

แผนบริหารจัดการความเสี่ยง
เทคโนโลยีสารสนเทศ
IT RISK MANAGEMENT

สารบัญ

บทนำ

สารบัญ

หน้า

หลักการและเหตุผล	1
วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง ผลที่คาดว่าจะได้รับ	1
ความหมายของการบริหารความเสี่ยง	2
ขอบเขตการดำเนินงานและสถานภาพเทคโนโลยีสารสนเทศและการบริหารจัดการ ในปัจจุบันของโรงพยาบาลบ้านฝ้อ	2-11
การวิเคราะห์การบริหารจัดการความเสี่ยง	12-14
การประมาณความเสี่ยง	14-16
การประเมินค่าความเสี่ยง	16-18
การรายงานผลการวิเคราะห์ความเสี่ยง	19-19
การจัดการความเสี่ยง	20-22

บทนำ

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลบ้านฝ้อ ประจำปี 2566 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยงและการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้บรรลุผลตามเป้าประสงค์ของหน่วยงาน เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ ทั้งทางตรงและทางอ้อม องค์กร จึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้ เลือกวิธีการที่เหมาะสมใน การบริหารความเสี่ยงเหล่านั้นให้ อยู่ในระดับที่องค์กรสามารถรองรับได้และทำให้ การปฏิบัติงานมีประสิทธิภาพ มากยิ่งขึ้นโรงพยาบาลบ้านฝ้อ หวังเป็นอย่างยิ่งว่าแผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านฝ้อนี้จะช่วยลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลกระทบต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านฝ้อ ต่อไป

กลุ่มงานเทคโนโลยีสารสนเทศ
โรงพยาบาลบ้านฝ้อ
สิงหาคม 2566

หลักการและเหตุผล

สืบเนื่องจากแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดให้มีการปรับเปลี่ยนบริการของภาครัฐ เพื่อตอบสนองการบริการประชาชน ผู้ประกอบการ ทุกภาคส่วนให้มีความสะดวก รวดเร็ว และแม่นยำ มีโครงสร้างการจัดเก็บและบริหารฐานข้อมูลที่เป็นบูรณาการ ไม่ซ้ำซ้อน สามารถรองรับการเชื่อมโยงการทำงาน ระหว่างหน่วยงาน และให้บริการประชาชนได้อย่างทั่วถึงและมีประสิทธิภาพ

การบริหารจัดการความเสี่ยง จึงมีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้องงานตามภารกิจของหน่วยงานให้รอดพ้นจากความเสียหายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย ซึ่งขั้นตอนในการบริหารจัดการความเสี่ยง ควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน มีกระบวนการในการบริหารจัดการความเสี่ยงด้าน เทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อให้การดำเนินงานตามภารกิจของหน่วยงานบรรลุผลตามวัตถุประสงค์ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่ง ผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่า ด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2556 เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุวัตถุประสงค์ตามภารกิจที่ตั้งไว้และเป็นการพัฒนาการปฏิบัติงานของหน่วยงาน เพื่อนำไปสู่การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

วัตถุประสงค์

1. เพื่อให้การจัดการภายในหน่วยงานมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านผือ
2. เพื่อให้มีการวางแผน การควบคุม แก่ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม
3. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในโรงพยาบาลบ้านผือ

ผลที่คาดว่าจะได้รับ

เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่อาจมีผลกระทบต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลบ้านผือ แล้วพิจารณาหาแนวทางใน

การป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานตามแผน

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์ สารสนเทศของหน่วยงาน เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ความความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง และพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชา

แผนการลดความเสี่ยง (Treatment Plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยง สำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชาเพื่อพิจารณาอนุมัติดำเนินการ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้เกิดวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็น สาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยง ในภายหลังได้อย่างถูกต้อง

ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของโรงพยาบาลบ้านผือ

สถานภาพเทคโนโลยีสารสนเทศและการบริหารจัดการในปัจจุบันของโรงพยาบาลบ้านผือ

ระบบเครือข่ายคอมพิวเตอร์

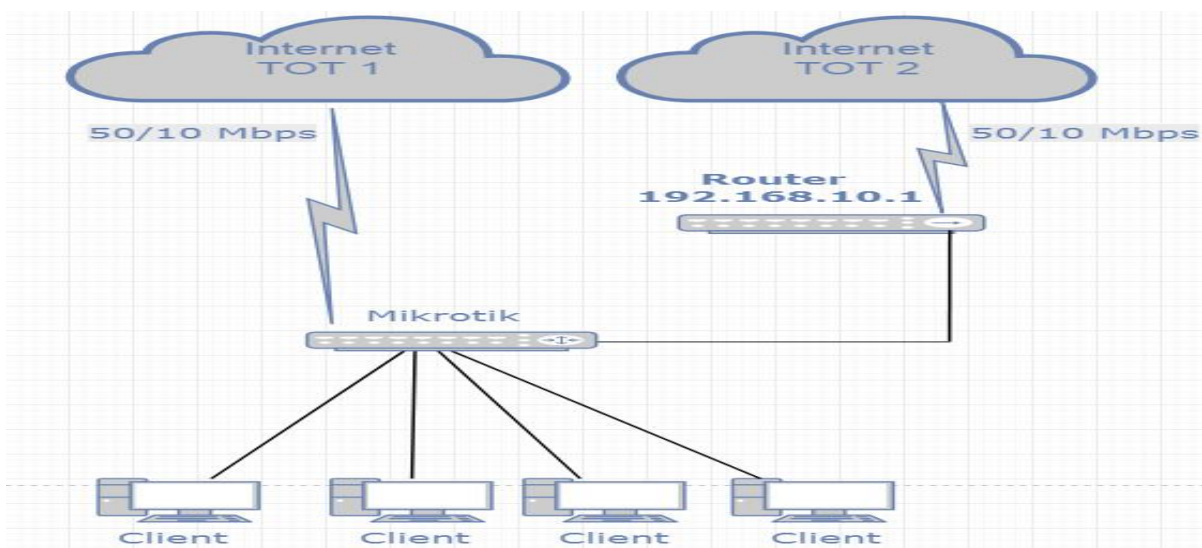
ระบบเครือข่ายของโรงพยาบาลบ้านผือ ประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (Wire Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองแยกการบริหารจัดการออกจากกัน โดยเครือข่ายใช้สาย (Wire Network) โรงพยาบาลบ้านผือจะเป็นผู้บริหารจัดการ ส่วนระบบเครือข่ายไร้สาย (Wireless Network) จะเป็นการใช้บริการจากผู้ให้บริการ อินเทอร์เน็ต (Internet service provider: ISP) โดยมีรายละเอียดของระบบเครือข่ายทั้ง 2 ประเภท ดังต่อไปนี้

1 . ระบบเครือข่ายใช้สาย (Wire Network) โรงพยาบาลบ้านผือ เครือข่ายใช้สายเชื่อมโยงกันระหว่างที่โรงพยาบาลบ้านผือและที่ ศูนย์สุขภาพชุมชน (PCU)

ซึ่งทั้ง 2 สถานที่ที่ผู้ให้บริการอินเทอร์เน็ตรายเดียวกันในการเชื่อมโยงระบบเครือข่ายใช้สายเข้าด้วยกันและใช้ในการออกสู่อินเทอร์เน็ต

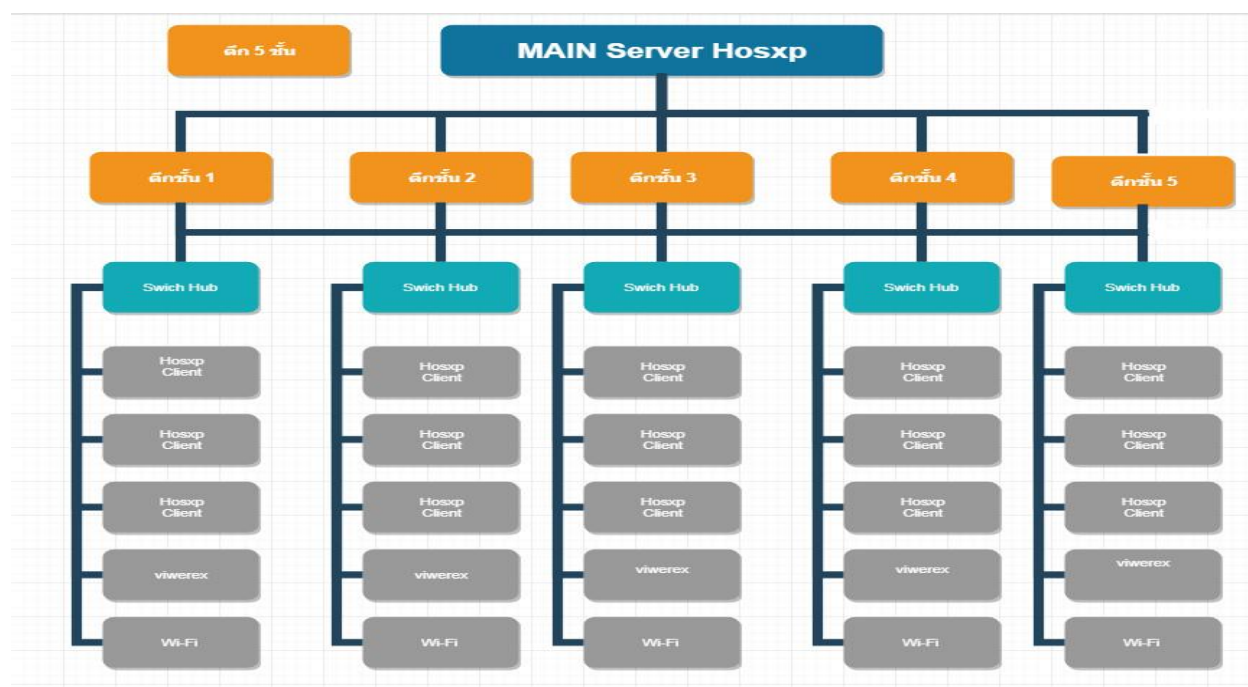
โรงพยาบาลบ้านผือ มีโครงข่ายอินเทอร์เน็ต ให้บริการแก่เจ้าหน้าที่ ประกอบด้วย

1. เครือข่ายโรงพยาบาลบ้านผือ ความเร็ว 100/20 Mbps จำนวน 2 โครงข่าย
2. เครือข่าย Hosxp ความเร็ว 50/10 Mbps จำนวน 1 โครงข่าย



รูปที่ 1 แสดงการเชื่อมโยงระบบเครือข่าย อินเทอร์เน็ต

โดยระบบเครือข่ายใช้สายภายในโรงพยาบาลบ้านผือ จะทำการเชื่อมโยงระบบเครือข่ายเข้ากับอุปกรณ์เครือข่ายของผู้ให้บริการอินเทอร์เน็ต (Internet Service provider: ISP) และ เชื่อมต่อมายังอุปกรณ์รักษาความมั่นคงปลอดภัยในระบบเครือข่าย โรงพยาบาลบ้านผือ จากนั้นจะทำการต่อเข้ากับอุปกรณ์เครือข่ายหลัก (Core Switch) ก่อน จะทำการกระจายไปยัง ลูกข่าย ตั้งแต่ชั้น ที่ 1 ถึงชั้นที่ 5 และตึกอื่น ๆ เพื่อใช้ในการดำเนินงานของโรงพยาบาลบ้านผือ



รูปที่ 2 แสดงระบบเครือข่ายที่โรงพยาบาลบ้านผือ

โรงพยาบาลบ้านผือได้ดำเนินการติดตั้งระบบป้องกันการบุกรุก (Network Security System) และระบบติดตามการทำงานของระบบเครือข่ายใช้สาย (Network Monitor System) เพื่อใช้ในการติดตามการทำงานของระบบเครือข่ายและเป็นการป้องกันการบุกรุกทางระบบเครือข่ายของโรงพยาบาลบ้านผือ โดยมีเจ้าหน้าที่ผู้ดูแลระบบเครือข่าย จะทำการเข้าติดตามการทำงานของอุปกรณ์ป้องกันการบุกรุกและการทำงานของระบบเครือข่ายทางหน้าเว็บเพจของอุปกรณ์โดยแบ่งเป็นอุปกรณ์ป้องกันการบุกรุกที่ 1 และ อุปกรณ์ป้องกันการบุกรุกที่ 2 ดังรูป

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (B/s)
0	shotspot-0-10>	10.0.1.213	5M	5M		
1	shotspot-0-10>	10.0.1.206	5M	5M		
2	shotspot-Somwang-2>	10.0.1.210	5M	5M		
3	shotspot-0-6>	10.0.1.187	10M	10M		
4	shotspot-Nid>	10.0.1.176	5M	5M		
5	shotspot-0-8>	10.0.0.120	5M	5M		
6	shotspot-1-2>	10.0.1.230	5M	5M		
7	shotspot-Nitaduen>	10.0.1.194	5M	5M		
8	shotspot-a-3>	10.0.1.105	10M	10M		
9	shotspot-Kaeng>	10.0.1.159	5M	5M		
10	shotspot-Nantiya>	10.0.1.214	5M	5M		
11	shotspot-0-6>	10.0.0.202	5M	5M		
12	shotspot-0-4>	10.0.1.216	5M	5M		
13	shotspot-36611>	10.0.1.45	5M	5M		
14	shotspot-EAY>	10.0.1.201	5M	5M		
15	shotspot-0-6>	10.0.1.39	5M	5M		
16	shotspot-2gpd>	10.0.0.201	1048576	1048576		
17	shotspot-gumthong>	10.0.2.49	5M	5M		
18	shotspot-0-7>	10.0.1.185	5M	5M		
19	shotspot-Jahamas>	10.0.1.38	5M	5M		
20	shotspot-Kittiyapom>	10.0.1.53	5M	5M		
21	shotspot-Maybosa-2>	10.0.1.89	5M	5M		
22	shotspot-Somwang-2>	10.0.0.185	5M	5M		
23	shotspot-saisawan>	10.0.1.193	5M	5M		
24	shotspot-0-9>	10.0.0.149	5M	5M		
25	shotspot-abc-2>	10.0.1.211	5M	5M		
26	shotspot-Lookmee>	10.0.1.199	5M	5M		
27	shotspot-0-0thong>	10.0.1.27	5M	5M		
28	shotspot-Sunnee>	10.0.0.254	5M	5M		
29	shotspot-Maybosa>	10.0.1.189	5M	5M		
30	shotspot-0-2>	10.0.1.195	5M	5M		
31	shotspot-Sunnee>	10.0.0.183	5M	5M		
32	shotspot-Saranya>	10.0.0.200	5M	5M		
33	shotspot-0-3>	10.0.3.116	5M	5M		
34	shotspot-NUY>	10.0.0.71	5M	5M		
35	shotspot-Saranya-2>	10.0.0.188	5M	5M		
36	shotspot-0-3>	10.0.3.61	5M	5M		
37	shotspot-kantida>	10.0.0.196	5M	5M		
38	shotspot-abc>	10.0.0.213	5M	5M		
39	shotspot-11023>	10.0.0.227	5M	5M		
40	shotspot-0-5>	10.0.1.166	5M	5M		
41	shotspot-ded>	10.0.0.206	5M	5M		
42	shotspot-0>	10.0.0.111	5M	5M		

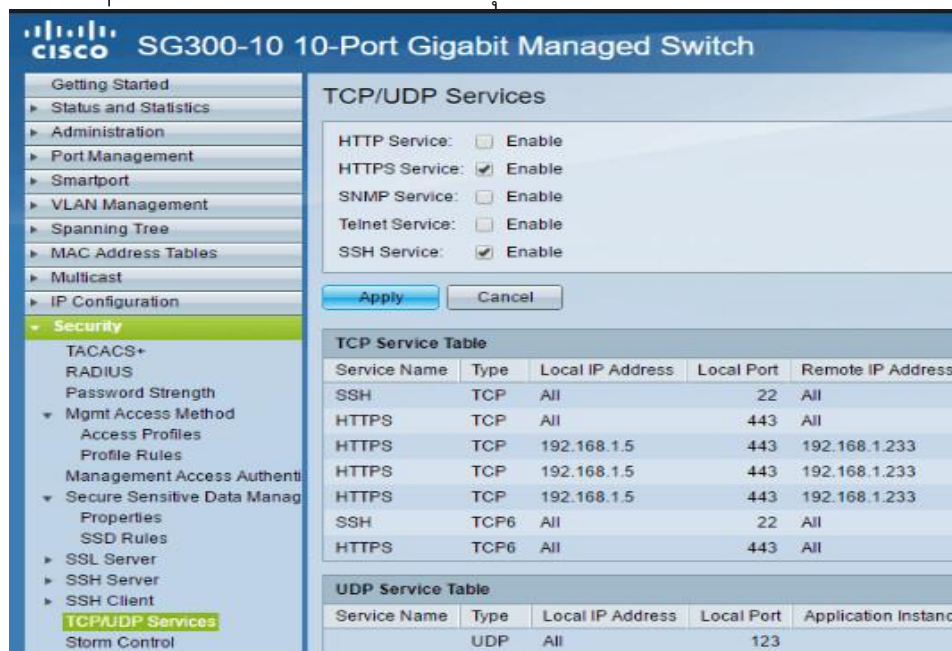
รูปที่ 3 แสดงสถานการณ์การทำงานของระบบป้องกันการบุกรุกที่ 1

จากรูปที่ 3 แสดงสถานการณ์การทำงานของอุปกรณ์ป้องกันการบุกรุกแสดงให้เห็น ว่า ทรัพยากรในระบบป้องกันการบุกรุกที่ 1 ยังเพียงพอต่อการทำงานของระบบ โดยหน่วยความจำถูกใช้งานร้อยละ 57 และประสิทธิภาพถูกใช้งานอยู่ที่ร้อยละ 11

#	Src	Address	Dst	Address	Prot	Conn	Timeout	TCP State	Outg./Rpt. Rate	Outg./Rpt. Bytes
0	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
1	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
2	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
3	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
4	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
5	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
6	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
7	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
8	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
9	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
10	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
11	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
12	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
13	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
14	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
15	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
16	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
17	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
18	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
19	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
20	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
21	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
22	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
23	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
24	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
25	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
26	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
27	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
28	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
29	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
30	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
31	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
32	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
33	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
34	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
35	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
36	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
37	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
38	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
39	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
40	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
41	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0
42	192.168.10.153	192.168.10.153	192.168.10.153	192.168.10.153	6	8	00:00:00	established	0	0

ที่ 4 แสดงสถานการณ์การทำงานของระบบป้องกันการบุกรุกที่ 2

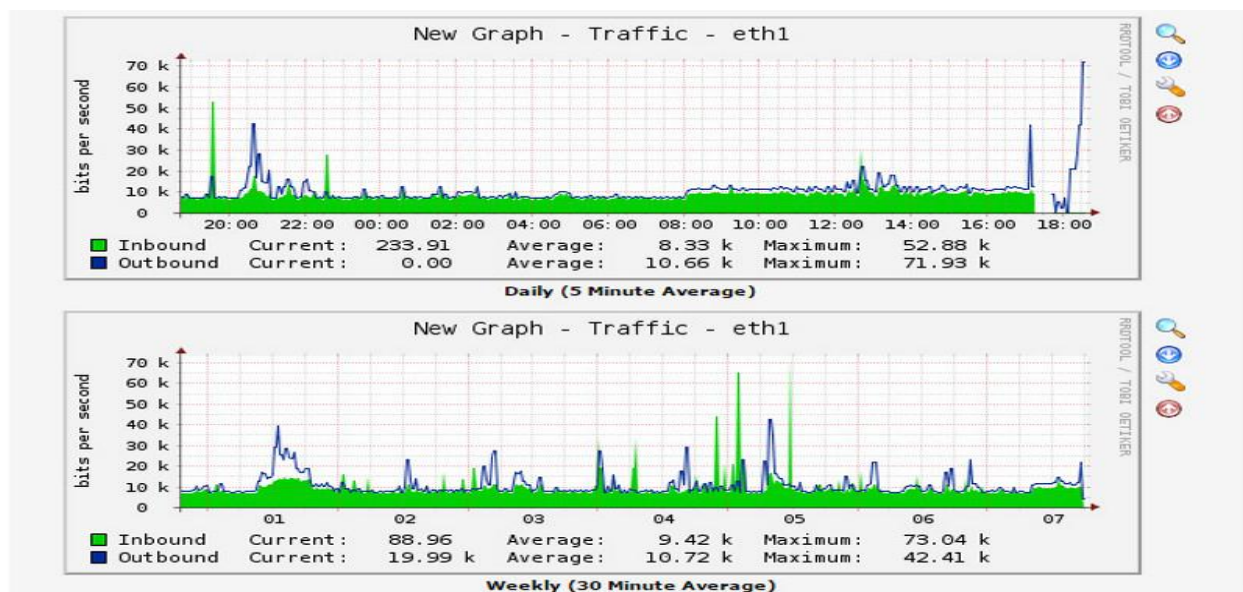
จากรูปที่ 4 แสดงสถานการณ์การทำงานของอุปกรณ์ป้องกันการบุกรุกแสดงให้เห็น ว่า ทรัพยากรในระบบป้องกันการบุกรุกที่ 2 ยังเพียงพอต่อการทำงานของระบบ และมีการติดตั้งอุปกรณ์ป้องกันการบุกรุกในลักษณะทำงานทดแทนกันได้ ในกรณีที่ตัวใดตัวหนึ่งไม่สามารถทำงานได้ โดยหน่วยความจำถูกใช้งานร้อยละ 54 และทรัพยากรอื่นๆ เหลือเพียงพอต่อการใช้งานในปัจจุบัน



รูปที่ 5 แสดงสถานการณ์การทำงานของอุปกรณ์เครือข่ายหลัก (Core Switch)

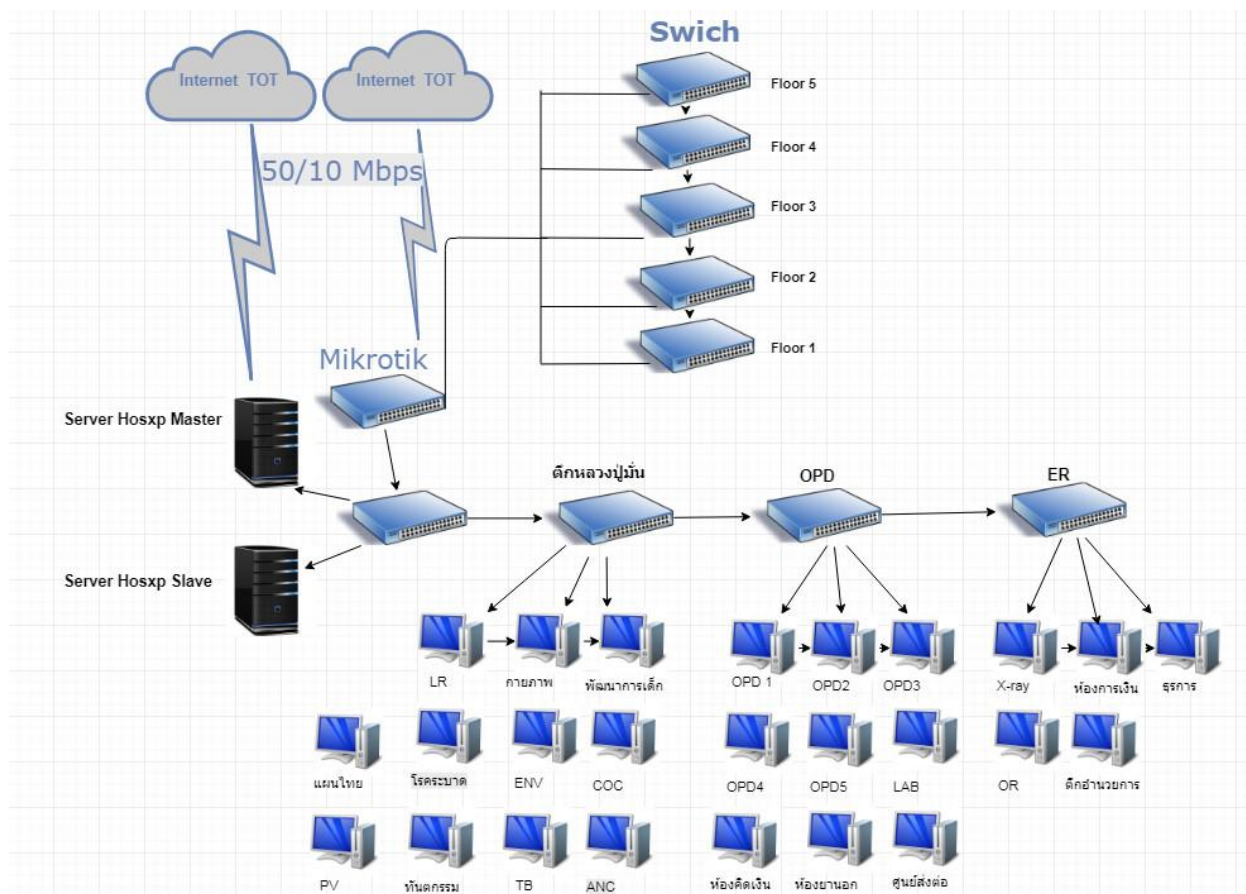
จากรูปที่ 5 แสดงสถานการณ์การทำงานของอุปกรณ์เครือข่ายหลัก (Core Switch) แสดงให้เห็นว่า ทรัพยากรเพียงพอต่อการทำงาน โดยจากรูปหน่วยความจำของอุปกรณ์เครือข่ายหลัก ถูกใช้งานร้อยละ 31 และหน่วยประมวลผลถูกใช้งานร้อยละ 4 ส่วนอุปกรณ์เครือข่ายที่ติดตั้งให้กับหน่วยงานต่าง มีทรัพยากรเพียงพอต่อการทำงานของอุปกรณ์ รวมทั้งได้รับการดูแลบำรุงรักษา และ แก้ไข ปัญหา เช่นเดียวกับ อุปกรณ์เครือข่ายหลัก

โรงพยาบาลบ้านฝ้อ ได้ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์ และระบบเครือข่าย (Authentication) สำหรับใช้ในการติดตามการทำงานของระบบใช้ โรงพยาบาลบ้านฝ�



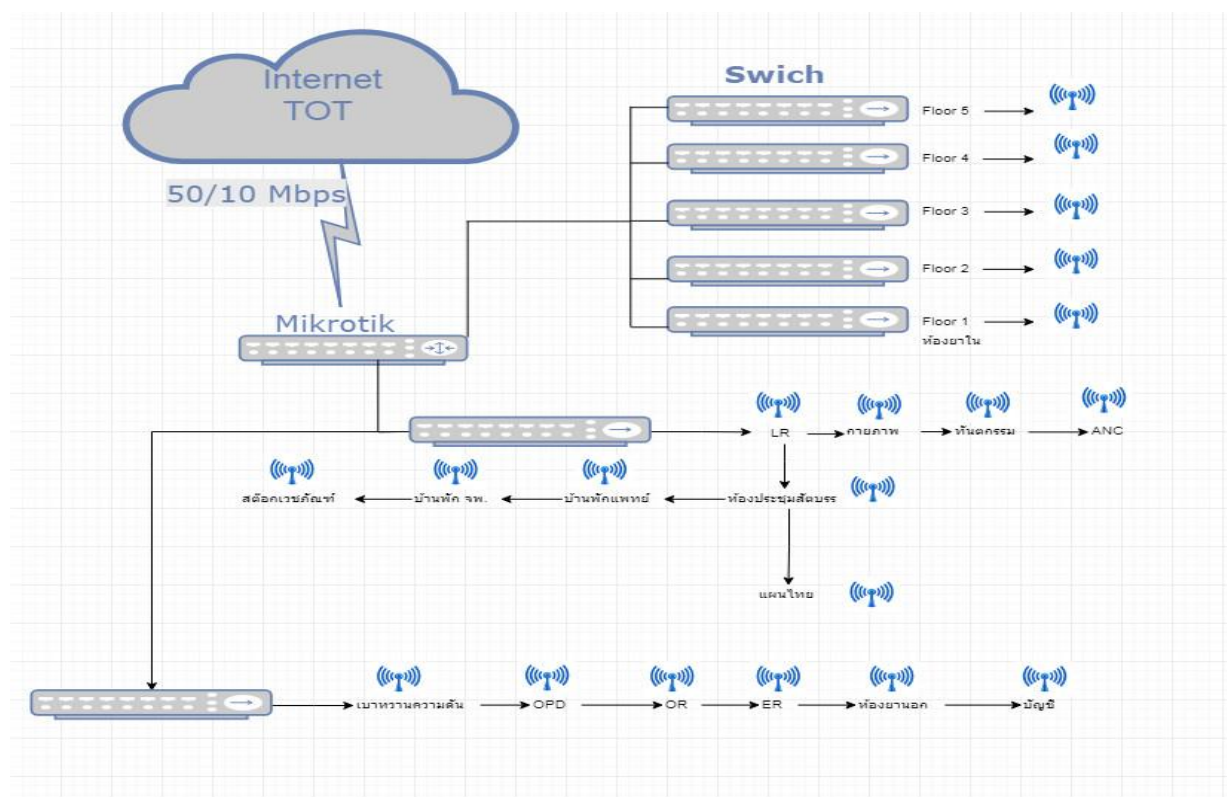
รูปที่ 6 แสดงการทำงานของโปรแกรมติดตามการทำงานของระบบเครือข่าย

ระบบเครือข่ายใช้สายภายในโรงพยาบาลบ้านฝ้อ จะมีลักษณะคล้ายคลึงกันกับการเชื่อมต่อระบบเครือข่ายจากผู้ให้บริการอินเทอร์เน็ตมายังอุปกรณ์ควบคุมเส้นทางงานในระบบเครือข่ายของศูนย์ (Router) และเชื่อมต่อไปยังอุปกรณ์ป้องกันการบุกรุก รุก (Firewall) แล้วต่อเข้าอุปกรณ์เครือข่ายหลักของศูนย์ฯ (Core Switch) ก่อนจะกระจายไปยังส่วนงาน ต่างๆ ภายใน โรงพยาบาลบ้านฝ้อ



รูปที่ 7 แสดงระบบเครือข่ายโรงพยาบาลบ้านฝ้อ

2.ระบบเครือข่ายไร้สาย (Wireless Network) ปัจจุบัน โรงพยาบาลบ้านฝ้อ ได้ให้บริการระบบเครือข่ายไร้สายจากผู้ให้บริการอินเทอร์เน็ต ทั้งที่โรงพยาบาลบ้านฝ้อ โดยผู้ให้บริการอินเทอร์เน็ตได้ทำการติดตั้งจุดกระจายสัญญาณ (Access Point) เข้ากับระบบ เครือข่ายหลักของ โรงพยาบาลบ้านฝ้อ และใช้วิธีทำงานเทคนิคในการบังคับให้ผู้ใช้งานสามารถใช้งานเครือข่ายไร้สายเฉพาะบริการอินเทอร์เน็ตเพียงอย่างเดียว ไม่สามารถเข้าใช้งานระบบงานภายในของ โรงพยาบาลบ้านฝ้อได้ และมีการควบคุมสิทธิในการใช้งานระบบเครือข่ายไร้สายอีกด้วย



รูปที่ 8 แสดงระบบเครือข่ายไร้สายที่โรงพยาบาลบ้านฝ้อ

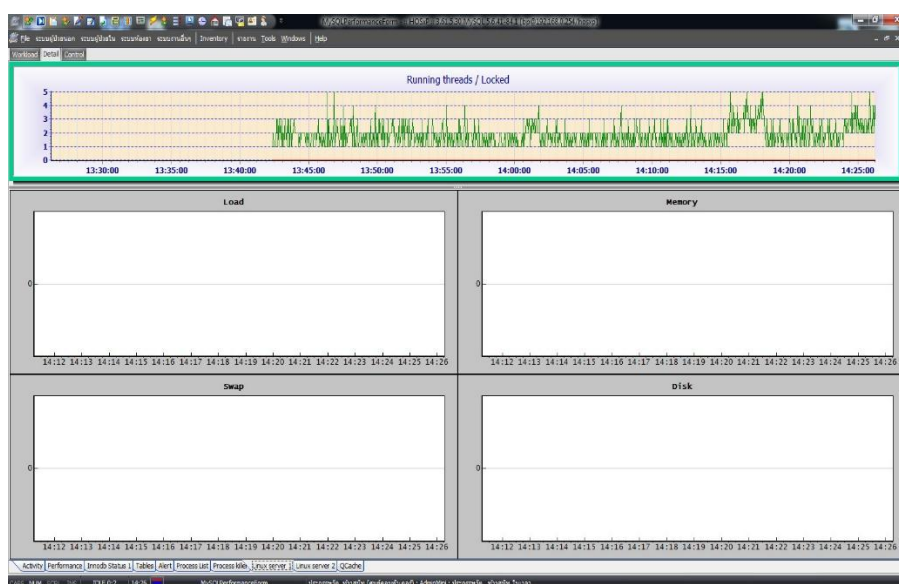
ระบบคอมพิวเตอร์

โรงพยาบาลบ้านฝ้อได้ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง ปัจจุบันได้นำเทคโนโลยีแร็คเซิร์ฟเวอร์ (Rack Server) เข้ามาใช้งาน โดยนำเครื่องแม่ข่ายที่มีความสำคัญต่างๆ ไปติดตั้งไว้ในแร็คเซิร์ฟเวอร์ (Rack Server) ซึ่งจะทำให้ลดปัญหาที่เกิดจากอุปกรณ์ เครื่องแม่ข่ายชำรุดและส่งผลกระทบต่อการทำงานของเครื่องแม่ข่ายนั้นได้ โดยระบบที่สำคัญต่อการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่อยู่แร็คเซิร์ฟเวอร์ (Rack Server) เช่น ระบบป้องกันไวรัส ระบบติดตามและบริหารการทำงานของระบบเครือข่าย (Network Monitor) ระบบบริหารเครื่องแม่ข่ายเสมือนในแร็คเซิร์ฟเวอร์ และระบบฐานข้อมูลของโรงพยาบาลบ้านฝ้อ เป็นต้น



รูปที่ 10 แสดงภาพรวม แร็คเซิร์ฟเวอร์ 42U (Rack Server)ของรพ.บ้านผือ

โรงพยาบาลบ้านผือ มีระบบบันทึกข้อมูล (Storage) สำหรับจัดเก็บฐานข้อมูล และ ข้อมูลต่างๆ ของโรงพยาบาลบ้านผือ แยกจากแร็คเซิร์ฟเวอร์ (Rack Server) ซึ่งเป็นไปตามหลักการใช้งานเทคโนโลยีนี้ โดยระบบบันทึกข้อมูลมีความจุ (Capacity) ทั้งสิ้นประมาณ 4 เทระไบต์ (Tera Byte) ปัจจุบันยังมีความ เพียงพอต่อการใช้งานและสามารถรองรับการใช้งานได้ในระยะเวลา 3 ปี



รูปที่ 11 แสดงภาพรวม ระบบบันทึกข้อมูล (Storage) ของรพ.บ้านผือ

ตารางแสดงเซิร์ฟเวอร์ (Blade Server) ที่อยู่ในความดูแลของโรงพยาบาลบ้านฝ้อ

ชื่อ Server	หมายเลข IP	หน่วยงาน	ผู้ติดต่อ	เบอร์ติดต่อ	cpu/ram(v isual)	Hard disk (Physical)	ระบบปฏิบัติการ OS
HOSxP	192.168.0.254	ศูนย์เทคโนโลยี สารสนเทศ	อิทธิพล ผลทิพย์	181	8:16	250*4	CentOs7
HOSxP Slave	192.168.0.2	ศูนย์เทคโนโลยี สารสนเทศ	อิทธิพล ผลทิพย์	181	4:8	250*2	CentOs6
Wi-Fi	192.168.2.1	ศูนย์เทคโนโลยี สารสนเทศ	บุญเพ็ง ตริรัตน์	181	4:4	-	Router
Lis	192.168.0.3	ห้อง LAB	ลำไพร มุ่งแสง	107	4:8	250*4	Windows server 2008
Pack	192.168.0.40	X-ray	วิทยา ทวีวัฒนเสถียร	165	4:8	250*4	Windows server 2008

สถานภาพครุภัณฑ์ คอมพิวเตอร์โรงพยาบาลบ้านฝ้อ ประจำปี พ.ศ. 2566

สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งโปรแกรมพื้นฐานต่างๆ ที่ โรงพยาบาลบ้านฝ้อ ใช้ ในการดำเนินงานปัจจุบันจะมีการสำรวจสภาพความพร้อมใช้ และแผนในการจัดหาทดแทนประจำปี โดยศูนย์เทคโนโลยีสารสนเทศได้ ทำการสำรวจข้อมูล ณ ปีงบประมาณ พ.ศ. 2566 มีรายละเอียดดังตารางต่อไปนี้

ตารางแสดงรายการเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของโรงพยาบาลบ้านฝ้อ

ลำดับ	รายการครุภัณฑ์คอมพิวเตอร์	จำนวน (เครื่อง)	หมายเหตุ
1	เครื่องคอมพิวเตอร์แม่ข่าย	4	
2	เครื่องคอมพิวเตอร์ (PC)	190	
3	เครื่องคอมพิวเตอร์โน้ตบุ๊ก	10	
4	เครื่องพิมพ์ชนิดเลเซอร์	80	
5	เครื่องพิมพ์ชนิดฉีดหมึก (Inkjet Printer)	4	
6	เครื่องสแกนเนอร์	2	
7	เครื่องสำรองไฟฟ้า	15	
8	เครื่องพิมพ์ชนิด Design jet	7	
9	Scanner ชนิด Scan jet	2	
10	โปรแกรมระบบปฏิบัติการ Windows	190	
11	โปรแกรม Microsoft Office	190	
12	SQL Server	1	
13	Microsoft Access 2013	30	
14	Windows Server	2	

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานสามารถแยกประเภทความเสี่ยงเป็น 7 ประเภท ดังนี้

1. ความเสี่ยงจากผู้ปฏิบัติงาน (People ware) เป็นความเสี่ยงที่ อาจเกิดขึ้นจากการดำเนินการการบริหารจัดการสิทธิ์ในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ หรืออนุญาตให้ผู้อื่นใช้สิทธิ์ในการเข้าถึงระบบ อาจทำให้เกิดความเสียหายต่อระบบและข้อมูลสารสนเทศได้
2. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิด ขึ้นจากระบบคอมพิวเตอร์ เครื่อง มือหรืออุปกรณ์เทคโนโลยีสนับสนุน ถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดีถูกก่อกวนจาก Hacker หรือถูกเจาะ ทำลายระบบจาก Cracker
3. ความเสี่ยงด้าน อุปกรณ์ (Hardware) เป็นความเสี่ยงที่อาจเกิดขึ้นจากอุปกรณ์ต่อพ่วง อุปกรณ์เครือข่าย ทำหน้าที่สนับสนุนการทำงานของคอมพิวเตอร์ในลักษณะต่าง ๆ เช่น External Hard disk, Flash Drive, Switch, Router, SD Card เป็นต้น
4. ความเสี่ยง ด้านโปรแกรมคอมพิวเตอร์ (Software) ระบบงาน การใช้โปรแกรมละเมิดลิขสิทธิ์ต่าง ๆ ซึ่งขัดต่อระเบียบ กฎหมายที่เกี่ยวข้อง และอาจส่งผลให้ไม่สามารถใช้งานโปรแกรมได้เต็มประสิทธิภาพ
5. ความเสี่ยงด้านสถานการณ์ฉุกเฉิน คือความเสี่ยงที่เกิดจากภัยพิบัติตามธรรมชาติ เช่น ไฟฟ้าดับ ไฟกระชาก ไฟไหม้ น้ำท่วม การชุมนุมประท้วง เป็นต้น
6. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการเปลี่ยนแปลงแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการทำงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- 7.

ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
1. ความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านเทคนิค	- ผู้ใช้ขาดความระมัดระวังในการใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าสู่ระบบหรือใช้งานแทน - ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker - ขาดการกำหนดนโยบายในการให้บริการ Web Service	- การสวมรอยผู้ใช้ - การเข้าถึง ข้อมูล/เปลี่ยนแปลง ข้อมูล - โอยไม่ได้รับอนุญาต - การเปิดช่องให้มีการเข้าถึงระบบได้จากภายนอก - เปิดให้บริการ Web Service โดยไม่กำหนด ช่วงเวลา	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์ - แม่ข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านอุปกรณ์	ผู้ใช้ขาดความระมัดระวังในการใช้ ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อ ระบบเครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาต และมีการ กำหนดค่า (Configuration) ที่ไม่ถูกต้อง ทำให้ อุปกรณ์ หรือ เครื่องคอมพิวเตอร์อื่น ในระบบ เครือข่ายไม่สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่ต่อระบบรักษา ความปลอดภัยของหน่วยงาน	- การนำอุปกรณ์ อื่นมาเชื่อมต่อเข้า ระบบ - ความล้มเหลว ทางเทคนิค - การใช้อุปกรณ์ใน การถ่ายโอนข้อมูล	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับไฟกระชาก	ความเสี่ยงด้านเทคนิค/ความเสี่ยงสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือ เกิดไฟกระชาก ทำให้เครื่อง คอมพิวเตอร์และอุปกรณ์ต่าง ๆ อาจได้รับความเสียหายจาก แรงดันไฟฟ้าไม่คงที่หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้ เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิด ไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูล สารสนเทศบางส่วนเกิดการสูญ หาย หรือไม่สามารถให้บริการได้ เช่น ระบบงานภายใน รพ.บ้านฝ้อ	- การเกิดภัยพิบัติ ต่าง ๆ - การชำรุด เสียหายของ อุปกรณ์ หรือ ความพร้อมของ อุปกรณ์ในการ รับมือต่อ สถานการณ์ ฉุกเฉิน ต่าง ๆ - ระบบไฟสำรองไม่ สามารถสำรอง ไฟฟ้าสำหรับห้อง server ได้ตลอดเวลา	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย/อุปกรณ์ เครือข่าย
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี/การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน/ ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจ ส่งผลให้โปรแกรมไม่มี ประสิทธิภาพ อาจก่อให้เกิดการ บุกกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker /Cracker เป็นต้น การ ดักจับข้อมูล การส่งข้อมูลคำสั่ง เจตนาร้าย การติดไวรัส Malware, Worm ต่าง ๆ	- การใช้ โปรแกรมลิขสิทธิ์	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ ข่าย/อุปกรณ์ เครือข่าย
5. ความเสี่ยงจากการขาดทักษะ ความชำนาญ เฉพาะด้านของบุคลากร ผู้ปฏิบัติงาน/บุคลากรไม่ ¹ เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดทักษะความชำนาญเฉพาะ ด้าน ทำให้การทำงานอาจเกิด ข้อผิดพลาด และจำนวนบุคลากร ที่มีไม่ ¹ เพียงพอต่อระบบเทคโนโลยี สารสนเทศที่เพิ่มขึ้น ส่งผลกระทบ ต่อการควบคุมดูแลระบบ	- บุคลากรไม่ เพียงพอ/บุคลากร ไม่พัฒนา ศักยภาพ ให้เกิดความชำนาญเฉพาะ ด้าน	ผู้ใช้งาน ระบบ สารสนเทศ ผู้ดูแลระบบ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบาย ผู้บังคับบัญชา / เปลี่ยนแปลง ผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการเทคโนโลยีสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- การ เปลี่ยนแปลง นโยบาย ผู้บริหารทำให้ขาดความ ต่อเนื่อง	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย/อุปกรณ์ เครือข่าย
7 ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุนการปฏิบัติงาน ทำให้ทำให้ไม่สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกองค์กร หรือไม่สามารถเข้ากันได้กับเทคโนโลยีสมัยใหม่	-การ เปลี่ยนแปลง ทางด้าน เทคโนโลยีเพื่อ ตอบสนองภารกิจ งานตามนโยบายภาครัฐ -ระยะเวลาใน การตั้งงบประมาณ	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย/อุปกรณ์ เครือข่าย

การประมาณความเสี่ยง

โดยโรงพยาบาลบ้านผือ กำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับความรุนแรง โอกาสที่จะเกิดความเสี่ยง ระดับความเสี่ยง ดังนี้

ระดับและโอกาสในการเกิดเหตุการณ์ต่าง ๆ			ระดับความรุนแรง (5 คะแนน)	
ระดับ	โอกาสที่จะเกิด	คำอธิบาย	ต่อระบบงาน	ต่อพันธกิจ
5	สูงมาก	5 ครั้ง/ปี	5	5
4	สูง	4 ครั้ง/ปี	4	4
3	ปานกลาง	3 ครั้ง/ปี	3	3
2	น้อย	2 ครั้ง/ปี	2	2
1	น้อยมาก	1 ครั้ง/ปี	1	1

ตารางแสดงการประมาณความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง
1. ความเสี่ยงจากการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน/ ความเสี่ยงด้านเทคนิค	ผู้ใช้ขาดความระมัดระวังในการ ใช้ระบบ สารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้ รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งาน แทน ถูกก่อกรวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ขาดการกำหนดนโยบายในการให้บริการ Web Service	5	2
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับ อนุญาต มาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน/ ความเสี่ยงด้านอุปกรณ์	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบ เครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อกับระบบ เครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาต และมีการกำหนดค่า (Configuration) ที่ ไม่ถูกต้อง ทำให้ อุปกรณ์ หรือเครื่อง คอมพิวเตอร์อื่น ในระบบเครือข่าย ไม่สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่กับ ระบบรักษาความปลอดภัยของหน่วยงาน การใช้อุปกรณ์ในการถ่ายโอนข้อมูล	2	3
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟ กระชาก	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงสถานการณ์ อุกเหต	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดไฟ กระชาก ทำให้เครื่องคอมพิวเตอร์และ อุปกรณ์ต่าง ๆ อาจได้รับความเสียหายจาก แรงดันไฟฟ้าไม่คงที่หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่าย คอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำ ให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย หรือไม่'สามารถให้บริการได้	5	4
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ ไม่ประสงค์ ดี/การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน/ ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจส่งผลให้ โปรแกรมไม่มีประสิทธิภาพ อาจก่อให้เกิด การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker /Cracker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส Malware, Worm ต่าง ๆ	5	4

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง
5. ความเสี่ยงจากการขาดทักษะความชำนาญเฉพาะด้านของบุคลากร ผู้ปฏิบัติงาน/บุคลากรไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดทักษะความชำนาญเฉพาะด้าน ทำให้การทำงานอาจเกิดข้อผิดพลาด และ จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบ เทคโนโลยีสารสนเทศที่เพิ่มขึ้นส่งผลกระทบต่อ การควบคุมดูแลระบบ	3	2
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบาย ผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้ นโยบายการบริหารจัดการเทคโนโลยี สารสนเทศเปลี่ยนแปลงด้วย ทำให้การ ดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	1	3
7. ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุน การปฏิบัติงาน ทำให้ทำให้ไม่สามารถ เชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายใน และภายนอกองค์กร หรือไม่สามารถเข้ากัน ได้กับเทคโนโลยีสมัยใหม่	1	3

การประเมินค่าความเสี่ยง

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยต่าง ๆ เช่น โอกาสที่จะเกิดภัยคุกคาม ระดับผลกระทบ ความรุนแรงที่มีต่อระบบ

ระดับความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง
1-5	ต่ำ	ยอมรับความเสี่ยง
6-10	ปานกลาง	ยอมรับความเสี่ยง
11-15	สูง	ควบคุมความเสี่ยง
20	สูงมาก	ควบคุมความเสี่ยง

ตารางแสดงการประเมินความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
1. ความเสี่ยงจาก การเข้าถึงข้อมูล ของบุคคลอื่น	ความเสี่ยงจาก ผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบ สารสนเทศ เช่น การให้ผู้อื่นใช้รหัสผ่านของ ตนเองเข้าใช้ระบบหรือใช้งานแทน การตั้งค่าให้ระบบจำรหัสผ่านในการเข้าใช้ งาน	5	2	10
2. ความเสี่ยงจาก การนำเอาอุปกรณ์ อื่นที่ไม่ได้รับ อนุญาตมาเชื่อมต่อ	ความเสี่ยงจาก ผู้ปฏิบัติงาน/ ความเสี่ยงด้านอุปกรณ์	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อต่อบริเวณเครือข่ายของหน่วยงาน โดยไม่ได้ปฏิบัติตาม อนุญาต และมีการกำหนดค่า (Configuration) ที่ ไม่ถูกต้อง ทำให้ อุปกรณ์ หรือเครื่อง คอมพิวเตอร์อื่น ในระบบเครือข่ายไม่ สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่กับ ระบบรักษาความปลอดภัยของหน่วยงาน	2	3	6
3. ความเสี่ยงจาก กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟ กระจาย	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดไฟกระจาย ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ อาจได้รับความเสียหายจาก แรงดันไฟฟ้าไม่คงที่หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย หรือไม่สามารถให้บริการได้	5	4	20
4. ความเสี่ยงจาก การถูกบุกรุก โดยผู้ ไม่ประสงค์ดี/การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจาก ผู้ปฏิบัติงาน/ ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจส่งผลให้ โปรแกรมไม่มีประสิทธิภาพ อาจก่อให้เกิด การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker /Cracker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่ง เจตนาร้าย การติดไวรัส Malware, Worm ต่าง ๆ	5	4	20

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
5.ความเสี่ยงจาก การขาดทักษะ ความชำนาญเฉพาะด้านของ บุคลากร ผู้ปฏิบัติงาน/ บุคลากรไม่เพียงพอ	ความเสี่ยงด้านการบริหาร จัดการ	การขาดทักษะความชำนาญเฉพาะด้าน ทำให้การทำงานอาจเกิดข้อผิดพลาด และ จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบ เทคโนโลยีสารสนเทศที่เพิ่มขึ้น ส่งผลกระทบ ต่อการควบคุมดูแลระบบ	3	2	6
6.ความเสี่ยงจาก การเปลี่ยนแปลง นโยบาย ผู้บังคับบัญชา / เปลี่ยนแปลง ผู้บังคับบัญชา	ความเสี่ยงด้านการบริหาร จัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้ นโยบายการบริหารจัดการเทคโนโลยีสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	1	3	3
7.ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุน การปฏิบัติงาน ทำให้ทำให้ไม่สามารถ เชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายใน และภายนอกองค์กร หรือไม่สามารถเข้าค้น ได้กับเทคโนโลยีสมัยใหม่	1	3	3

การรายงานผลการวิเคราะห์ความเสี่ยง

จากผลการประเมินความเสี่ยงสามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพ ดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
1	ความเสี่ยงจากการ เข้าถึงข้อมูลของบุคคล อื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน การตั้งค่าให้ระบบจำรหัสผ่านในการเข้าใช้งาน	10
2	ความเสี่ยงจากการ นำเอาอุปกรณ์อื่นที่ไม่ได้ รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงด้านอุปกรณ์	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless Router หรือ Switch/Hub มาเชื่อมต่อระบบเครือข่ายของหน่วยงาน โดยไม่ได้รับอนุญาต และมีการกำหนดค่า (Configuration) ที่ไม่ถูกต้อง ทำให้อุปกรณ์ หรือเครื่องคอมพิวเตอร์อื่น ในระบบเครือข่ายไม่สามารถใช้งานได้ อาจทำให้เกิดช่องโหว่ระบบรักษาความปลอดภัยของหน่วยงาน	6
3	ความเสี่ยงจาก กระแสไฟฟ้า ชัดข้อง ไฟฟ้าดับ ไฟกระชาก	ความเสี่ยงด้านเทคนิค/ความเสี่ยงสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดไฟกระชาก ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ อาจได้รับความเสียหายจากแรงดันไฟฟ้าไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูก ปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วน เกิดการสูญหาย หรือไม่สามารถให้บริการได้	20
4	ความเสี่ยงจากการถูก บุกกรุก โดยผู้ไม่ประสงค์ ดี/การใช้โปรแกรมละเมิดลิขสิทธิ์	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน/ ความเสี่ยงทางด้าน Software	การใช้โปรแกรมละเมิดลิขสิทธิ์อาจส่งผลให้โปรแกรมไม่มีประสิทธิภาพ อาจก่อให้เกิดการบุกรุกโจมตีโดยผู้ไม่ประสงค์ ดี เช่น Hacker /Cracker เป็นต้น การดักจับข้อมูล การส่งข้อมูลค่าส่งเจตนาร้าย การติดไวรัส Malware, Worm ต่างๆ	20

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
5	ความเสี่ยงจากการขาด ทักษะ ความชำนาญ เฉพาะด้านของ บุคลากร ผู้ปฏิบัติงาน/บุคลากร ไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดทักษะความชำนาญเฉพาะด้าน ทำให้การทำงาน อาจเกิดข้อผิดพลาด และจำนวนบุคลากรที่มีไม่เพียงพอต่อ ระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นส่งผลกระทบต่อ การควบคุมดูแลระบบ	6
6	ความเสี่ยงจากการ เปลี่ยนแปลง นโยบาย ผู้บังคับบัญชา	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการ บริหารจัดการเทคโนโลยีสารสนเทศเปลี่ยนแปลงด้วย ทำให้ การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	3
7	ความเสี่ยงจากการ เปลี่ยนแปลง เทคโนโลยี สมัยใหม่	ความเสี่ยงด้านเทคนิค	ขาดเทคโนโลยีสมัยใหม่ที่สามารถสนับสนุนการปฏิบัติงาน ทำให้ทำให้ไม่สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานทั้ง ภายในและภายนอกองค์กร หรือไม่สามารถเข้ากันได้กับ เทคโนโลยีสมัยใหม่	3

การจัดการความเสี่ยง

หน่วยงานกำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ 10 ขึ้นไป ส่วนความเสี่ยงที่มีระดับต่ำกว่า 10 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการ ความเสี่ยง	แนวทางการดำเนินการ จัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
1	ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	10	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักใน เรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสีทธิ์ในส่วน ของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามนโยบายและแนวปฏิบัติด้านการ รักษาความมั่นคงปลอดภัยสารสนเทศฯ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายและแนว ปฏิบัติด้านเทคโนโลยีสารสนเทศฯ หรือระเบียบ ด้านสารสนเทศอย่างจริงจัง	ผู้ใช้ในหน่วยงาน/ ศูนย์เทคโนโลยีสารสนเทศ	ก.ย. 66

ลำดับ	ความเสี่ยง	ค่า ระดับ ความ เสี่ยง	กลยุทธ์การ จัดการ ความเสี่ยง	แนวทางการดำเนินการ จัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลา การ ปฏิบัติ
2	ความเสี่ยง จากการ นำเอา อุปกรณ์อื่นที่ ไม่ได้รับ อนุญาตมา เชื่อมต่อ	6	ยอมรับ ความเสี่ยง (มีมาตรการ ติดตาม)	- จัดหาเครื่องและอุปกรณ์ ลำรองเพื่อให้สามารถใช้ ทดแทนชั่วคราวเพื่อ สามารถปฏิบัติงานได้ จัดทำ แผนการตรวจสอบ และจัดจ้างบำรุงรักษา เครื่องและ อุปกรณ์อย่าง สม่าเสมอ/ดำเนินการเพิ่ม จุดเชื่อมต่อ สัญญาณ อินเทอร์เน็ตให้ครอบคลุม	ผู้ใช้งาน หน่วยงาน/ ศูนย์เทคโนโลยี สารสนเทศ	ก.ย. 66
3	ความเสี่ยง จาก กระแสไฟฟ้า ขัดข้อง ไฟฟ้า ดับ ไฟกระ ชาก	10	- ยอมรับ ความเสี่ยง (มีมาตรการ ติดตาม)	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้า แบบ ป้องกันปัญหาแรงดันไฟฟ้า ไม่คงที่ - ประสานงานกับฝ่าย อาคาร สถานที่ เพื่อจัดหา ระบบสำรองไฟฟ้าสำหรับ ห้อง Server เพิ่มเติม	ผู้ใช้งาน หน่วยงาน/ ศูนย์เทคโนโลยี สารสนเทศ	ก.ย. 66
4	ความเสี่ยง จากการถูก บุกรุก โดยผู้ ไม่ ประสงค์ ดี/การใช้ โปรแกรม ละเมิด ลิขสิทธิ์	20	- ควบคุม ความเสี่ยง (มีแผน ควบคุม ความ เสี่ยง)	- จัดฝึกอบรมเพื่อสร้างความ ตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความ มั่นคงปลอดภัยสารสนเทศ - ใช้อุปกรณ์เครือข่ายที่ สามารถจำกัดสิทธิ์การเข้าถึง สำหรับอุปกรณ์ที่ไม่ได้รับ อนุญาตให้เชื่อมต่อเข้า เครือข่าย - จัดหาโปรแกรมลิขสิทธิ์ เพื่อใช้ในการปฏิบัติงาน	ผู้ใช้งาน หน่วยงาน/ ศูนย์เทคโนโลยี สารสนเทศ	ก.ย. 66
5	ความเสี่ยง จากการ ขาด ทักษะความ ชำนาญ เฉพาะด้าน ของบุคลากร ผู้ปฏิบัติงาน/ บุคลากร ไม่ เพียงพอ	6	- ยอมรับ ความเสี่ยง (มีมาตรการ ติดตาม)	- จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม - จัดทำคู่มือปฏิบัติงาน เพื่อให้บุคลากรอื่นสามารถ ปฏิบัติตามคู่มือได้กรณีที่ บุคลากรผู้รับผิดชอบไม่ ¹ สามารถมาปฏิบัติงานได้	ผู้ใช้งาน หน่วยงาน/ ศูนย์เทคโนโลยี สารสนเทศ	ก.ย. 66

ลำดับ	ความเสี่ยง	ค่า ระดับ ความ เสี่ยง	กลยุทธ์การ จัดการ ความ เสี่ยง	แนวทางการดำเนินการ จัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลา การ ปฏิบัติ
6	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บังคับบัญชา / เปลี่ยนแปลงผู้บังคับบัญชา	3	ยอมรับความเสี่ยง(มีมาตรการติดตาม)	แต่งตั้งคณะทำงานเทคโนโลยีสารสนเทศตามวาระของที่มีความเสี่ยงที่เปลี่ยนแปลง	ศูนย์เทคโนโลยีสารสนเทศ	ก.ย. 66
7	ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีสมัยใหม่	3	ยอมรับความเสี่ยง(มีมาตรการติดตาม)	จัดทำโครงการเพื่อจัดหาเทคโนโลยีทันสมัยเพื่อสนับสนุนการปฏิบัติงานตามภารกิจและยุทธศาสตร์	ศูนย์เทคโนโลยีสารสนเทศ	ก.ย. 66

แผนบริหารการจัดการความเสี่ยงเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะทำงานบริหารและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อให้เจ้าหน้าที่โรงพยาบาลบ้านผือ ได้ใช้เป็นแนวทางปฏิบัติในการดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อไป



(นายแพทย์ทวิรัช ศรีกุลวงศ์)
 นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)
 รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลบ้านผือ