet	1 2 3 4 5	1 2 3 4 5	
4.2 Internet	1 2 3 4 5	1 2 3 4 5	
4.3	1 2 3 4 5	1 2 3 4 5	
5. IT – Operational (Human) Error	1 2 3 4 5	1 2 3 4 5	
5.1 Backup Error	1 2 3 4 5	1 2 3 4 5	
5.2 Data Loss Error	1 2 3 4 5	1 2 3 4 5	
5.3	1 2 3 4 5	1 2 3 4 5	
6. IT –Project Failure	1 2 3 4 5	1 2 3 4 5	
6.1 Inappropriate System Analysis	1 2 3 4 5	1 2 3 4 5	
6.2 Inappropriate System Design	1 2 3 4 5	1 2 3 4 5	
6.3 Inadequate Resources	1 2 3 4 5	1 2 3 4 5	
6.4 Poor Project Management	1 2 3 4 5	1 2 3 4 5	
6.5	1 2 3 4 5	1 2 3 4 5	
7. IT –Future Development	1 2 3 4 5	1 2 3 4 5	
7.1 No Data Dictionary	1 2 3 4 5	1 2 3 4 5	
7.2 No System Blueprint	1 2 3 4 5	1 2 3 4 5	
7.3 No Program Document or Comments	1 2 3 4 5	1 2 3 4 5	
7.4	1 2 3 4 5	1 2 3 4 5	
8. IT – Vendor and Outsource Failure	1 2 3 4 5	1 2 3 4 5	
8.1 Vendor Stop Support	1 2 3 4 5	1 2 3 4 5	
8.2	1 2 3 4 5	1 2 3 4 5	
9. IT – Hacking, Unauthorized Intrusions	1 2 3 4 5	1 2 3 4 5	
10. Environment Factors	1 2 3 4 5	1 2 3 4 5	
10.1 Flooding – Internal	1 2 3 4 5	1 2 3 4 5	
10.2 Flooding – External	1 2 3 4 5	1 2 3 4 5	
10.3 Fire – Internal	1 2 3 4 5	1 2 3 4 5	
10.4 Fire – External	1 2 3 4 5	1 2 3 4 5	
10.5 Utilities – Electricity	1 2 3 4 5	1 2 3 4 5	
10.6 Criminal – Theft	1 2 3 4 5	1 2 3 4 5	
10.7 Criminal – Break-ins	1 2 3 4 5	1 2 3 4 5	
10.8 Civil Unrest – Protest, Mob	1 2 3 4 5	1 2 3 4 5	
10.9	1 2 3 4 5	1 2 3 4 5	
11. Other	1 2 3 4 5	1 2 3 4 5	
	1 2 3 4 5	1 2 3 4 5	

การคำนวนคะแนนความเสี่ยง

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

ประเมินผลเสียหาย มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

คะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15

การประเมินความเสี่ยงโอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ 1-5 ดังนี้

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

1. ต่ำมาก ไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2. ต่ำ มีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี
3. ปานกลาง มีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง
4. สูง มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5. สูงมาก มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆ สัปดาห์

ประเมินผลเสียหาย มีค่าได้เป็น

1. ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2. ต่ำ มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3. ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1 - 2 แผนก
4. สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล 3 - 4 แผนก
5. สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

หลังจากนั้นให้ประเมินคะแนนความเสี่ยง คำนวณได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15
เมื่อคำนวณคะแนนความเสี่ยงแล้ว ให้นำคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยงดังนี้

ค่าความเสี่ยง (ระดับ)			โอกาสที่จะเกิดความเสียหาย (Likelihood : L				
			ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
			1	2	3	4	5
ความรุนแรงของผลกระทบ (Impact : I)	สูงมาก	5	5	10	15	20	25
	สูง	4	4	8	12	16	20
	ปานกลาง	3	3	6	9	12	15
	ต่ำ	2	2	4	6	8	10
	ต่ำมาก	1	1	2	3	4	5

ระดับการประเมินความเสี่ยง

ระดับการประเมินความเสี่ยง		
ระดับคะแนนความเสี่ยง	**ระดับความเสี่ยง**	**คำอธิบาย**
1 - 3	ต่ำ (Low)	เป็นระดับความเสี่ยงที่องค์กรสามารถยอมรับได้
4-9	ปานกลาง (Medium)	เป็นระดับความเสี่ยงที่องค์กรพอสามารถยอมรับ แต่ต้องมีมาตรการควบคุมความเสี่ยง/ปรับปรุงความเสี่ยงในระดับที่องค์กรยอมรับได้
10 – 16	สูง (High)	ระดับที่ไม่สมารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
17 - 25	สูงมาก(Very High)	เป็นระดับที่องค์กรไมสามารถยอมรับได้/มีการปรับปรุงอย่างเร่งด่วน

มีการจัดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยง โดยค่าที่มีความเสี่ยงสูงมาก (17-25) จะถือว่าเป็นความเสี่ยงที่ไม่สามารถยอมรับได้ ต้องเร่งจัดการให้ยอมรับได้โดยทันที

มีการกำหนดวิธีแก้ไขความเสี่ยง ให้กับเหตุการณ์ต่างๆ และมีแผนจัดการเหตุการณ์ไม่ปกติ ซึ่งกำหนดแนวทางการปฏิบัติอย่างชัดเจน ทำให้มั่นใจได้ว่าผลการประเมินถูกต้องและสามารถนำผลการประเมินมาใช้ได้

กลยุทธ์ในการแก้ไขความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง
กลยุทธ์ที่ 2 การย้ายความเสี่ยง
กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง
กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

ศูนย์คอมพิวเตอร์และสารสนเทศ ได้มีการนำแผนงาน/โครงการ มาวิเคราะห์รายละเอียดความเสี่ยง ภายใต้ภารกิจรับผิดชอบ ดังนี้

ผลการประเมินความเสี่ยงในระบบสารสนเทศของโรงพยาบาลตามมาตรฐาน TMI

ลำดับ	ส่วนประกอบทางด้านสารสนเทศ	P	I	ค่าคะแนน	ระดับความเสี่ยง
1	Hacking / Intrusion / Malware	3	5	15	สูง
2	Server crash/failure	2	5	10	สูง
3	Network crash/failure	2	5	10	สูง
4	External fire	2	5	10	สูง
5	Workstation failure	4	2	8	ปานกลาง
6	Project failure	2	4	8	ปานกลาง
7	OS failure	3	2	6	ปานกลาง
8	Front office (HOSxP, PACs)	3	2	6	ปานกลาง
9	Back office (Finance)	3	2	6	ปานกลาง
10	No program document / comments	2	3	6	ปานกลาง
11	Vender stop support	1	5	5	ปานกลาง
12	Internal flood	1	5	5	ปานกลาง
13	Internal fire	1	5	5	ปานกลาง
14	Electricity	1	5	5	ปานกลาง
15	Theft / Break-ins / Protest / Mob	1	5	5	ปานกลาง
16	Intranet / Internet	1	4	4	ปานกลาง
17	Backup error / Data loss	1	2	2	ต่ำ
18	No data dictionary / System blueprint	1	2	2	ต่ำ
19	External flood	1	1	1	ต่ำ

หมายเหตุ ประเมินเมื่อ 15 พ.ค. 2560

วิธีแก้ไขความเสี่ยง (Risk treatment)

ระดับความเสี่ยงสูง

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
1.Hacking / Intrusion / Malware 1.1.Intrusion IP detected : FTP Brute force (ปี 58-59) 1.2. Web server hacked : www.nbhospital.com HTTP redirect (ปี 58-59) 1.3Web server hacked : www.nbhospital.go.th HTTP redirect (พ.ค.60) 1.4. Outbreak of Wannacry Ransomware outside (12พ.ค.60)	1. ลดโอกาสเกิด 2. ลดความเสียหาย	1.ใช้ระบบควบคุมและปิดกั้นการบุกรุกผ่านทางเครือข่าย (Firewall) 2.แก้ไขข้อบกพร่องของระบบปฏิบัติการและโปรแกรม Server software (Apache, IIS, PHP) โดยติดตั้งรุ่นล่าสุด 3.เฝ้าระวังตรวจสอบการบุกรุกหรือสิ่งผิดปกติของระบบอย่างสม่ำเสมอ 1.สำรองข้อมูลอย่างสม่ำเสมอ 2.ทบทวนและปรับปรุงนโยบายการควบคุมและปิดกั้นการสื่อสารข้อมูลผ่านเครือข่ายอย่างสม่ำเสมอ 3. ทบทวนนโยบายการบริหารการใช้งานของกลุ่มผู้ใช้งานในเครือข่ายอย่างสม่ำเสมอ 4. ใช้โปรแกรม Antivirus สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายให้ครอบคลุมทั้งองค์กร 5. ใช้นโยบายด้านความปลอดภัยให้ครอบคลุมทั้งผู้ใช้งานและผู้ดูแลระบบ	กิตติ หาญอาษา กิตติ หาญอาษา

วิธีแก้ไขความเสี่ยง (Risk treatment)

ระดับความเสี่ยงสูง

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
2.Server crash / failure 2.1.MySQL database structure corruption (ปี 58-59) 2.2.HOSxP bug: MySQL table duplicate primary key (ปี 59)	1.ลดโอกาสเกิด	1.ปรับปรุงโครงสร้างฐานข้อมูลใหม่ทุกเดือน 2. ตรวจสอบการใช้ Primary key และปรับปรุงรหัสนำหน้าเมื่อถึงเวลาที่เหมาะสม 3. ใช้นโยบายลดการสร้างสูตรยาเดิมซ้ำ 4. แจ้งผู้พัฒนาโปรแกรม HOSxP ให้ปรับปรุงแก้ไขข้อผิดพลาด	กิตติ หาญอาษา
	2. ลดความเสียหาย	1. สำรองข้อมูลอย่างสม่ำเสมอ 2. มีระบบฐานข้อมูลสำรองที่พร้อมใช้งานตลอดเวลา	กิตติ หาญอาษา

วิธีแก้ไขความเสี่ยง (Risk treatment)

ระดับความเสี่ยงสูง

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
3. Network crash / failure 3.1. Illegal router connection: IP conflict (ปี 59) 3.2.Switch power supply failure (ปี 59) 3.3.Switch operation failure (ปี 60)	1.ลดโอกาสเกิด	1. ใช้เครื่องสำรองไฟฉุกเฉินที่มีคุณสมบัติป้องกันไฟกระชากกับสวิตช์หลักให้ครอบคลุมทุกจุด 2. ใช้นโยบายควบคุมป้องกันการลักลอบเชื่อมต่ออุปกรณ์ที่ไม่ได้รับอนุญาตกับเครือข่ายของรพ. 3. ทบทวนและกำหนดแนวทางการควบคุมการซ่อมบำรุงสายไฟโดยช่างจากภายนอกรพ.ร่วมกับแผนกซ่อมบำรุง	กิตติ หาญอาษา
	2. ลดความเสียหาย	1. มีสวิตช์สำรองที่พร้อมใช้งานอย่างเพียงพอ 2. มีแบตเตอรี่สำรองเครื่องสำรองไฟฉุกเฉินที่พร้อมใช้งานอย่างเพียงพอ	กิตติ หาญอาษา

วิธีแก้ไขความเสี่ยง (Risk treatment)

ระดับความเสี่ยงสูง

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม	ผู้รับผิดชอบ
3. External fire 3.1.เครื่องอบผ้าไฟฟ้าลัดวงจร (ปี 59) 3.2. เตาอบไมโครเวฟไฟไหม้ (ปี60)	1. ลดโอกาสเกิด	1.ลดปัจจัยเสี่ยงต่อการเกิดอัคคีภัย 2.ตรวจสอบสภาพอุปกรณ์ไฟฟ้าอย่างสม่ำเสมอ 3.ใช้นโยบายควบคุมการทำงานของเจ้าหน้าที่ในอาคาร	กิตติ หาญอาษา
	2. ลดความเสียหาย	1. เฝ้าระวังเหตุอัคคีภัยตลอดเวลา และมีระบบแจ้งเตือนที่มีประสิทธิภาพ 2. มีการเตรียมพร้อมรับเมื่อเกิดเหตุอัคคีภัย	กิตติ หาญอาษา

แผนกิจกรรมการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน สารสนเทศเวชระเบียน **หน่วยงาน ศูนย์คอมพิวเตอร์** **วันที่จัดทำ 15 พ.ค .2560**

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 1 ข้อมูลและเอกสารสำคัญเวชระเบียนผู้ป่วยนอกและใน	1. ข้อมูลถูกจารกรรม 2. ข้อมูลเสียหาย จากโปรแกรมที่ประสงค์ร้าย 3. ระบบเก็บข้อมูล ถูกบุกรุก 4. สถานที่เก็บข้อมูลทางกายภาพถูกบุกรุก 5. สภานที่เก็บข้อมูลทางกายภาพถูกทำลายจากภัยภิบัติ เช่น ไฟไหม้ ฟ้าผ่า	1. จัดหา Firewall server และ Free firewall software	กิตติ, ครึ่งท่อน		ปี 59-60
		2. ดำเนินการตรวจสอบ Log อย่างสม่ำเสมอ	กิตติ		ปี 60
		3. ปรับปรุงระบบให้บริการเว็บให้ทันสมัย (Apache 2.4.2, IIS update, PHP4) เพื่ออุดช่องโหว่ของระบบ	อรสิทธิ์		ปี 60
		4. ปรับปรุงระบบปฏิบัติการให้ทันสมัย (Windows 7/10 patch) เพื่ออุดช่องโหว่ของระบบ	กิตติ,พัชระ		ปี 60
		5. จัดหาอุปกรณ์เพื่อทำระบบ Offline backup : External HDD ให้เพียงพอต่อการใช้งาน 3 เดือน อย่างน้อย 3 ชุด (อย่างน้อย 1 Terabytes)+HDD Docking	กิตติ	10,000.-	ปี 61
		6. ดำเนินการ Offline backup อย่างสม่ำเสมอ			
		7. ทบทวนการบริหารจัดการจัดการเครือข่ายโดยการจัดกลุ่มเครื่องลูกข่ายงานข้อมูลแยกส่วน(VLAN)และทบทวนปรับปรุงนโยบายการจัดการจราจรเครือข่าย (Traffic policy) ทุก 2-3 เดือน	กิตติ กิตติ		ปี 60 ปี 59-60
		8. จัดหาโปรแกรม Antivirus สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายที่ได้มาตรฐาน	อรสิทธิ์, กิตติ		ปี 60-61
		9. นโยบายด้านความปลอดภัยของข้อมูล : ผู้ใช้งาน และผู้ดูแลระบบ			
		10. ติดตั้งอุปกรณ์ตรวจจับความร้อนและควันไฟ พร้อมระบบแจ้งเตือน	เตือนศักดิ์,กิตติ วรวิช ครึ่งท่อน		ปี 60
		11. ติดตั้งอุปกรณ์ป้องกันฟ้าผ่า	ครึ่งท่อน,อรสิทธิ์	39,500	ปี 60
		12. ติดตั้งระบบควบคุมการเข้าออกโดยสแกนลายนิ้วมือและป้อนรหัสผ่าน	ครึ่งท่อน		ปี 58-59

		13. ติดตั้งระบบกล้องวิดีโอวงจรปิด พร้อมจัดเวรยามเพื่อสังเกตการณ์ตลอด 24 ชม. 14. จัดทำแผนปฏิบัติเมื่อเกิดอัคคีภัย 15. ดำเนินการซ้อมแผนอัคคีภัยอย่างน้อยปีละ 1 ครั้ง 16. อุปกรณ์ตรวจจับความชื้นห้องแม่ข่าย	ครึ่งท่อน, งานบริหาร ครึ่งท่อน,อรสิทธิ์ เตือนศักดิ์ เตือนศักดิ์ ครึ่งท่อน,อรสิทธิ์	34,150 69,000 81,000	ปี 60 ปี 60 ปี 60 ปี 60

แผนกิจกรรมการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน สารสนเทศเวชระเบียน **หน่วยงาน ศูนย์คอมพิวเตอร์** **วันที่จัดทำ 15 พ.ค .2560**

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 2 ครุภัณฑ์ระบบสารสนเทศ 2.1 เครื่องแม่ข่าย (Server) 2.1.1 Database HOSxP master server (MySQL) 2.1.2 Database HOSxP slave server (MySQL)	1. Database structure corrupt 2. Invalid primary key of “sp_use” bug 3. Data loss cause application (HOSxP) crash	1. ดำเนินการเฝ้าระวังฐานข้อมูลทำงานผิดพลาด และ Re-up structure ทุกเดือน 2. จัดทำแผนสำรองข้อมูล 3. จัดหาคอมพิวเตอร์แม่ข่ายสำรองให้พร้อมใช้งาน(DR site) 4. แจ้งผู้พัฒนาโปรแกรม HOSxP ให้ดำเนินการปรับปรับแก้ไขข้อผิดพลาด 5. ดำเนินการเฝ้าระวังตรวจสอบ Primary key ของตาราง “sp_use” และเปลี่ยนรหัสนำหน้าของ Primary key เมื่อถึงเวลาที่เหมาะสม 6. จัดทำนโยบายรณรงค์ให้ผู้ใช้งานนำสูตรยาที่มีรหัสเดิมมาใช้ใหม่ และประกาศใช้ 7. จัดระบบงานสำรองเพื่อใช้งานแทนระบบหลักที่ขัดข้อง ได้แก่ OPD scan viewer, HOSxP with database on notebook, PACS viewer 8. จัดทำแผนกู้คืนระบบงานหลักและระบบข้อมูลเมื่อเกิดความเสียหาย 9. ดำเนินการซ้อมแผนการใช้ระบบงานสำรองและกู้คืนระบบงานหลักอย่าสม่ำเสมออย่างน้อยปีละ 2 ครั้ง	กิตติ,ปิยะณัฐ กิตติ, เตือนศักดิ์ กิตติ, ครึ่งท่อน กิตติ,ปิยะณัฐ กิตติ,ปิยะณัฐ วรวิช,ปิยะณัฐ กิตติ, ปิยะณัฐ เตือนศักดิ์ กิตติ, เตือนศักดิ์ กิตติ, เตือนศักดิ์		ปี 59-ปัจจุบัน ปี 59-ปัจจุบัน ปี 60 มี.ค.59 ปี 59-ปัจจุบัน ปี 61 ปี 59-60 ปี 60 ปี 60

แผนกิจกรรมการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน สารสนเทศเวชระเบียน **หน่วยงาน ศูนย์คอมพิวเตอร์** **วันที่จัดทำ 15 พ.ค .2560**

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 2 ครุภัณฑ์ระบบสารสนเทศ 2.1 เครื่องแม่ข่าย (Server) 2.1.3 Gateway(HOSxP-LIS-PACs) server 2.1.4 Internet authentication server 2.1.5 Image scan database server 2.1.6 WWW + HOSxP report server 2.1.7 PHP + E-office server 2.1.8 RMC server 2.1.9 Referlink + DSR + TBCM + Thai cancer server 2.1.10 Referlink sync server 2.1.11 DNS1 + DNS2 server 2.1.12 EKG server 2.1.13 Firewall server	1. ภัยพิบัติทางกายภาพ ได้แก่ ความร้อน และไฟไหม้ (เนื่องจากใช้พื้นที่ชั้นบนภายในอาคารจ่ายกลาง ซึ่งมีกิจกรรมซักอบรีด และนึ่งเครื่องมือแพทย์ และได้รับแสงสะท้อนมากในเวลากลางวัน) 2. ระบบไฟฟ้าสำรองและระบบไฟฟ้าหลักไม่สเถียร (ไฟตกไฟดับบ่อย) 3. การถูกบุกรุกทางกายภาพและโจรกรรม (เนื่องจากในเวรดึกไมมีเจ้าหน้าที่ขึ้นปฏิบัติงานทั้งอาคารซึ่งอยู่ห่างไกลจากจุดที่มีผู้ปฏิบัติงาน และไม่มีอุปกรณ์ในการช่วยเฝ้าระวังที่มีประสิทธิภาพ)	1. ติดตั้งบานเกล็ดที่บริเวณภายนอกอาคารเพื่อลดความร้อนจากแสงสะท้อนในเวลากลางวัน 2. จัดทำแผนปฏิบัติเมื่อเกิดอัคคีภัย 3. ดำเนินการซ้อมแผนอัคคีภัยอย่างน้อยปีละ 1 ครั้ง 4. ติดตั้งถังดับเพลิงสีเขียวและสีแดงไว้บริเวณห้องคอมพิวเตอร์แม่ข่ายและห้องปฏิบัติงาน 5. ดำเนินการตรวจสอบความพร้อมใช้งานของถังดับเพลิงอย่างสม่ำเสมอทุกเดือน 6. ติดตั้งอุปกรณ์ตรวจจับความร้อนและควันไฟพร้อมระบบแจ้งเตือน 7. ติดตั้งกล้องวิดีโอวงจรปิดพร้อมจัดเวรยามเพื่อสังเกตการณ์ตลอด 24 ชม. 8. ติดตั้งอุปกรณ์สลับไฟฟ้าสำรองอัตโนมัติ 9. ดำเนินการตรวจสอบประสิทธิภาพของเครื่องสำรองไฟฟ้าฉุกเฉินสำหรับเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอทุกเดือน 10. ประสานการไฟฟ้าส่วนภูมิภาคเพื่อเชื่อมต่อสายไฟให้นำมาใช้งานได้อย่างเต็มประสิทธิภาพครบทั้ง 3 เฟส 11. ติดตั้งระบบควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและห้องปฏิบัติงานโดยสแกนลายนิ้วมือและป้อนรหัสผ่าน 12. ดำเนินการตรวจสอบอุณหภูมิในห้องคอมพิวเตอร์แม่ข่ายทุกวัน	ซ่อมบำรุง เตือนศักดิ์,อรสิทธิ์ เตือนศักดิ์,อรสิทธิ์ ซ่อมบำรุง,อรสิทธิ์ ซ่อมบำรุง,อรสิทธิ์ ครึ่งท่อน,อรสิทธิ์ ครึ่งท่อน ซ่อมบำรุง ครึ่งท่อน,อรสิทธิ์ ครึ่งท่อน,งานบริหาร ครึ่งท่อน,อรสิทธิ์ ครึ่งท่อน,อรสิทธิ์ เตือนศักดิ์,อรสิทธิ์ ครึ่งท่อน,เตือนศักดิ์,กิตติ		ปี 60-61 ปี 60 ปี 60 ปี 59-60 ปี 59-ปัจจุบัน ปี 60 ปี 60 ปี 59 ปี 59-60 ปี 59 ปี 60 ปี 60

หมวด 3 อาคารสถานที่ 3.1 ห้องคอมพิวเตอร์แม่ข่ายหลัก (ศูนย์คอมพิวเตอร์) 3.2 ห้องปฏิบัติงานเจ้าหน้าที่ (ศูนย์คอมพิวเตอร์)		13. จัดทำนโยบายควบคุมการทำงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ และประกาศใช้	เตือนศักดิ์		ปี 60

แผนกิจกรรมการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน สารสนเทศเวชระเบียน **หน่วยงาน ศูนย์คอมพิวเตอร์** **วันที่จัดทำ 15 พ.ค .2560**

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 2 ครุภัณฑ์ระบบสารสนเทศ 2.2 อุปกรณ์เครือข่าย (Network) 2.2.1 Switch หลัก อาคารอำนวยการชั้น 3 (การเงิน) 2.2.2 Switch หลัก อาคารวินิจฉัยชั้น 2 (ห้องปฏิบัติการ) 2.2.3 Switch Backbone หลักของแม่ข่ายรพ. 2.2.4 Router	1. Power failure 2. Device failure 3. Illegal device 4. Improper setting	1. ประสานงานซ่อมบำรุงเพื่อจัดการระบบไฟฟ้าที่สเถียร (ไฟฟ้า 3 เฟส) 2. ประสานงานซ่อมบำรุงเพื่อกำหนดแนวทางการควบคุมการซ่อมบำรุงสายไฟโดยช่างจากภายนอกรพ. 3. จัดหาอุปกรณ์สำรองไฟฉุกเฉินและป้องกันไฟกระชาก (UPS with surge protection) สำหรับ Switch หลักของแผนกพัสดุ 1 เครื่อง 4. ตรวจสอบความพร้อมใช้งานอุปกรณ์ Switch และอุปกรณ์สำรองไฟอย่างสม่ำเสมอ 5. จัดหาแบตเตอรี่ทดแทนของอุปกรณ์สำรองไฟฉุกเฉิน (UPS) ให้เพียงพอและพร้อมใช้งาน (เสื่อมปีละ 14 ลูก) 6. จัดหา Switch ทดแทนให้เพียงพอและ พร้อมใช้งาน (พร้อมใช้งาน 1 เครื่อง)	ครึ่งท่อน ครึ่งท่อน ครึ่งท่อน ครึ่งท่อน,อรสิทธิ์ ครึ่งท่อน,ศาตร์ตรา ครึ่งท่อน,อรสิทธิ์	 15,000 15,000 	ปี 59 ปี 59 ปี 58-59 ปี 60-61 ปี 60-61 ปี 60-61