การบริหารจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

โรงพยาบาลอุทัยธานี

(Uthaithani Hospital IT Risk Management)

ศูนย์คอมพิวเตอร์

โรงพยาบาลอุทัยธานี

ปี2565-2567

คำนำ

โรงพยาบาลอุทัยธานีได้จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2562 ด้วยการวิเคราะห์และประเมิน ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อที่จะบริหารจัดการความเสี่ยงตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) โดยได้วิเคราะห์ความเสี่ยงให้ครอบคลุมและเป็นไปตามข้อกำหนดตามเกณฑ์การพัฒนาคุณภาพการบริหารจัดการภาครัฐ ซึ่งสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

แผนบริหารจัดการความเสี่ยงดังกล่าว จะใช้เป็นกรอบและแนวทางานในการปฏิบัติงาน ของหน่วยงานต่างๆ ที่เกี่ยวข้อง ตลอดจนการกากับดูแลการใช้งานด้านเทคโนโลยีสารสนเทศของโรงพยาบาลอุทัยธานีเพื่อให้เทคโนโลยีสารสนเทศสามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและมีความมั่นคงปลอดภัยสูงสุด

ทั้งนี้จะมีการตรวจสอบและประเมินความเสี่ยงที่มีแนวโน้มอาจจะเกิดขึ้น เพื่อบริหารจัดการได้อย่างถูกต้อง ไม่เกิดเหตุการณ์ความเสียหาย และทำการทบทวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ศูนย์คอมพิวเตอร์
โรงพยาบาลอุทัยธานี
ปี2565-2567

สารบัญ

สารบัญ Flowchart

บทที่ 1

บทนำ

หลักการและเหตุผล

โรงพยาบาลอุทัยธานีได้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานของโรงพยาบาลอุทัยธานีในหลายด้าน ดังนั้นจึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชนสูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น

แผนบริหารจัดการความเสี่ยง มีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบ และประเมิน ความเสี่ยงด้านสารสนเทศของโรงพยาบาลอุทัยธานี ด้วยการคาดการณลวงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการการบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี ที่จะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสม มีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแกองค์กรภายใตสภาวะการดำเนินงานของทุกองค์กรล้วนแต่มีความเสี่ยง ซึ่งเป็นความไมแน่นอนที่อาจจะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร

จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบโดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงาน หรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของความเสี่ยง กำหนดแนวทางในการจัดการความเสี่ยง และต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอยางเหมาะสม แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อเป็นแนวทำงานที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศด้วยการคาดการณลวงหนา ในกรณีที่ความเสี่ยงเกิดขึ้นจริง และสามารถนำแนวทำงานจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการได้

วัตถุประสงค์ของแผนบริหารความเสี่ยง

1) เพื่อให้ผู้บริหารและผูปฏิบัติงาน เข้าใจหลักการ และกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2) เพื่อให้การจัดการภายในกลุ่มงานสารสนเทศทางการแพทย์ข้อมูลมีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไมตองการกับระบบเทคโนโลยีสารสนเทศ

3) เพื่อให้ผู้ปฏิบัติงานไดรับทราบขั้นตอน และกระบวนการในการวางแผนบริหารความเสี่ยง

4) เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอยางเป็นระบบและต่อเนื่อง

5) เพื่อลดโอกาสและผลกระทบของความเสี่ยงที่จะเกิดขึ้นกับองค์กรการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลอุทัยธานี 2565

6) เพื่อเป็นแนวทำงานการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร ความรูความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในโรงพยาบาลอุทัยธานี

7) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทำงานในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

เป้าหมาย

1) ผู้บริหารและผูปฏิบัติงาน มีความรูความเข้าใจเรื่องการบริหารความเสี่ยง เพื่อนำไปใช้ในการดำเนินงานตามยุทธศาสตร์และแผนปฏิบัติงานประจำปีให้บรรลุตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

2) ผู้บริหารและผูปฏิบัติงาน สามารถระบุความเสี่ยง วิเคราะห์ความเสี่ยง ประเมินความเสี่ยง และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3) สามารถนำแผนบริหารความเสี่ยงไปใช้ในการบริหารงานที่รับผิดชอบ

4) เพื่อพัฒนาความสามารถของบุคลากรและกระบวนการดำเนินงานภายในองค์กรอย่างต่อเนื่อง

5) ความรับผิดชอบต่อความเสี่ยงและการบริหารความเสี่ยงถูกกำหนดขึ้นอย่างเหมาะสมทั่วทั้งองค์กร

6) การบริหารความเสี่ยงไดรับการปลูกฝังให้เป็นวัฒนธรรมขององค์กร

ประโยชนของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจไดดียิ่งขึ้นและทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดไดในสถานการณที่ไมคาดคิด หรือสถานการณที่อาจทำให้องค์กรเกิดความเสียหาย ประโยชนที่คาดหวังว่าจะไดรับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

1) เป็นส่วนหนึ่งของหลักการบริหารกิจการที่ดี การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผูบริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญและสามารถทำหนาที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

2) สรางฐานข้อมูลที่มีประโยชนต่อการบริหารและการปฏิบัติงานในองค์กร การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ ซึ่งรวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานในการตอบสนองต่อเป้าหมาย และภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

3) ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญไดทั้งหมด การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลอุทัยธานี

4) เป็นเครื่องมือที่สำคัญในการบริหารงาน การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงไดรับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของโรงพยาบาลอุทัยธานีเป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชนรวมทั้งเพิ่มมูลค่าแก่องค์กร

5) ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจในกลยุทธ์วัตถุประสงค์ขององค์กร และระดับความเสี่ยงอยางชัดเจน

6) ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผลการจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสาหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูงย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

นิยามความเสี่ยง

ความเสี่ยง (Risk)

ความเสี่ยง หมายถึง เหตุการณหรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณที่ไมแน่นอน และจะส่งผลกระทบหรือสรางความเสียหาย (ทั้งที่เป็นตัวเงินและไมเป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และ การบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด(Likelihood) ของเหตุการณ

ลักษณะของความเสี่ยง สามารถแบงออกได้เป็น 3 สวน ดังนี้

1) ปัจจัยเสี่ยง คือ สาเหตุที่จะทำให้เกิดความเสี่ยง

2) เหตุการณเสี่ยง คือ เหตุการณที่ส่งผลกระทบต่อการดำเนินงาน หรือ นโยบาย

3) ผลกระทบของความเสี่ยง คือ ความรุนแรงของความเสียหายที่น่าจะเกิดขึ้นจากเหตุการณเสี่ยง

การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแลว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบงออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยง หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณความเสี่ยงลดลงอยู่ในระดับ ที่องค์กรยอมรับได้ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทำงานหลัก คือ การยอมรับ การลด/ควบคุมการยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยงการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศโรงพยาบาลอุทัยธานี

การควบคุม (Control)

การควบคุม หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์แบ่งได้4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะและการควบคุมเพื่อการแกไข

ทรัพย์สิน (Asset)

ทรัพย์สิน หมายถึง ทรัพย์สินต่างๆ ขององค์กรแบ่งเป็น 4 หมวด ไดแก หมวดข้อมูล หมวดบุคลากร หมวดฮาร์ดแวร์และหมวดซอฟต์แวร์

หลักการวิเคราะห์ประเมิน และจัดทาความเสี่ยงอย่างเหมาะสม

ตามกระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Tread way Commission) มีดังนี้

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุความเสี่ยงต่างๆ (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7. การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

บทที่ 2
แนวทางการบริหารความเสี่ยง

แนวทางดำเนินงานและกลไกการบริหารความเสี่ยง

แนวทางดำเนินงาน ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลอุทัยธานี แบ่งเป็น 2 ระยะ ดังนี้

ระยะที่ 1 การเริ่มต้นและพัฒนา

1) กำหนดนโยบายหรือแนวทางในการบริหารจัดการความเสี่ยง

2) ระบุปัจจัยเสี่ยง และประเมินโอกาส ผลกระทบจากปัจจัยเสี่ยง

3) วิเคราะห์และจัดลาดับความสำคัญของปัจจัยเสี่ยงจากการดำเนินงาน

4) จัดทำแผนบริหารความเสี่ยงของปัจจัยเสี่ยงที่อยู่ในระดับสูง (High) และสูงมาก (Extreme)รวมทั้งปัจจัยเสี่ยงที่อยู่ในระดับปานกลาง (Medium) ที่มีนัยสำคัญ

5) สื่อสารทำความเข้าใจเกี่ยวกับแผนบริหารความเสี่ยงให้ผู้ปฏิบัติงานของกลุ่มงานเทคโนโลยีสารสนเทศรับทราบ และสามารถนาไปปฏิบัติได้

6) รายงานความก้าวหนาของการดำเนินงานตามแผนบริหารความเสี่ยง

7) รายงานสรุปการประเมินผลความสำเร็จของการดำเนินการตามแผนบริหารความเสี่ยง

ระยะที่ 2 การพัฒนาสูความยั่งยืน

1) ทบทวนแผนบริหารความเสี่ยง

2) พัฒนากระบวนการบริหารความเสี่ยงสาหรับความเสี่ยงแต่ละประเภท

3) ผลักดันให้มีการบริหารความเสี่ยงทั่วทั้งองค์กร

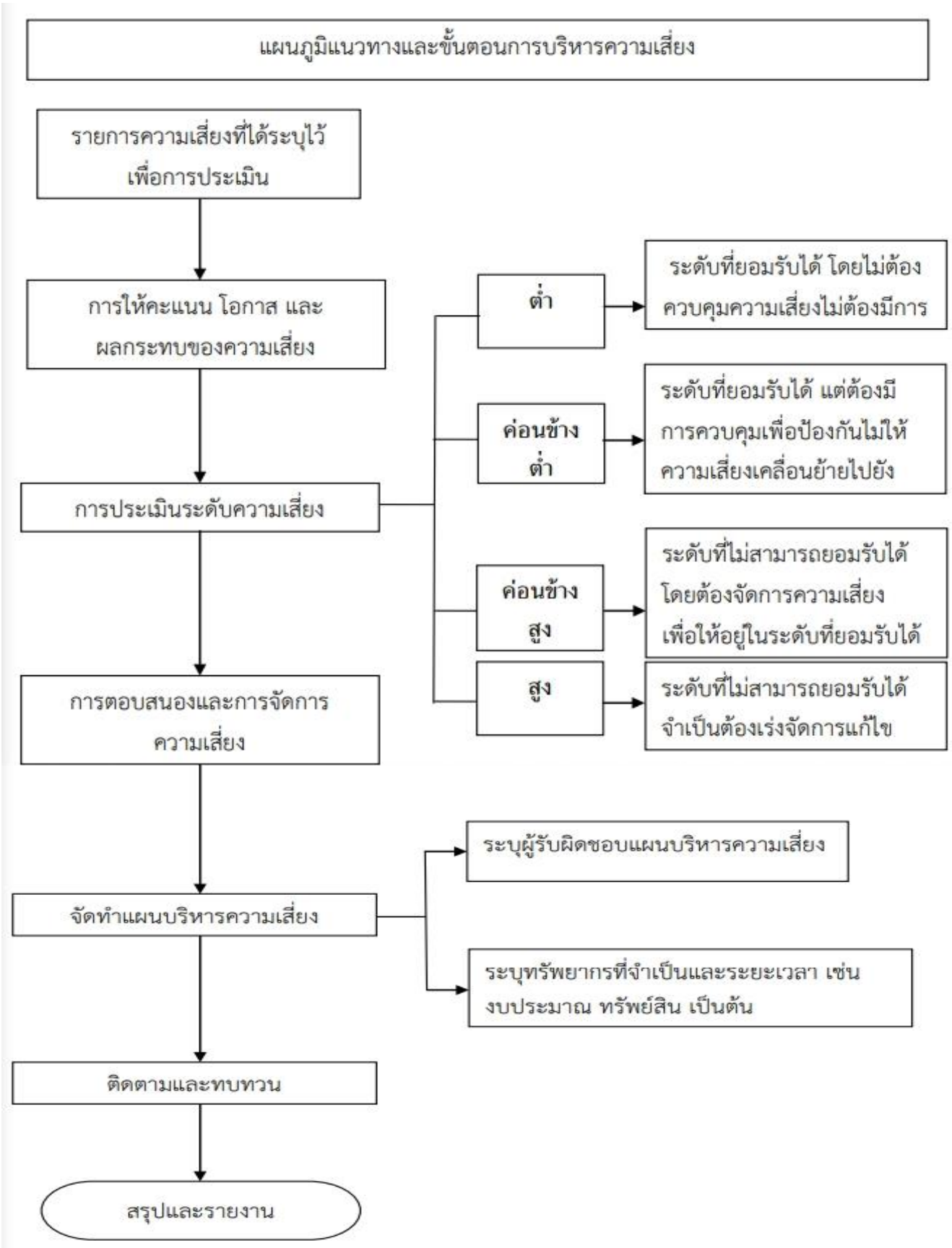
4) พัฒนาขีดความสามารถบุคลากรในการดำเนินงานตามกระบวนการบริหารความเสี่ยง

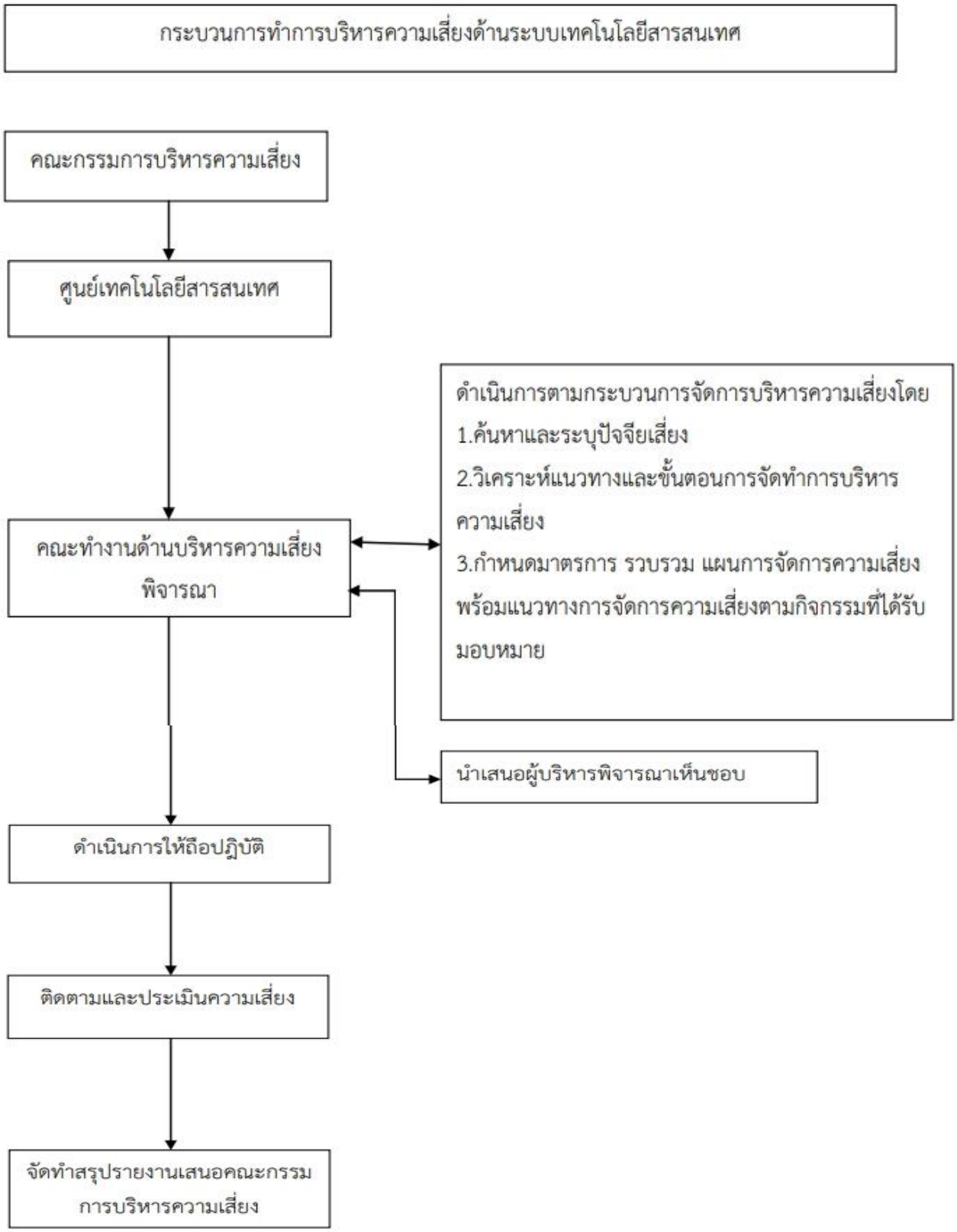
กลไกการบริหารความเสี่ยง ประกอบด้วย

1) ผู้อำนวยการ มีหนาที่แต่งตั้งคณะทำงานบริหารความเสี่ยง ส่งเสริมให้มีการบริหารจัดการความเสี่ยงอยางมีประสิทธิภาพและเหมาะสม รวมทั้งพิจารณาให้ความเห็นชอบหรืออนุมัติแผนการบริหารความเสี่ยงเพื่อนำไปปฏิบัติต่อไป (คณะกรรมการชุด HIMS)

2) คณะทำงานบริหารความเสี่ยง มีหนาที่ดำเนินการให้มีระบบการบริหารความเสี่ยง จัดทำแผนบริหารความเสี่ยง รายงานและประเมินผลการดำเนินงานตามแผนการบริหารความเสี่ยงรวมทั้งทบทวนแผนการบริหารความเสี่ยงเพื่อปรับปรุงการดำเนินงานต่อไปในอนาคต (คณะกรรมการชุด HIMS)

3) ผู้ปฏิบัติงาน บุคลากรที่มีหนาที่สนับสนุนข้อมูลที่เกี่ยวข้องให้กับคณะทำงานบริหารความเสี่ยง และให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยง


แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง
รายการความเสี่ยงที่ได้ระบุไว้เพื่อการประเมิน
การให้คะแนน โอกาส และผลกระทบของความเสี่ยง
การประเมินระดับความเสี่ยง
ต่ำ
ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงไม่ต้องมีการ
ค่อนข้างต่ำ
ระดับที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยัง
ค่อนข้างสูง
ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้
สูง
ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการแก้ไข
การตอบสนองและการจัดการความเสี่ยง
จัดทำแผนบริหารความเสี่ยง
ระบุผู้รับผิดชอบแผนบริหารความเสี่ยง
ระบุทรัพยากรที่จำเป็นและระยะเวลา เช่น งบประมาณ ทรัพย์สิน เป็นต้น
ติดตามและทบทวน
สรุปและรายงาน


กระบวนการทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
คณะกรรมการบริหารความเสี่ยง
ศูนย์เทคโนโลยีสารสนเทศ
คณะทำงานด้านบริหารความเสี่ยง พิจารณา
ดำเนินการตามกระบวนการจัดการบริหารความเสี่ยงโดย
1.ค้นหาและระบุปัจจัยเสี่ยง
2.วิเคราะห์แนวทางและขั้นตอนการจัดทำการบริหารความเสี่ยง
3.กำหนดมาตรการ รวบรวม แผนการจัดการความเสี่ยง พร้อมแนวทางการจัดการความเสี่ยงตามกิจกรรมที่ได้รับมอบหมาย
นำเสนอผู้บริหารพิจารณาเห็นชอบ
ดำเนินการให้ถือปฏิบัติ
ติดตามและประเมินความเสี่ยง
จัดทำสรุปรายงานเสนอคณะกรรมการบริหารความเสี่ยง

บทที่3
การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศในโรงพยาบาล
Hospital IT Risk Management

นิยามระบบสารสนเทศ

คือระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบสารสนเทศ

โครงสร้างขององค์กรระบบสารสนเทศจะทำหนาที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆ ขององค์กรบุคลากรที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์ อาจใช้เทคโนโลยีเป็นอุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศเพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

1. Hardware หมายถึงอุปกรณ์ต่างๆ ที่กระทำกับข้อมูลเอกสารทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์
2. Software หมายถึงชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน
3. บุคลากร หมายถึงกลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศคือเป็นผู้นำจัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์
4. ข้อมูลและแฟ้มข้อมูล หมายถึงข้อมูลและสารสนเทศที่ระบบจัดเก็บไวในช่วงเวลาหนึ่ง
5. หนาที่การปฏิบัติงาน หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

คือเหตุการณหรือการกระทำใดๆ ที่อาจเกิดขึ้นภายในสถานการณที่ไมแน่นอน และจะส่งผลกระทบหรือสรางความเสียหาย หรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

1. เพื่อเตรียมความพรอมรองรับสถานการณฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลอุทัยธานี
2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพรอมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแกไขสถานการณไดอย่างทันท่วงทีกรณีเกิดสถานการณความไมแน่นอนและภัยพิบัติ

สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software)

ระบบฐานข้อมูลบริหารงานภายใน (Back Office) ไดแกฐานข้อมูลกลาง (Files Center) ฐานข้อมูลระบบบัญชี (Winspeed) ฐานข้อมูลระบบแจ้งซ่อม ฐานข้อมูลระบบเวชภัณฑ์

ระบบให้บริการเครือข่าย ไดแก โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์ภายในโรงพยาบาลอุทัยธานี (Web Application Program) เป็นต้น

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์(Web Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบ (IPD Paperless) อุปกรณ์ป้องกันการจูโจมข้อมูลจากบุคคลภายนอก (Firewall)

กระบวนการบริหารจัดการความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุวิเคราะห์ประเมินจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กรรวมทั้งการบริหาร/จัดการความเสี่ยงรวมทั้งการกำหนดแนวทาง การดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยงซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสมและครอบคลุม

ความหมาย และ ความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณหรือการกระทำใดๆที่อาจจะเกิดขึ้นภายในสถานการณที่ไม่แน่นอนและจะส่งผลกระทบหรือสรางความเสียหาย (ทั้งที่เป็นตัวเงินและไมเป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กรทั้งในด้านยุทธศาสตร์การปฏิบัติงานการเงินและการบริการซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ไดโดยวัดจากผลกระทบ (Impact) ที่ไดรับและความเป็นไปไดที่จะเกิด (Likelihood) ของเหตุการณ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไมบรรลุวัตถุประสงค์ที่กำหนดไวโดยต้องระบุไดด้วยว่าเหตุการณนั้นจะเกิดที่ไหน เมื่อใด เกิดขึ้นไดอย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะไดวิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังไดอย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยงการวิเคราะห์ความเสี่ยงและจัดลำดับความเสี่ยงโดยการประเมินจากโอกาสความเป็นไปได้ที่จะเกิด (Likelihood) และผลกระทบ(Impact) เมื่อทำการประเมินแล้วทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึงสถานะของความเสี่ยงที่ไดจากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบงออกเป็น 5 ระดับคือ สูงมาก ค่อนข้างสูง ปานกลาง น้อย และน้อยมาก

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได ซึ่งการจัดการความเสี่ยงอาจแบ่งโดยสรุปไดเป็น 4 แนวทางหลักคือการยอมรับการลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบายแนวทางหรือขั้นตอนปฏิบัติตางๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์แบ่งได้ 4 ประเภทคือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแกไขหลักการวิเคราะห์ประเมินและจัดทำความเสี่ยงอยางเหมาะสมตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุความเสี่ยงต่างๆ (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication

การจัดการความเสี่ยง

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ กระบวนการการทำงานที่ช่วยให้ IT Managers สามารถสรางความสมดุลของต้นทุนเชิงเศรษฐศาสตร์การดำเนินธุรกิจระหวางมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

ปัจจัยเสี่ยง

1.จุดอ่อน หรือ ชองโหว (Vulnerabilities) หรือ ปัจจัยภายใน

2. ภัยคุกคาม (Threats) หรือปัจจัยภายนอก

1.จุดอ่อน หรือ ชองโหว (Vulnerabilities) หรือ ปัจจัยภายใน

1.1.บุคลากร

1.1.1 บุคลากรภายใน ไมปฏิบัติหนาที่ หรือทำหนาที่ผิดพลาด

1.1.2 บุคลากรภายนอก ไมตรวจสอบข้อมูลก่อนการบันทึกและไมรอบคอบในการสแกนไวรัส

1.2.เครื่องแม่ข่ายและอุปกรณ์ (Hardware & Accessory)

1.3.โปรแกรม (software)

1.4.การเชื่อมโยงเครือข่าย (Network & Communicate)

1.5.ระบบงานและข้อมูล (System & Information)

2. ภัยคุกคาม (Threats) หรือปัจจัยภายนอก

2.1 Virus

2.2.ระบบไฟฟ้า

2.3.เครื่องสำรองไฟฟ้า

2.4.ระบบปรับอากาศ

2.5.ภัยธรรมชาติ

จุดอ่อน หรือ ชองโหว (Vulnerabilities) หรือ ปัจจัยภายใน

1.ความเสี่ยงด้านบุคลากร

ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสานสนเทศของโรงพยาบาล รวมถึงการวางแผนการตรวจสอบการทำงานการมอบหมายหนาที่และสิทธิของบุคลากร / คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรูความเข้าใจในการใช้งาน การดูและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ตลอดจนบุคลากรภายนอกทีเกี่ยวข้องทั้งทางตรงและทางออมล้วนแต่เป็นความเสี่ยง ความเสี่ยงด้านบุคลากรเป็นความเสี่ยงหนึ่งที่สำคัญ ดังนั้นจึงควรมีแนวทางและการวางแผนที่กำกับดูแลการบริหารจัดการและควบคุมความเสี่ยงอยางจริงจังการบริหารจัดการความเสี่ยงด้านบุคลากรมีประเด็นหลัก ดังนี้

1.1 กำหนดโครงสรางบุคลากรด้านเทคโนโลยีสารสนเทศของโรงพยาบาลอุทัยธานี และการบริหารจัดการด้านบุคลากร

การแต่งตั้งเจาหนาที่ฯ ที่มีความเหมาะสม (มีความรูความสามารถและประสบการณด้านคอมพิวเตอร์ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีด้านการรักษาความปลอดภัยระบบฯ และสามารถถ่ายทอดความรูนั้นให้แกผู้ใช้งานระบบฯของหน่วยงานไดอย่างมีประสิทธิภาพ) เมื่อมีการปรับและแจ้งรายชื่อผู้รับผิดชอบ

เจาหนาที่ที่รักษาความปลอดภัยระบบฯ และผูดูแลระบบฯ ที่มีการเปลี่ยนแปลง เช่น โยกย้าย ลาออก ฯลฯ จะต้องแจ้งให้แกผู้บังคับบัญชาไดรับทราบเพื่อประโยชนในการบริหารบุคลากรการติดต่อประสานการฝกอบรมและการรักษาความปลอดภัยระบบสารสนเทศอย่างมีประสิทธิภาพ

บุคลากรด้านเทคโนโลยีสารสนเทศ ไมมีการจัดโครงสรางและการบริหารจัดการที่ดีเพียงพอทำให้เกิดความเสี่ยงด้านโครงสรางการบริหารงานไดการกำหนดโครงสรางการแบ่งอำนาจหนาที่การกำหนดนโยบายและขั้นตอนการปฏิบัติงานและกำกับดูแลควบคุมการปฏิบัติงานเป็นหลัก

1.2.บุคลากรขาดความรูความเข้าใจเรื่องของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรมและนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้โดยการส่งเจ้าหนาที่เข้ารับการอบรมความรูทางเทคโนโลยีสารสนเทศรวมถึงการรับบุคลากรที่มีความรูความเข้าใจด้านระบบเทคโนโลยีสารสนเทศมาปฏิบัติงานในหน่วยงานราชการมากยิ่งขึ้น

2.เครื่องแม่ข่ายและอุปกรณ์คอมพิวเตอร์

หองคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารหลัก (Server Room & Network Equipment) ที่จะเป็นที่จัดเก็บและติดตั้งระบบเทคโนโลยีสารสนเทศไวยังเครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และการกำหนดที่ตั้งระบบเทคโนโลยีสารสนเทศไวยังเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้าสายวงจรสายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไมตั้งระบบไวในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ ,ตู Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย, ระบบความความชื้น, ถังดับเพลิง , การควบคุมการเขาออกห้อง ควบคุมระบบคอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) โดยมีการจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงระบบสัญญาณเครือข่ายที่เชื่อมโยงไวในห้องควบคุมระบบคอมพิวเตอร์ (Server Room) ของโรงพยาบาลอุทัยธานี

การเขาออกห้องควบคุมระบบคอมพิวเตอร์ ซึ่งเป็นบุคคลที่มีหนาที่เกี่ยวข้องประจำห้องควบคุมระบบคอมพิวเตอร์ หรือ ผู้ที่ไมมีหนาที่เกี่ยวข้อง มีความจำเป็นเข้าออกเป็นบางกรณีจำเป็นต้องมีการควบคุมอย่างรัดกุม และรอบคอบ เช่น กำหนดให้เจาหนาที่ผู้รับผิดชอบควบคุมดูแลการทำงานตลอดเวลา ผู้ที่ไมมีหนาที่เกี่ยวข้องมีความจำเป็นต้องเข่าหองควบคุมจะต้องมีการแจ้งให้ศูนย์คอมพิวเตอร์ทราบก่อนทุกครั้งและมีการบันทึกไว้ในระบบ ถ้าเป็นบุคคลภายนอกต้องมีหนังสือแจ้งล่วงหน้าเสนอผู้อำนวยการโรงพยาบาลรับทราบทุกครั้ง

การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม มีระบบตรวจจับควันไฟ จัดให้มีถังดับเพลิงที่พรอมใช้งานไดตลอดเวลากรณีฉุกเฉิน เพื่อใช้ในการดับเพลิงเบื้องต้น มีการป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าลัดวงจร ทำไดโดยมีระบบป้องกันไฟฟ้ากระชากไมให้คอมพิวเตอร์แม่ข่ายให้รับความเสียหายจากความไมคงที่ของกระแสไฟฟ้า อีกทั้งการติดตั้งระบบสายดิน (Ground) ที่ไดมาตรฐาน ระบบไฟฟ้าสำรองสำหรับคอมพิวเตอร์ทั้งแม่ข่ายและลูกข่าย เพื่อให้การดำเนินงานมีความต่อเนื่องสามารถใช้งานได้

3.ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

ความเสี่ยงที่เกิดจากระบบงานของโปรแกรม ที่ไดจัดทำและพัฒนาขึ้นสำหรับโครงการด้านต่างๆ รวมถึงโปรแกรมประยุกต์อื่นๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่างเช่น การใช้โปรแกรมที่ไมมีลิขสิทธิ์ ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแกไขเปลี่ยนแปลงคำสั่ง และการถูกผู้ไมหวังดีทำลายระบบ (Hacker) รวมถึงความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไมมีการอัพเดทให้ทันสมัย เพื่อลดช่องโหวที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ

4. ความเสี่ยงด้านการเชื่อมโยงระบบเครือข่าย

ความเสี่ยงหรือภัยต่างๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเตอรเน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโปรโตคอล (Protocol) TCP/IP เช่น ความเสี่ยงด้านกายภาพ ,ความเสี่ยงด้านระบบปฏิบัติการ ,ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ ความเสียหายที่เกิดขึ้นจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่ายและการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่าย ไดมีระบบการติดตามและเฝ้าดูแลการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน รวมทั้งการกำหนด Policy เพื่อป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูล ระบบ Web server

5.System & information

ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกการโจรกรรมข้อมูลสำคัญ การลักลอบเข้ามาแกไขเปลี่ยนแปลงข้อมูล ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล การรักษาความมั่นคงปลอดภัยของข้อมูลจึงเป็นเรื่องที่สำคัญ ข้อมูลสารสนเทศเป็นส่วนสำคัญสำหรับผู้บริหารเพื่อนำข้อมูลมาประกอบการตัดสินใจ ในการวางแผนการจัดการข้อมูล (Management of Data and Communication) การรักษาความปลอดภัยของระบบข้อมูลและ Computer จากภัยต่างๆทั้งจากคนจากธรรมชาติหรือเหตุการณใดๆ จึงสำคัญและจำเป็นเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

ภัยคุกคาม (Threats) หรือปัจจัยภายนอก

1. Virus

โรงพยาบาลอุทัยธานีไดมีการจัดซื้ออุปกรณ์ Filewall ที่มีขนาดเหมาะสมกับองค์กร และมีการต่อ License ทุกปี โดยระบบของ Filewall มีระบบการสแกนไวรัสมาให้ สามารถสแกนและจัดการ block ตลอดการเข้าออก Internet ของเครื่องที่ใช้งาน และเตรียมทำแผนจัดซื้อโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) เพื่อเสริมการทำหนาที่ติดตามเฝ้าระวังระบบการทำงานของคอมพิวเตอร์การเข้าใช้ระบบตรวจจับปองกัน และลบไฟล์ที่พึงระวังไวรัสและโปรแกรมไมพึงประสงค์ปรับปรุงกำหนดค่าระบบความปลอดภัยให้เหมาะสมกับปัญหาอัพเดท และการป้องกันไวรัสจากอุปกรณ์เชื่อมต่อต่างๆ เช่น USB Drive

2.ระบบไฟสำรองของห้องควบคุมระบบคอมพิวเตอร์ /เครื่องสำรองไฟฟ้า

มีแผนดำเนินการเชื่อมต่อระบบไฟผ่านเครื่องสำรองไฟ ขนาด 10KVA 3เฟส มีความเหมาะสมกับห้องควบคุมระบบคอมพิวเตอร์ และเชื่อมต่อระบบสำรองไฟผ่านระบบไฟฟ้าสำรองของอาคาร (เครื่องปั่นไฟฉุกเฉิน) เครื่องแม่ข่าย Server แต่ละชุด ทำการต่อระบบสำรองไฟทั้ง2แบบ เพื่อความเหมาะสมของระบบสำรองไฟตลอด 24 ชม.เพื่อให้ระบบไฟฟ้าสำรองทำงานได้อย่างมีประสิทธิภาพ ผู้ดูแลระบบ ตรวจสอบการทำงานของเครื่องสำรองไฟภายในห้อง Server ทุกวันในช่วงเวรบ่าย (16.00 -24.00 น) และติดตามตรวจสอบระบบไฟฉุกเฉิน โดยทำงานร่วมกับช่างไฟฟ้าของโรงพยาบาล

3.ระบบปรับอากาศ

ห้อง Server มีเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ทำงานตลอดเวลา ซึ่งจะมีการระบายความร้อนออกมาทำให้มีความร้อนสะสมมาก ถ้ามีความร้อนมากเกินไปเครื่องก็อาจจะพังเสียหายได้

จึงมีการติดตั้งเครื่องปรับอากาศในห้อง Server จำนวน 3 เครื่อง มีระบบสลับการทำงานอัตโนมัติ มีระบบควบคุมความชื้นและควบคุมความเย็น โดยอุณหภูมิจะไม่เกิน 25c และความชื้นไม่เกิน 80% ซึ่งถ้าเกินกว่ากำหนดจะมีการแจ้งเตือนไปยังเจ้าหน้าที่ศูนย์คอมพิวเตอร์เพื่อมาตรวจสอบทันที

4. ภัยธรรมชาติ

ไฟไหมหอง Server

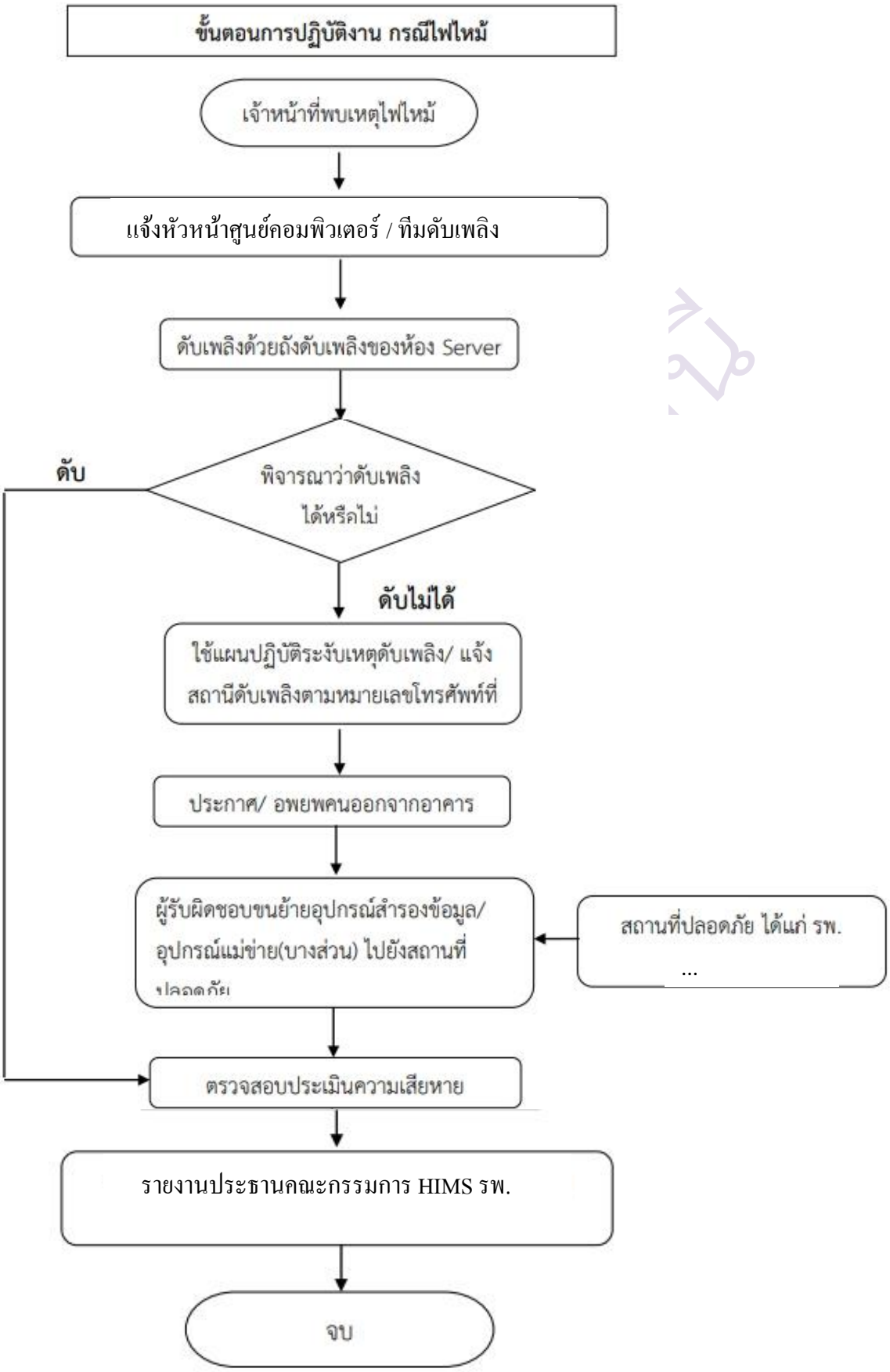
เกิดความเสียหายกับทรัพย์สินระบบเครือข่ายอุปกรณ์และฐานข้อมูลถูกทำลายทั้งหมดการดำเนินงานหยุดชะงัก หยุดระบบประมวลผลทั้งระบบลง ผู้ปฏิบัติงานและผูรับบริการไมสามารถใช้งานระบบได

ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

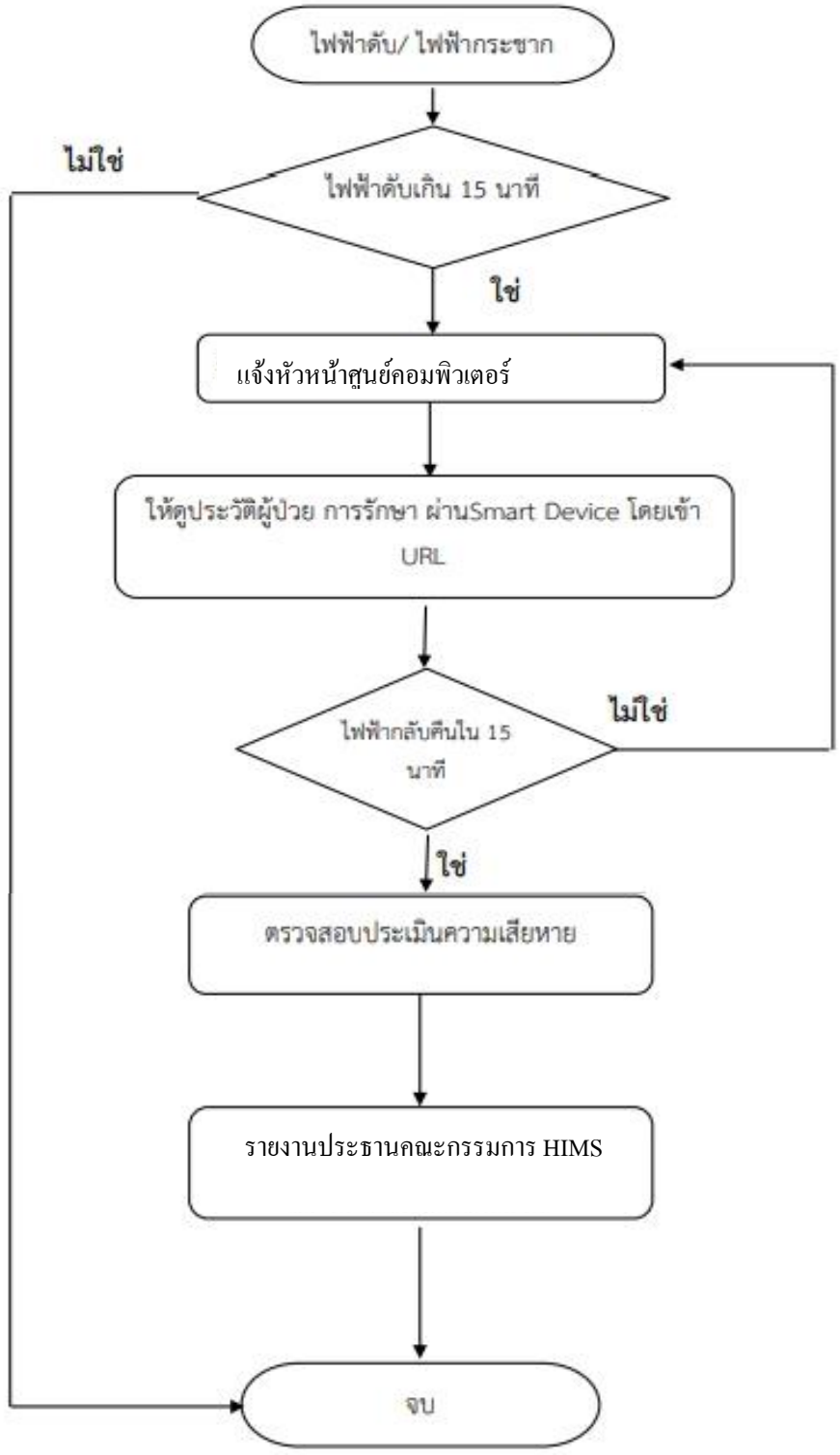
ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการไดเครื่องคอมพิวเตอร์ไมสามารถทำงานไดชั่วคราว ผู้ใช้งาน (User) ไมสามารถเข้ามาใช้งานในระบบไดทั้งหมด ทำความเสียหายระยะยาวให้แกอุปกรณ์คอมพิวเตอร์และเมื่อมีกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับบ่อยครั้ง ส่งผลให้เกิดความเสียหายที่ถาวรแกอุปกรณ์เครื่องคอมพิวเตอร์ได

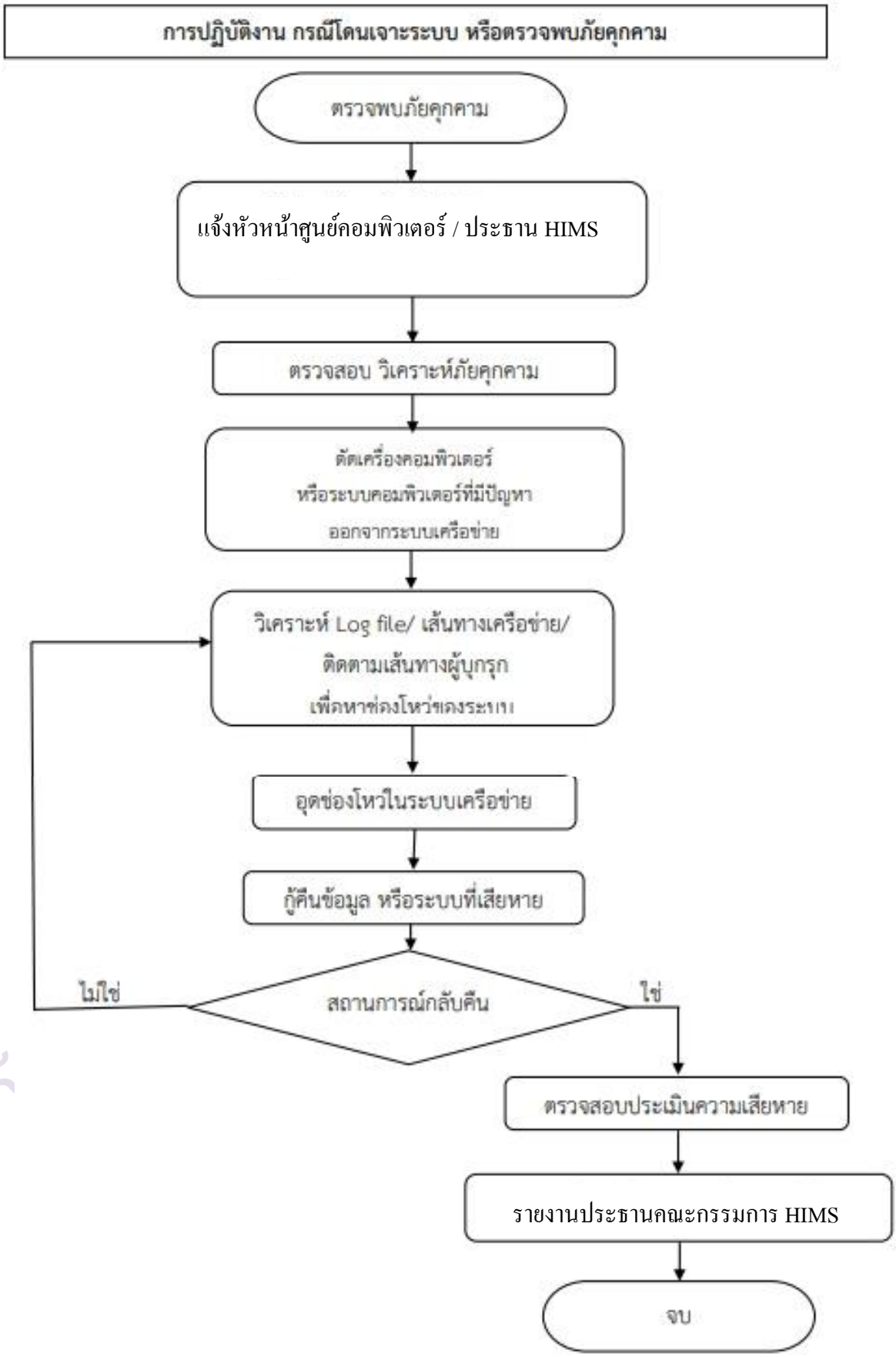
การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server

ถ้าบุคคลที่ไมมีอำนาจหนาที่เกี่ยวข้องไดลวงรูข้อมูล และอาจนำไปแสวงหาประโยชนโดยมิชอบได้ข้อมูลและการทำงานของระบบคอมพิวเตอร์ถูกแกไขเปลี่ยนแปลงทำลาย หรืออาจกระทำการแกไขสิทธิแกบุคคลที่มีหนาที่รับผิดชอบให้ไมสามารถเข้าถึงข้อมูล และระบบคอมพิวเตอร์ไดส่งผลให้ไมสามารถปฏิบัติงานได ระบบขาดความน่าเชื่อถือและไมมีประสิทธิภาพ


ขั้นตอนการปฏิบัติงาน กรณีไฟไหม้
เจ้าหน้าที่พบเหตุไฟไหม้
แจ้งหัวหน้าศูนย์คอมพิวเตอร์ / ทีมดับเพลิง
ดับเพลิงด้วยถังดับเพลิงของห้อง Server
พิจารณาว่าดับเพลิง ได้หรือไม่
ดับ
ดับไม่ได้
ใช้แผนปฏิบัติระงับเหตุดับเพลิง/ แจ้งสถานีดับเพลิงตามหมายเลขโทรศัพท์ที่
ประกาศ/ อพยพคนออกจากอาคาร
ผู้รับผิดชอบขนย้ายอุปกรณ์สำรองข้อมูล/ อุปกรณ์แม่ข่าย(บางส่วน) ไปยังสถานที่ปลอดภัย
สถานที่ปลอดภัย ได้แก่ รพ. ...
ตรวจสอบประเมินความเสียหาย
รายงานประธานคณะกรรมการ HIMS รพ.
จบ

ขั้นตอนการปฏิบัติงาน กรณีไฟฟ้าดับ/ ไฟฟ้ากระชาก/ หม้อไฟระเบิด




การปฏิบัติงาน กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม
ตรวจพบภัยคุกคาม
แจ้งหัวหน้าศูนย์คอมพิวเตอร์ / ประธาน HIMS
ตรวจสอบ วิเคราะห์ภัยคุกคาม
ตัดเครื่องคอมพิวเตอร์
หรือระบบคอมพิวเตอร์ที่มีปัญหา
ออกจากระบบเครือข่าย
วิเคราะห์ Log file/ เส้นทางเครือข่าย/
ติดตามเส้นทางผู้บุกรุก
เพื่อหาช่องโหว่ของระบบ
อุดช่องโหว่ในระบบเครือข่าย
กู้คืนข้อมูล หรือระบบที่เสียหาย
สถานการณ์กลับคืน
ไม่ใช่
ใช่
ตรวจสอบประเมินความเสียหาย
รายงานประธานคณะกรรมการ HIMS
จบ

มาตรฐานความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical Security)

1.ระบบงานตรวจสภาพเบื้องต้นของเครื่องตรวจ แสดงผล และเตือนภัยภายในห้องควบคุม (Environment monitoring & Tele alarm)

เพื่อให้การป้องกันความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical Security) เป็นไปอย่างมีคุณภาพ ผู้ดูแลระบบไดเพิ่มช่องทางในการแสดงผล สถานะภาพในห้อง เพื่อที่จะสามารถทราบถึงอุณหภูมิ ความชื้น และระบบไฟฟ้าเป็นต้น มีการติดตั้งระบบแจ้งเตือนภายในห้อง Server เพื่อแสดงสถานะภายในห้อง หากพบความผิดปกติ โดยมีค่าอุณหภูมิเกิน 25 องศาเซลเซียส หรือพบความชื่นเกิน 80% ระบบการสง message ไปยังผู้ดูแลระบบ ไดแบบ Realtime ผ่านระบบ Line

2.ระบบวงจรปิด CCTV

ผู้ดูแลระบบไดติดตั้งระบบกล่องวงจรปิดเพื่อบันทึกเหตุการณภายในห้องควบคุมระบบคอมพิวเตอร์และมีการบันทึกภาพแบบตรวจจับความต่อเนื่อง ตลอด24ชม. จำนวน 2 กลองสามารถบันทึก และดูภาพย้อนหลังได 1 เดือนสามารถดูภาพผ่านระบบ Internet ไดตลอด 24ชม.

การประมาณความเสี่ยง (Risk Estimation)

เป็นการดูปัญหาความเสี่ยงในแงของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใดเกณฑ์การประมาณเป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ไดแกระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยงใช้เกณฑ์ดังนี้(แนวทางพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศ)

ระดับโอกาสในการเกิดเหตุการณตางๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	5 ครั้ง / ป
4	สูง	4 ครั้ง / ป
3	ปานกลาง	3 ครั้ง / ปี
2	น้อย	2 ครั้ง / ป
1	น้อยมาก	ไมเกิน 1 ครั้ง / ป

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	ค่อนข้างสูง	เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

การประเมินความเสี่ยง (Risk Assessment)

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของโรงพยาบาลอุทัยธานี สามารถแยกประเภทความเสี่ยงเป็น 4 ประเภทดังนี้

1.ความเสี่ยงด้านเทคนิคเป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือ และอุปกรณ์เองอาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่พึงประสงค์ ถูกกอกวนจาก Hacker

2.ความเสี่ยงจากผู้ปฏิบัติงานเป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งาน หรือการให้บริการโดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหนาที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได

3.ความเสี่ยงจากภัยหรือสถานการณฉุกเฉินเป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม อาคารถล่ม การชุมนุมประท้วง หรือความไมสงบเรียบร้อยในบ้านเมือง เป็นต้น

4.ความเสี่ยงด้านการบริหารจัดการเป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจสงผลกระทบต่อการดำเนินการด้านสารสนเทศ

การจัดระดับความเสี่ยง

ประกอบด้วย 4 ขั้นตอนคือ

1 การกำหนดเกณฑ์การประเมินมาตรฐานเป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง โอกาสหรือความเป็นไปไดที่จะเกิดความเสี่ยง(Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง(Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้นซึ่งอาจกำหนดไดทั้งเกณฑ์เชิญปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุดสูงสูง/ค่อนข้างรุนแรงปานกลางน้อยและน้อยมาก) สวนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก ค่อนข้างสูง ปานกลาง น้อย และน้อยมาก)

2 การประเมินโอกาสและผลกระทบของความเสี่ยงเป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไวมาประเมินโอกาสที่จะเกิดเหตุการณความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความ

เสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยงซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงานโดยมีการประเมินใน 2 มิติ ไดแกมิติผลกระทบและมิติโอกาสเกิด

โอกาสของความเสี่ยงที่จะเกิดขึ้นเกณฑ์การประเมินผลกระทบเป็นดังนี้

ระดับการประเมิน

1 น้อยมาก

2 น้อย

3 ปานกลาง

4 ค่อนข้างสูง

5 สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยงเป็นดังนี้

ระดับการประเมิน

1 เกิดขึ้นน้อยมาก

2 เกิดขึ้นน้อย

3 เกิดขึ้นปานกลาง

4 เกิดขึ้นค่อนข้างสูง

5 เกิดขึ้นสูงมาก

3.การวิเคราะห์ความเสี่ยงเป็นการดูความสัมพันธ์ระหวางโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใดโดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อนดังรูป

4 การจัดลำดับความเสี่ยงเป็นการจัดลำดับความรุนแรงของความเสี่ยงที่ผลต่อองค์กรเพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้เลือกความเสี่ยงที่มีระดับสูงหรือค่อนข้างสูงมาจัดทำแผนการบริหารความเสี่ยงก่อน

ระดับความเสี่ยง	คะแนน	สี	แนวทางการจัดการ
1.ต่ำ	1-3	ฟ้า	การยอมรับความเสี่ยงโดยไม่ต้องมีการควบคุมความเสี่ยง
2.ค่อนข้างต่ำ	4-8	เขียว	การยอมรับความเสี่ยง แต่ต้องมีการลดและควบคุมความเสี่ยง
3.ค่อนข้างสูง	9-14	เหลือง	ระดับที่ไม่สามารถยอมรับได้ โดยต้องมีการจัดการความเสี่ยง เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไประดับต่อไป
4.สูง	15-25	แดง	ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้ทันที

แบบประเมินความเสี่ยง

องค์ประกอบความเสี่ยง	P โอกาส	I ผลกระทบ	ความเสี่ยง = P x I
บุคลากร			
I. บุคลากรภายใน			
1.Admin+Network ไม่สามารถปฏิบัติหน้าที่ WFH			
1.1 ป่วย/ขาดงานโดยไม่ได้แจ้ง	2	4	8
1.2 อุบัติเหตุ	1	4	4
1.3 ติดภารกิจด่วนมาก	1	4	4
2. IT Support ไม่ปฏิบัติหน้าที่			
2.1 ป่วย/ขาดงานโดยไม่ได้แจ้ง	2	4	8
2.2 อุบัติเหตุ	1	4	4
2.3 ติดภารกิจด่วนมาก	1	4	4
3. Admin + Networkทำหน้าที่ผิดพลาด			
3.1 ทำงานผิดขั้นตอน (ระบบเสียหาย)	2	4	8
3.2 ทำงานผิดขั้นตอน (Hardware เสียหาย)	1	4	4
3.3 ย้าย/แกไข/เปลี่ยนแปลง/เพิ่มอุปกรณ์ผิดพลาด	2	4	8
3.4 ประมาทเลินเล่อในการรักษาความปลอดภัย	2	4	8

องค์ประกอบความเสี่ยง	P โอกาส	I ผลกระทบ	ความเสี่ยง = P x I
3.5 เข้ามาใช้งานระบบโดยไม่มีสิทธิ์	2	4	8
3.6 ไมตรวจสอบการ Backup	1	4	4
3.7 ไมตรวจสอบผลหลังการ Backup	1	4	4
3.8 ไมดูแล Server อย่างสม่ำเสมอ	1	4	4
3.9 ไมดูแลรักษาอุปกรณ์ที่เกี่ยวข้อง	2	4	8
II. บุคลากรภายนอก			
1.เข้ามาใช้งานระบบโดยไมมีสิทธิ์	2	5	10
2.เข้ามาโจมตีระบบ (Hacker)	1	4	4
3.เข้ามาทำลายข้อมูลใน PC	1	4	4
4.เข้ามาทำลายอุปกรณ์ Hardware	1	4	4
5.ขโมยอุปกรณ์ Hardware	1	4	4
6.การแผ่กระจาย Virus	2	5	10
III.เครื่องแม่ข่ายและอุปกรณ์ (Hardware & Accessory)			
1 Server			
1.1Server ไมทำงาน	1	4	4
1.2 อุบัติเหตุที่เกิดจากภัยธรรมชาติ/ภัยพิบัติ	1	4	4
1.3 Server ตั้งอยู่ในที่ไม่เหมาะสม	1	4	4
2. Power Supply / UPS			
3.1 เกิดข้อผิดพลาดในการจ่ายไฟ	1	5	5
3.2 ไมมีการสำรองไฟเมื่อเกิดเหตุฉุกเฉิน	2	5	10
3.5 ระเบิด	1	5	5
IV.โปรแกรม (software)			
4.1 Software Error	2	2	4
V. การเชื่อมโยงเครือข่าย (Network &Communicate)			
1. Fiber			
1.1 สายขาด	1	5	5
1.2 เหตุจากภัยธรรมชาติ	1	5	5
2. สาย หรืออุปกรณ์ Network			
2.1 สาย หรืออุปกรณ์ Network ไมสามารถใช้งานได	2	5	10
3. Wireless			

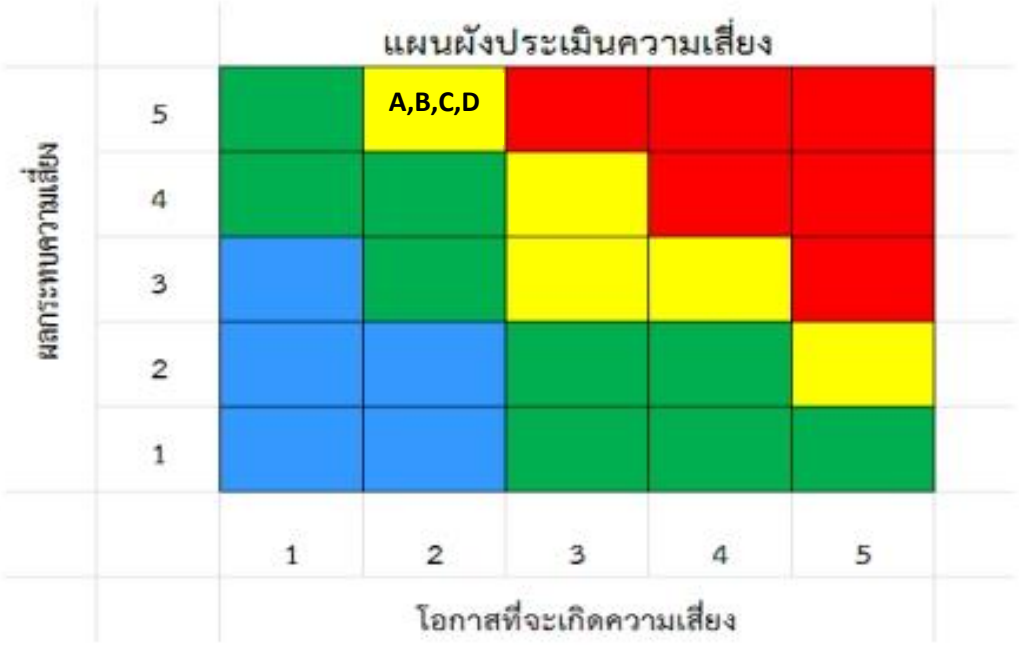
3.1 Wireless ตัวส่งสัญญาณไมสามารถใช้งานได้	2	4	8
4 System Data/ Information (Client Information)			
4.1 ข้อมูลสูญหาย	1	4	4
4.2 ข้อมูลโดน Virus	1	4	4
VII. ระบบไฟฟ้าและเครื่องสำรองไฟฟ้า			
1 ไฟฟ้า			
1.1.ไฟดับ	1	5	5
1.2 ไฟกระตุก	1	5	5
1.3 ฟ้าผ่า	1	5	5
2.เครื่องสำรองไฟ			
2.1.เครื่องสำรองไฟเสีย/ไม่เก็บไฟ	1	5	5
3.ระบบปรับอากาศ			
3.1.ระบบปรับอากาศไมทำงาน/ไม่เย็น	1	4	4
3.3.เครื่องมีน้ำหยด	1	5	5
4.ภัยธรรมชาติ			
4.1.น้ำท่วม	1	5	5
4.2.ไฟไหม	1	5	5
4.3.พายุ	1	5	5
4.4.แผ่นดินไหว	1	5	5

สรุปความเสี่ยงที่ต้องเร่งดำเนินการในปี 2565

องค์ประกอบความเสี่ยง	CODE	P โอกาส	I ผลกระทบ	ความเสี่ยง = PxI
การเข้าใช้งานข้อมูล				
- เข้ามาใช้งานระบบโดยไม่มีสิทธิ์	A	2	5	10
- การแพร่กระจาย virus computer	B	2	5	10
อุปกรณ์สำรองไฟฟ้าและป้องกันไฟ				
- ระบบสำรองไฟใช้ไม่ได้ ไม่เก็บไฟ	C	2	5	10
สาย หรืออุปกรณ์ Network				
- สาย หรืออุปกรณ์ Network ไมสามารถใช้งานได้	D	2	5	10

สรุปการวิเคราะห์ความเสี่ยง

เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่ผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได เลือกความเสี่ยงที่มีระดับสูง หรืออ่อนข้างสูงมาจัดทำแผนการบริหารความเสี่ยงก่อน



ประเภทความเสี่ยงแบ่งเป็น 3 ประเภทดังนี้

1 ความเสี่ยงด้านเทคนิคเป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือและอุปกรณ์เองอาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไมประสงค์ดีถูกกอกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker

2 ความเสี่ยงจากผู้ปฏิบัติงานเป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการการจัดความสำคัญในการเข้าถึงข้อมูลไมเหมาะสมกับการใช้งานหรือการให้บริการโดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆของกรมเกินกว่าอำนาจหนาที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได

3 ความเสี่ยงจากภัยหรือสถานการณฉุกเฉินเป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศเช่นไฟฟ้าขัดข้องน้ำท่วมไฟไหม อาคารถล่มการชุมนุมประท้วงหรือความไมสงบเรียบร้อยในบ้านเมือง

แผนจัดการความเสี่ยง (Risk management action plan)

แนวทางจัดการความเสี่ยงประกอบด้วย 4 รูปแบบ

1.การหลีกเลี่ยงความเสี่ยง(Risk Avoidance) การหลีกเลี่ยงความเสี่ยงโดยการปรับ / เปลี่ยนแปลงรูปแบบการทำงาน

2. การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับความเสี่ยง เหตุผล คือ ค่าใช้จ่ายจะสูงกว่าผลที่ไดรับแต่จะมีมาตรการหรือแผนในการกำกับดูแล

3. การลด/ควบคุมความเสี่ยง (Risk Mitiagatigation) การลด/ควบคุมความเสี่ยง ด้วยมาตรการต่างๆ

4. การกระจายหรือถ่ายโอนความเสี่ยง(Risk Transfer) การกระจายความเสี่ยงด้วยการโอนความเสี่ยงไปให้หน่วยงานอื่นรับผิดชอบ เช่น จ้างผู้อื่นมาดูแล

เมื่อความเสี่ยงไดรับการบ่งชี้และประเมินความสำคัญแลว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได และผลของการจัดการเหล่านั้นการพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับไดและต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชนที่จะไดรับ เพื่อให้การบริหารความเสี่ยงมีประสิทธิผลผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณให้อยู่ในช่วงที่องค์กรสามารถยอมรับได (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการคือ

การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือการเลือกที่จะไมรับความเสี่ยงไวเลยอาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได การหลีกเลี่ยงความเสี่ยง เมื่อพบว่าผลประโยชนที่จะไดรับนั้นไมคุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้นโดยมิไดคิดทบทวนถึงผลที่จะไดรับนามา ซึ่งการเสียโอกาสของหน่วยงานได

การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไวเองโดยไมทำอะไร และยอมรับในผลที่อาจตามมาเนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยูในวิสัยที่หน่วยงานยอมรับไดหรือไมคุ้มค่าสำหรับค่าให้จ่ายในการสรางระบบในการจัดการหรือปองกันความเสี่ยง

การลด/ควบคุมความเสี่ยง (Risk Reduction / Control) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้นเป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไมสามารถป้องกันไมให้ความเสี่ยงเกิดขึ้นไดก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผน หรือมาตรการควบคุมขึ้นอาจกำหนดเป็นแนวทางปฏิบัติไว ลวงหนาทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลักคือการป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสียเป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการ หรือวิธีการใดๆ ในการป้องกันไมให้ความสูญเสียเกิดขึ้น

การกระจายหรือถ่ายโอนความเสี่ยง (Risk Sharing) เป็นการโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไมทำงานองค์กรอาจเลือกซื้อประกันหรือสัญญาการบำรุงรักษาหลังการขาย

การดำเนินงานตามแผนการจัดการความเสี่ยง

1. บุคคลภายนอกเข้าใช้งานระบบคอมพิวเตอร์โดยไม่มีสิทธิ

การดำเนินการ

- ชี้แจง สร้างความตระหนัก ออกนโยบายไม่ให้บุคคลภายนอกเข้าใช้งานเครื่องคอมพิวเตอร์
- ออกระเบียบการลงทะเบียนขอเข้าใช้งานระบบคอมพิวเตอร์ เพื่อเก็บข้อมูลการเข้าใช้งานและกำหนดสิทธิการเข้าถึงตามความเหมาะสม
- หากพบการทำผิด รายงานหัวหน้างานและรายงานความเสี่ยง

ผู้ดำเนินการ

-คณะกรรมการ HIMS รพ.อุทัยธานี

ผลที่คาดจะได้รับ

- ไม่พบการใช้งานระบบคอมพิวเตอร์จากบุคคลภายนอกโดยไม่ได้รับอนุญาต

2. การแพร่กระจาย Virus computer

การดำเนินการ

- ประชาสัมพันธ์ ออกประกาศ ถึงการใช้งานที่ปลอดภัยจาก Virus
- update firewall (การบำรุงรักษารายปี) เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์
- ติดตั้งโปรแกรม Anti virus และ update ให้ทันสมัยอยู่เสมอ

- เจ้าหน้าที่ศูนย์คอมพิวเตอร์ monitor ดูสิ่งผิดปกติในระบบคอมพิวเตอร์ตลอดเวลา หากพบสิ่งผิดปกติให้ดำเนินการตรวจสอบและแก้ไขทันที
- update patch ของโปรแกรมระบบคอมพิวเตอร์ให้ทันสมัย

ผู้ดำเนินการ

- คณะกรรมการ HIMS , ศูนย์คอมพิวเตอร์

ผลที่คาดว่าจะได้รับ

- ไม่พบการติด Virus computer ในระบบคอมพิวเตอร์

3. ระบบสำรองไฟใช้ไม่ได้ /ไม่เก็บไฟ

การดำเนินการ

- ทำแผนตรวจสอบการทำงานของ UPS และรวบรวมข้อมูล
- จัดซื้อแบตเตอรี่มาดำเนินการเปลี่ยนตามข้อมูลที่ตรวจสอบ
- หากพบการชำรุด ให้แจ้งงานช่างเพื่อซ่อมแซมต่อไป
- จัดซื้อ UPS มาติดตั้งในจุดที่สำคัญ เช่น อุปกรณ์กระจายสัญญาณ(Switch hub)

ผู้ดำเนินการ

ศูนย์คอมพิวเตอร์

ผลที่คาดจะได้รับ

- เครื่องสำรองไฟใช้งานได้อย่างน้อย 5 นาทีถ้าเกิดไฟดับ

4. สายหรืออุปกรณ์ Network ไม่สามารถใช้งานได้

การดำเนินการ

-สำรวจจุดที่สาย LAN เก่า และมีสภาพชำรุด
- ดำเนินการซ่อมสาย LAN ใหม่ เช่น เปลี่ยนหัว RJ45 หรือ เดินสายใหม่
- เปลี่ยนอุปกรณ์กระจายสัญญาณเมื่อมีการใช้งานเกิน 3 ปี

ผู้ดำเนินการ

-ศูนย์คอมพิวเตอร์

ผลที่คาดว่าจะได้รับ

-ไม่พบระบบ LAN ใช้งานไม่ได้