แผนจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17
ประจำปีงบประมาณ 2567 – 2570

โดย

กลุ่มงานเทคโนโลยีสารสนเทศ

โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 สำนักงานสาธารณสุขจังหวัดสุพรรณบุรี

คำนำ

แผนจัดการความเสี่ยง ด้านระบบเทคโนโลยีสารสนเทศโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ประจำปีงบประมาณ 2567 - 2570 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลด ความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการจัดการความเสี่ยงเหล่านั้นให้อยู่ระดับที่องค์กรสามารถรองรับได้ เพื่อให้การดำเนินงานมีประสิทธิภาพและบรรลุวัตถุประสงค์ผู้จัดทำหวังเป็นอย่างยิ่งว่าแผนจัดการความเสี่ยง ด้านระบบเทคโนโลยีสารสนเทศ โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ฉบับนี้จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทาง ในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้าน เทคโนโลยีสารสนเทศโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ต่อไป

กลุ่มงานเทคโนโลยีสารสนเทศ
โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17
มกราคม 2567

สารบัญ

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

สืบเนื่องจากแผนแม่บทโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ที่เน้นพัฒนาด้านการรักษาพยาบาล และระบบสารสนเทศที่สอดคล้อง กับนโยบายกระทรวง 4.0 เพื่อตอบสนองการบริการผู้ป่วยได้ถูกต้อง รวดเร็ว และแม่นยำมีโครงสร้างการจัดเก็บและบริหารฐานข้อมูลที่บูรณาการ ไม่ซ้ำซ้อน สามารถรองรับการเชื่อมโยงการทำงานระหว่างหน่วยงานและให้บริการประชาชนได้อย่างทั่วถึงและมีประสิทธิภาพ

การบริหารจัดการความเสี่ยง จึงมีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้องงานตามภารกิจของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย ซึ่งขั้นตอนในการบริหารจัดการความเสี่ยง ควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศ และการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน มีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงาน จากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อให้การดำเนินตามภารกิจของหน่วยงานบรรลุผลตามวัตถุประสงค์ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลลัมฤทธ์ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2556 เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุวัตถุประสงค์ตามภารกิจที่ตั้งไว้และเป็นการพัฒนาการปฏิบัติงานของหน่วยงาน เพื่อน่าไปสู่การใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

1.2 คำจำกัดความและความหมายที่เกี่ยวข้องกับการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์/การกระทำใดๆ ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงลบต่อวัตถุประสงค์หรือเป้าหมายขององค์กร หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมายและวัตถุประสงค์ของแผนงาน/โครงการที่จะก้าวสู่พันธกิจ และวิสัยทัศน์ ที่กำหนดไว้

ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุของความเสี่ยงซึ่งจะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยงและการวิเคราะห์ความเสี่ยงเพื่อจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบต่อการบรรลุเป้าหมายขององค์กร (Impact)

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น 5 ระดับ คือ ความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงปานกลาง ความเสี่ยงต่ำ และความเสี่ยงต่ำมาก

โอกาส (Opportunity) หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงบวก ต่อวัตถุประสงค์หรือเป้าหมายขององค์กร ซึ่งผู้บริหารและผู้ที่เกี่ยวข้องควรจะได้ทบทวนถึงกลยุทธ์ และแผนงาน ที่เหมาะสมใหม่ เพื่อสร้างคุณค่าเพิ่มให้กับองค์กรนอกเหนือจากแผนงานและโครงการที่ได้กำหนดไว้

แล้วการควบคุมภายใน (Internal Control) หมายถึง กระบวนการปฏิบัติงานที่บุคลากรในองค์กร โดยคณะกรรมการบริหาร ผู้บริหารทุกระดับ และพนักงานทุกคนมีบทบาทร่วมกันในการจัดให้มีขึ้น เพื่อสร้างความเชื่อมั่นอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ของการควบคุมภายใน

การบริหารจัดการความเสี่ยง (Risk Management) หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด

การบริหารความเสี่ยงโดยองค์รวม (Enterprise Risk Management : EMR) หมายถึง การบริหารความเสี่ยง โดยมีโครงสร้างองค์กร กระบวนการ และวัฒนธรรมองค์กรประกอบเข้าด้วยกัน และเป็นกลไกส่วนหนึ่งของการขับเคลื่อนไปสู่การกำกับดูแลกิจการที่ดี เพื่อบรรลุวัตถุประสงค์และการเติบโตอย่างยั่งยืนขององค์กร และเป็นที่พอใจของผู้มีผลประโยชน์ร่วม โดยครอบคลุมความเสี่ยงทั่วทั้งองค์กร ไม่ว่าจะเป็นความเสี่ยงเกี่ยวกับกลยุทธ์ การดำเนินงาน การปฏิบัติตามกฎระเบียบ และการเงิน ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหายความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์และความต้องการของผู้มีผลประโยชน์ร่วม

1.3 ประโยชน์ของการจัดการความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้องค์กรสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

1) เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

2) สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร การบริหารความเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ รวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานในการตอบสนองต่อเป้าหมายและภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

3) ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล

4) เป็นเครื่องมือที่สำคัญในการบริหารงาน การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของโรงพยาบาล โรงพยาบาลหนองหญ้าไซเป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่องค์กร

5) ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจ ในกลยุทธ์ วัตถุประสงค์ขององค์กร และระดับความเสี่ยงอย่างชัดเจน

6) ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูง ย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละ ประเภทย่อมใช้ทรัพยากรแตกต่างกัน เป็นต้น

บทที่ 2
แนวทางการบริหารความเสี่ยง

2.1 หลักการบริหารความเสี่ยง

หลักการบริหารความเสี่ยงโดยใช้กระบวนการบริหารความเสี่ยงตามมาตรฐานของ COSO (The Committee of Sponsoring Organization of the Tread way Commission) ซึ่งกำหนดกรอบการจัดการความเสี่ยงในแนวทาง COSO : ERM (Enterprise Risk Management) ประกอบด้วยหลักการสำคัญ 8 องค์ประกอบ เพื่อให้เกิดการบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง ดังภาพที่ 1

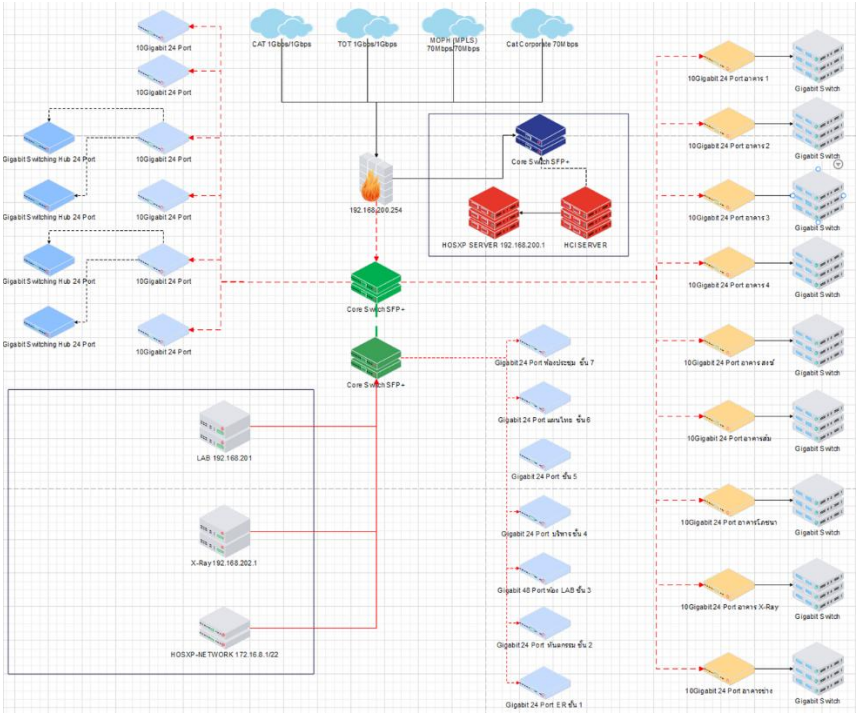
ภาพที่ 1 COSO : ERM (Enterprise Risk Management)

2.1.1. สภาพแวดล้อมภายในองค์กรด้านเทคโนโลยีสารสนเทศ (Internal Environment) ได้แก่

ระบบเครือข่ายของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (Wire Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองถูกบริหารจัดการโดยหน่วยงานศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบบเครือข่ายทั้ง 2 แบบนั้นสามารถใช้งานอินเตอร์เน็ตได้ โดยอินเตอร์เน็ตที่ใช้จะใช้บริการจากผู้ให้บริการอินเตอร์เน็ต (Internet

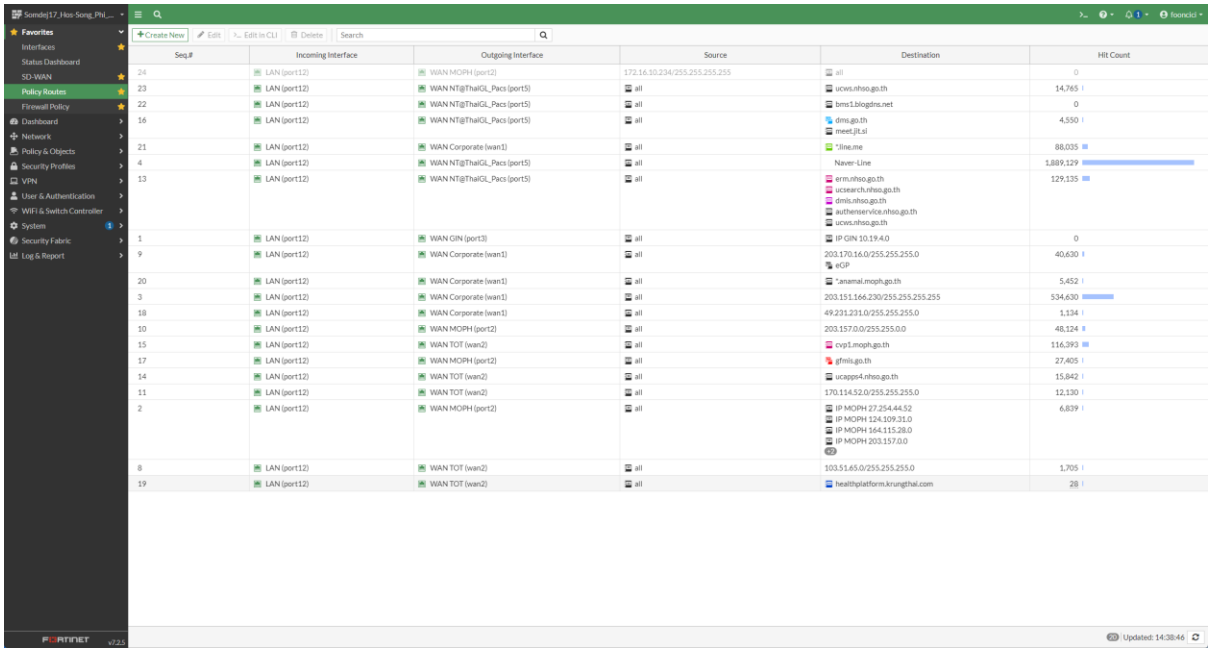
service provider: ISP) ทั้งหมด 1 ผู้ให้บริการ และ รับจัดสรรจากกระทรวงสาธารณสุข 1 ช่องทางด้วยดังรายการดังต่อไปนี้

1. บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) สาขาสุพรรณบุรี จำนวน 3 โครงข่าย
    1.1 วงจร TOT Broadband ความเร็ว 1000/1000 Mbps
    1.2 วงจร CAT Corporate ความเร็ว 50/50/5 Mbps
    1.3 วงจร CAT Broadband ความเร็ว 1000/1000 Mbps
2. ศูนย์เทคโลยีสารสนเทศ สำนักปลัดกระทรวงสาธารณสุข ระบบอินเตอร์เน็ต จำนวน 2 โครงข่าย และระบบอินทราเน็ต จำนวน 2 โครงข่าย
    2.1 ระบบอินเตอร์เน็ตของกระทรวง (MOPH)
        - วงจร MPLS ความเร็ว 60/60 Mbps
        - วงจร GIN ความเร็ว 10/10 Mbps



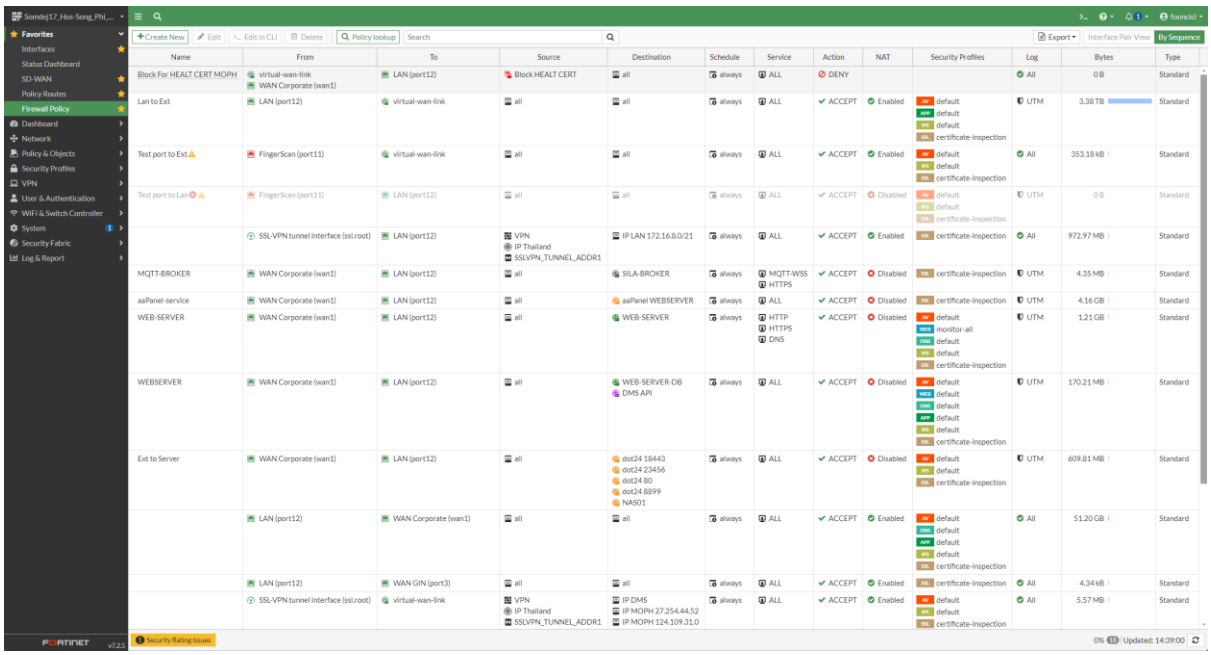
ภาพที่ 2 แสดงผังระบบเครือข่ายภายในโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17

โดยระบบเครือข่ายของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 จะทำการเชื่อมโยงระบบ เครือข่ายเข้ากับอุปกรณ์เครือข่ายของผู้ให้บริการอินเทอร์เน็ต (Internet Service provider: ISP) และเชื่อมต่อมายังอุปกรณ์เพื่อค้นหาเส้นทางของโรงพยาบาล พร้อมระบบป้องกันผู้บุกรุกทางเครือข่าย (Firewall) เพื่อรักษาความมั่นคงปลอดภัยในระบบเครือข่ายของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 จากนั้นจะทำการต่อเข้ากับอุปกรณ์เครือข่ายหลัก (Core Switch) ก่อนจะทำการกระจายไปยังจุดให้บริการต่างๆ ในโรงพยาบาล



ภาพที่ 3 แสดงสถานะอุปกรณ์ค้นหาเส้นทางอินเตอร์เน็ต (Router)

จากภาพที่ 3 แสดงสถานการณ์ทำงานของอุปกรณ์ค้นหาเส้นทางอินเตอร์เน็ตของโรงพยาบาล (Router) โดยหน่วยความจำถูกใช้งานร้อยละ 6.9 และทรัพยากรอื่นๆ เหลือเพียงพอต่อการใช้งานในปัจจุบัน



ภาพที่ 4 แสดงสถานะอุปกรณ์ค้นหาเส้นทางอินเตอร์เน็ต (Router)

จากภาพที่ 4 อุปกรณ์ค้นหาเส้นทางอินเตอร์เน็ตมีศักยภาพป้องกันข้อมูล เพื่อไม่ให้เกิดการบุกรุกจากบุคคลภายนอก เป็นอุปกรณ์ที่ช่วยกำหนดการรับ-ส่งข้อมูลภายในระบบเครือข่ายได้เป็นอย่างดี

สถานภาพครุภัณฑ์คอมพิวเตอร์ โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ประจำปี พ.ศ. 2568

สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งโปรแกรมพื้นฐานต่างๆ ที่โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ใช้ในการดำเนินงานปัจจุบันจะมีการสำรวจสภาพความพร้อมใช้และมีแผนในการจัดหาทดแทนเป็นประจำทุกปี โดยกลุ่มงานเทคโนโลยีสารสนเทศได้ทำการสำรวจข้อมูล ณ ปีงบประมาณ พ.ศ. 2567 มีรายละเอียดดังตารางต่อไปนี้

ลำดับ	รายการครุภัณฑ์คอมพิวเตอร์	จำนวน(เครื่อง)	หมายเหตุ
1	เครื่องคอมพิวเตอร์แม่ข่าย	11	
2	เครื่องคอมพิวเตอร์	514	
3	เครื่องพิมพ์ชนิดเลเซอร์ (Laser Printer)	114	
4	เครื่องพิมพ์ชนิดเลเซอร์ (Laser Multifunction Printer)	66	
5	เครื่องพิมพ์ชนิดเลเซอร์ (Color Laser Multifunction Printer)	3	
6	เครื่องพิมพ์ความร้อน (Thermal Printer)	86	
7	เครื่องพิมพ์หัวเข็ม (Dot Matrix Printer)	17	
8	เครื่องพิมพ์ชนิดฉีดหมึก (Inkjet Printer)	14	เครื่องส่วนตัวจัดซื้อเอง
9	เครื่องแสกนเนอร์ (Scanner)	7	
10	เครื่องแสกนเนอร์ความเร็วสูง (Scanner Jet)	8	
11	เครื่องสำรองไฟฟ้า (UPS)	434	
12	อุปกรณ์กระจายสัญญาณแบบสาย	36	
13	อุปกรณ์กระจายสัญญาณแบบไร้สาย	23	

ตารางที่ 1 แสดงรายการเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17

ระบบคอมพิวเตอร์

โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างต่อเนื่อง ปัจจุบันได้นำเทคโนโลยี Hyper Converged Infrastructure โครงสร้างของพื้นที่ข้อมูล (Data Center) ที่รวมเทคโนโลยีที่แตกต่างกันเข้าด้วยกันในรูปแบบของระบบเดียวกัน โดยประกอบด้วยคอมพิวเตอร์ประมวลผล (Server) ระบบเครือข่าย (Network) และพื้นที่จัดเก็บข้อมูล (Storage) ที่ทำงานร่วมกัน เพื่อให้มีความยืดหยุ่นในการขยายขนาดและจัดการทรัพยากรในศูนย์ข้อมูลอย่างมีประสิทธิภาพ ส่งผลทำให้ดูแลรักษาง่ายขึ้น ใช้เวลาในการติดตั้งโปรแกรมน้อยลง สำรองข้อมูลได้บ่อยขึ้น โดยปัจจุบันมี เครื่องแม่ข่ายเสมือนทั้งหมด 3 เครื่อง ที่รองรับเทคโนโลยีที่กล่าวมาข้างต้น

ตารางแสดงคอมพิวเตอร์แม่ข่ายแบบเสมือน (Virtual) ที่อยู่ในความดูแลของกลุ่มงานเทคโนโลยีสารสนเทศ

ลำดับ	เครื่อง Server	จำนวนหน่วยประมวลผล	OS	VM Name / Run ON	พื้นที่		หน่วยความจำ		IP	ผู้ดูแล/เบอร์โทรศัพท์
					Server	VM	Server	VM		
1	Dell PowerEdge R650 Server	Intel Xeon Platinum 8358P	VMware ESXi, 8.0.2	PRODUCTION_WEBHospital	42.01 TB	100 GB	3 TB	16 GB	172.16.9.33	
2				PRODUCTION_WEBServer		100 GB		16 GB	172.16.9.22	
3				PRODUCTION_Win10@invent		200 GB		8 GB	172.16.9.39	
4				PRODUCTION_Gateway_HIS_PACS		100 GB		16 GB	172.16.9.23	
5				PRODUCTION_HOSxP@Log_Image		2.66 TB		192 GB	172.16.9.16	
6				HOSxP_Cluster@Node1		1.66 TB		220 GB	172.16.9.15	

2.1.2. วัตถุประสงค์ของการจัดทำแผนจัดการความเสี่ยง (Objective Setting)

1) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17
2) เพื่อเป็นแนวทางในการรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
3) เพื่อให้มีการวางแผนการควบคุม และมีการปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้ทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.1.3. การบ่งชี้หรือการระบุความเสี่ยง (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม "What-if"
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสีย และความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบ ผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2.1.4. การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วย 4 ขั้นตอนคือ

1) การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก)

2) การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้น และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่ จะเกิดขึ้น

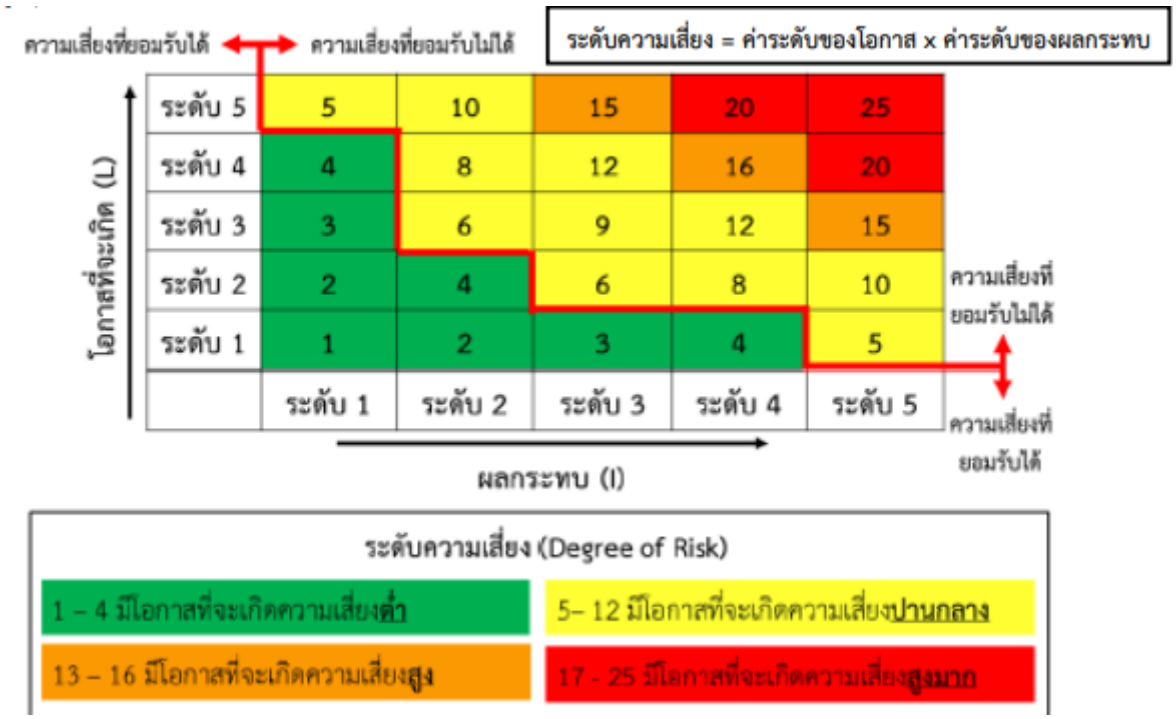
เกณฑ์ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง มีดังนี้

ระดับ	การประเมิน
1	มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก
2	มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี
3	มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง
4	มีจุดอ่อนมาก หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง
5	มีจุดอ่อนรอบด้าน หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆสัปดาห์

เกณฑ์การประเมินผลกระทบ มีดังนี้

ระดับ	การประเมิน
1	ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก
2	มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด
3	มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1-2 แผนก
4	มีผลกระทบต่อการให้บริการของโรงพยาบาล 3-4 แผนก
5	มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

3) การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและ ผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยง สูงสุดที่จะต้องบริหารจัดการก่อน



ภาพที่ 2 แสดงแผนผังการประเมินความเสี่ยง

4) การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจาก

ระดับ ความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

2.1.5. การตอบสนองความเสี่ยง (Risk Response)

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้ และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความ เสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้น และผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

- **การหลีกเลี่ยง (Terminate/Avoidance)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับ กิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้
- **การยอมรับ (Take/Acceptance)** เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะเกิดขึ้นไว้เอง โดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง
- **การควบคุมหรือการลด (Treat/Reduction)** เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือการป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสีย หลังเกิดความสูญเสียขึ้น การป้องกันการเกิดความสูญเสียเป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น
- **การถ่ายโอน (Transfer/Sharing)** การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

2.1.6. กิจกรรมการควบคุมความเสี่ยง (Control Activities)

การวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท คือ

- **ควบคุมเพื่อการป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึง เอกสาร เป็นต้น
- **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น
- **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีควบคุมที่ส่งเสริม หรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์
- **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้วจะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก ใช้ขั้นตอนดังนี้
    - นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูง มากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น
    - พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
    - ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

2.1.7. ข้อมูลสารสนเทศและการติดต่อสื่อสาร (Information & Communication)

เป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมิน และการบริหารจัดการความเสี่ยง ดังนั้น โรงพยาบาลศรีประจันต์ ได้รวบรวมและบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่ง ภายนอก และภายในตลอดจนเปิดเผยและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

2.1.8. การติดตาม (Monitoring)

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธี ซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้ว ให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดย พิจารณาจาก

1) พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
2) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่
3) กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง
4) ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ มาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยยะสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์ และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมิน และบริหารจัดการความเสี่ยงว่ามีความ

เสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ใน ระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

2.2 ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็น 8 ประเภท ดังนี้

1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2) ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการ ใช้งานการดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือ จาก คอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

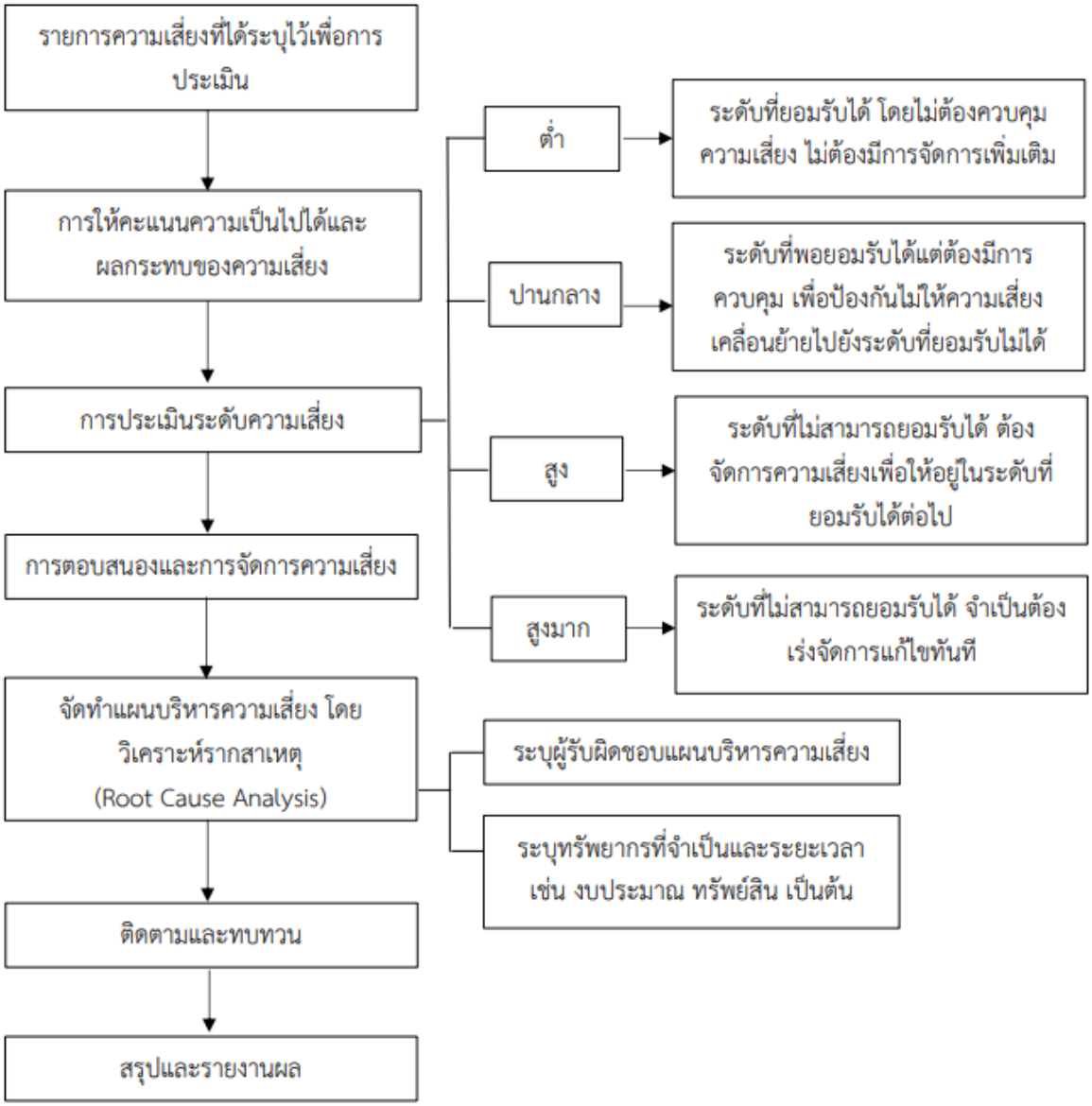
4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอับเดตให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งคณะฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

5) ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสาร อันอาจจะก่อให้เกิดความเสียหายเนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูลเพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

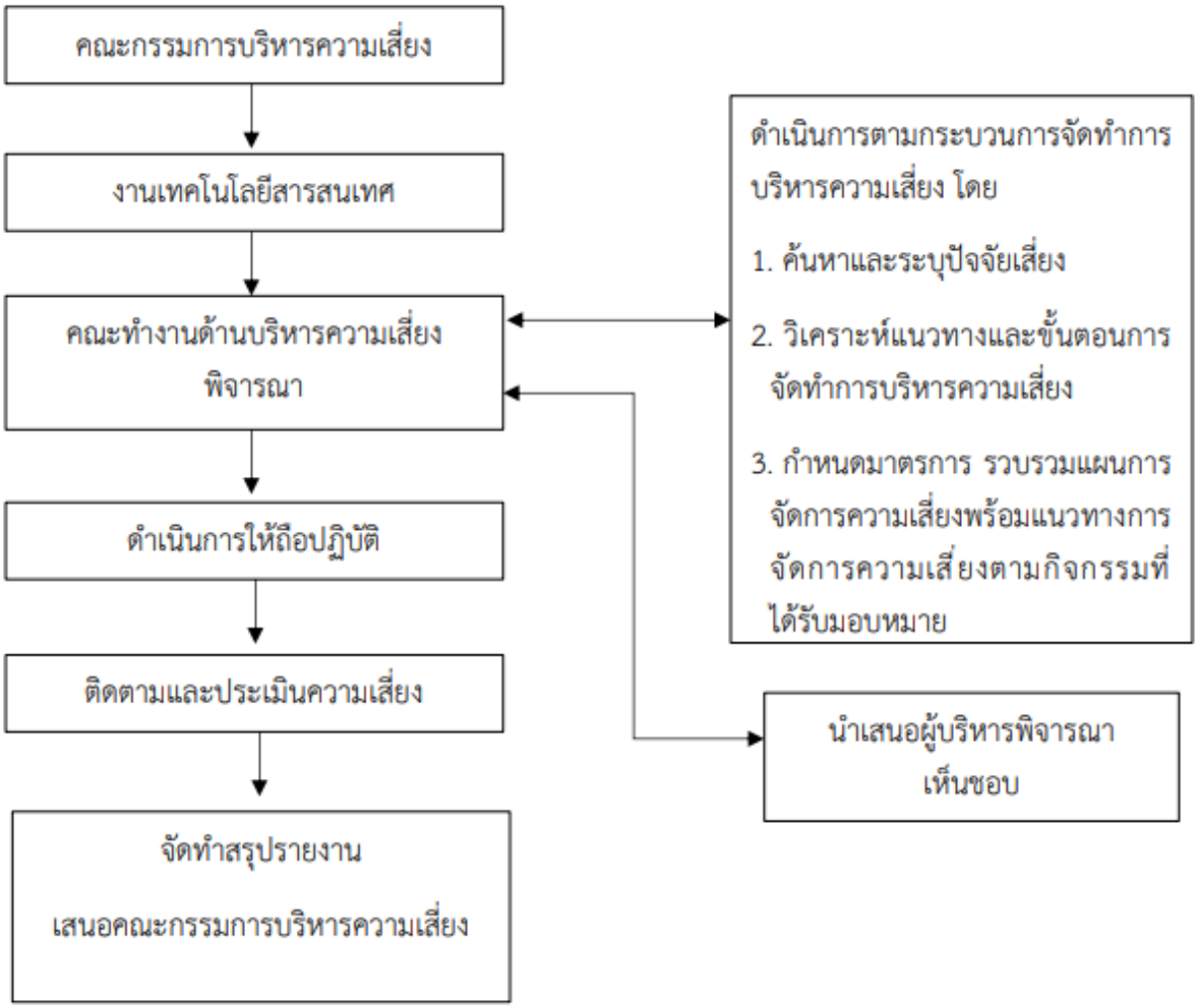
บทที่ 3
กระบวนการจัดการความเสี่ยง

โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงาน ด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

3.1 แผนภูมิแนวทางและขั้นตอนการจัดการความเสี่ยง



3.2 กระบวนการจัดทำการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้

แบบประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17

IT Components	Vulnerability		Score
- IT - Hardware			
1.1 Server and Main Switches Crash or Failure	อาจแยกประเมิน server แต่ละเครื่องหรือประเมินทั้งห้องร่วมกัน (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 4 = 5 5 – 7 = 4 8 – 11 = 3 12 – 14 = 2 15 – 16 = 1	● **กายภาพของห้อง server** - ระบบล็อคประตู => 1 - ระบบสลับการทำงานเครื่องปรับอากาศ => 1 - ระบบวัดอุณหภูมิ => 1 - ระบบตรวจจับควัน => 0 - ระบบแจ้งเตือนอัคคีภัย => 0 - ถังดับเพลิงที่เหมาะสม => 1 - ความสะอาด => 1 - การกำจัดสิ่งของไม่จำเป็นและเชื้อไฟออกจากห้อง => 1	6	**2**
	● **การจัดระเบียบสายสัญญาณและป้ายกำกับ** - สายสัญญาณด้านหน้า => 0 - สายสัญญาณด้านหลัง => 0 - ป้ายกำกับสายสัญญาณ => 1 - ป้ายกำกับ server => 1 - แผนผังตำแหน่งสายและช่องสัญญาณ => 1	3	
	● **การป้องกันการโจมตีพื้นฐาน** - มี firewall => 1 - เก็บ log => 1 - ตรวจสอบ log เป็นระยะ => 1	3	
1.2 Network Switches Crash or Failure	ประเมิน switches ที่อยู่ในจุดต่างๆ นอกห้อง (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 = 1	● **กายภาพของตู้ switches** - มีตู้ => 1 - ระบบล็อคประตู => 1 - ความสะอาด => 1 - การกำจัดสิ่งของไม่จำเป็น และเชื้อไฟออกจากตู้ => 1	4	**1**
	● **การจัดระเบียบสายสัญญาณและการป้องกันสัตว์กัดแทะ** - สายสัญญาณด้านหน้า => 1 - สายสัญญาณด้านหลัง => 1 - การป้องกันสัตว์กัดแทะ => 1	3	
	● **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 0	0	

IT Components	Vulnerability		Score
1.3 Workstation and Printers Failure	ประเมินภาพรวม PC ที่อยู่ในจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 = 1	• **กายภาพของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง** - ระบบป้องกันสายไฟสายสัญญาณ => 0 - ระบบป้องกันไฟตกไฟกระชาก => 1 - ความสะอาด => 1 - การป้องกันน้ำและอาหารหกใส่ => 0 - ระบบป้องกันคนนอกเข้าถึง => 1	3	**3**
	• **ระบบปฏิบัติการและระบบขับเคลื่อน (driver)** - ถูกลิขสิทธิ์ทั้งหมด => 1 - เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด => 1	2	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
2. IT – System Software			
2.1 Operating System Failure	ประเมินภาพรวม OS ที่อยู่ใน server ทั้งหมด ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 = 5 1 = 4 2 = 3 3 = 1	• **ระบบปฏิบัติการและระบบขับเคลื่อน (driver)** - ถูกลิขสิทธิ์ทั้งหมด => 1 - เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด => 1	2	**1**
	• **แผ่นติดตั้งระบบปฏิบัติการ ในกรณี ต้องกู้คืนระบบ** - มีแผ่นติดตั้งครบทั้งหมด => 1	1	
3. IT- Applications			
3.1 Front Offices	ประเมินระบบ HIS ที่ใช้บริการส่วนหน้าทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของ server** - CPU ไม่ overload => 1 - หน่วยความจำยังไม่หมด => 1 - พื้นที่ hard disk ยังเพียงพอ => 1	3	**1**
	• **แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ** - มีแผ่นติดตั้งครบทั้งหมด => 1	1	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
3.2 Back Offices	ประเมินระบบที่ใช้บริการส่วนหลังทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		

IT Components	Vulnerability		Score
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของ server** - CPU ไม่ overload => 1 - หน่วยความจำยังไม่หมด => 1 - พื้นที่ hard disk ยังเพียงพอ => 1	3	**1**
	• **แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ** - มีแผ่นติดตั้งครบทั้งหมด => 1	1	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
4. IT- Communication, Connectivity			
4.1 Intranet	ประเมินระบบเครือข่ายภายในของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของระบบเครือข่าย** - traffic ไม่เกินร้อยละ 80 => 1 - bandwidth ไม่เกินร้อยละ 80 => 1	2	**1**
	• **การแยกวง เช่น vlan** - มีการแยกวงที่เหมาะสม => 1 - แยกระบบ HIS ออกจากระบบอินเทอร์เน็ต => 1	2	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
4.2 Internet	ประเมินระบบเครือข่ายที่เชื่อมต่ออินเทอร์เน็ตของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **การใช้ทรัพยากรของระบบเครือข่าย** - Traffic ไม่เกินร้อยละ 80 => 1 - bandwidth ไม่เกินร้อยละ 80 => 1	2	**2**
	• **การเพิ่มสายสำรอง กรณีผู้ให้บริการหยุดชะงัก** - มีสายสำรองที่ 2 => 1 - มีสายสำรองที่ 3 => 0	1	
	• **ระบบบำรุงรักษา** - ตรวจสอบและบำรุงรักษาเป็นประจำ => 1	1	
5. IT – Operational (Human) Error			
5.1 Backup Error	ประเมินระบบงานที่ทำให้การสำรองข้อมูลเกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4	• **ขั้นตอนการปฏิบัติงานที่เหมาะสม** - มีขั้นตอนการปฏิบัติงานชัดเจน => 1 - ผู้สำรองข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง => 1	2	**2**

IT Components	Vulnerability		Score
3 = 3 4 = 2 5 = 1	• **ระบบตรวจสอบข้อมูลสำรอง** - มีระบบตรวจสอบความครบถ้วนสมบูรณ์ => 1 - มีการทดลอง restore กลับ => 0	1	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 1	1	
5.2 Data Loss Error	ประเมินระบบงานที่ทำให้ข้อมูลที่ผู้ใช้บันทึกไม่เกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **ขั้นตอนการปฏิบัติงานที่เหมาะสม** - มีขั้นตอนการปฏิบัติงานชัดเจน => 1 - ผู้บันทึกข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง => 1	2	**1**
	• **ระบบป้องกันข้อมูลสูญหายหรือผิดพลาด** - ปิดช่องว่างจากขั้นตอนการทำงาน => 1 - ปิดช่องว่างจากโปรแกรม => 1	2	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 1	1	
6. Data Loss and Privacy Breach			
6.1 Data Backup	ประเมินระบบงานที่ทำให้ข้อมูลสำรองสูญหาย (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **ระบบ offline backup** - มีระบบ offline backup => 1 - อุปกรณ์เก็บข้อมูลสำรองมีจำนวนเพียงพอ => 1 - อุปกรณ์เก็บข้อมูลสำรองมีที่เก็บปลอดภัย => 1	3	**1**
	• **ระบบป้องกันข้อมูลสำรองถูกจารกรรม** - มีระบบห้ามบุคลากรนำข้อมูลสำรองออกสู่ภายนอก => 1	1	
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 1	1	
6.2 Data Protection Policy and Regulations	ประเมินการป้องกันความลับและความเป็นส่วนตัวของข้อมูล (เลือก 0 หรือ 1 แต่ละข้อ)		
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	• **ระบบห้ามการเข้าถึงข้อมูลที่บุคลากรไม่มีส่วนเกี่ยวข้อง** - มีระบบล็อคหรือมีระเบียบห้ามการเข้าถึงข้อมูลที่ตนเองไม่มีส่วนเกี่ยวข้อง => 1	1	**3**
	• **ระบบอภิบาลข้อมูล** - มีการสำรวจและจัดทำทะเบียนข้อมูลสำคัญ => 1 - มีการจัดประเภทข้อมูลที่ต้องปกปิด => 1 - มีขั้นตอนการจัดการข้อมูลสำคัญตั้งแต่ต้นทางจนถึงปลายทาง => 0	2	

IT Components	Vulnerability		Score
	• **ระบบกำกับดูแลโดยผู้บังคับบัญชา** - กำกับดูแลเป็นประจำ => 0	0	
6.3 PDPA Implementation			
เกณฑ์คะแนน 0 – 1 = 5 2 = 4 3 = 3 4 = 2 5 = 1	- ประเมินการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้คะแนน 0 ถึง 5 => 5	4	**2**
7. IT – Future Development			
7.1 No Data Dictionary	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีเอกสาร Data Dictionary ครบทุกตารางในฐานข้อมูล => 0	1	**1**
7.2 No System Blueprint	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีเอกสาร วิเคราะห์และออกแบบระบบที่พัฒนาเอง => 0	1	**1**
7.3 No System Document or Comments	ประเมินการบันทึก comment และ version ของผู้พัฒนาโปรแกรม (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีเอกสาร version control และ source code comment => 0	1	**1**
8. IT – Vendor and Outsource Failure			
8.1 Vendor stop Support	ประเมินสัญญาที่ทำกับบริษัทภายนอก (เลือก 0 หรือ 1)		
เกณฑ์คะแนน 0 = 5 1 = 1	- มีสัญญาที่บริษัทจะต้องส่งมอบเอกสารสำคัญและข้อมูลทั้งหมดเมื่อหมดสัญญา => 1	1	**1**
9. IT – Hacking Unauthorized Intrusions			
ประเมินภาพรวมจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)			
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2	• **เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง** - มีระบบหรือระเบียบล็อคหน้าจอเมื่อไม่มีผู้ใช้งาน => 1 - เข้ารหัสข้อมูลส่วนตัวผู้ป่วย => 0 - มีการป้องกันการถ่ายภาพหน้าจอในจุดที่คนนอกเข้าถึง => 0	1	**3**

IT Components	Vulnerability		Score
8 – 9 = 1	• **ระบบเครือข่าย** - ปิดสัญญาณช่องเชื่อมต่อเครือข่ายที่ไม่มีการใช้าน => 0 - มีการเข้ารหัสและตั้งรหัสผ่านการใช้ WIFI access => 1 - เปลี่ยนรหัส WIFI บ่อย ๆ => 0	1	
	• **ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย** - ห้ามใช้ username ร่วมกัน => 1 - ตั้ง username และ password ซับซ้อน => 1 - ห้ามติด password ไว้ในที่เปิดเผย => 1	3	
10. Environment Factors			
เกณฑ์คะแนน 0 = 5 1 = 1	**10.1 Flooding – Internal** ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากน้ำรั่วในสำนักงาน (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้น้ำรั่วไหลลงสู่ทรัพย์สิน IT => 1	1	**1**
	10.2 Flooding – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอุทกภัยในพื้นที่ (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้อุทกภัยสร้างความเสียหายต่อทรัพย์สิน => 0	1	**1**
	10.3 Fire – Internal ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟไหม้ในโรงพยาบาล (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน => 1 -	1	**1**
	10.4 Fire – External ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอัคคีภัยในพื้นที่ (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน IT => 0	1	**1**
	10.5 Utilities – Electricity ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟฟ้าตกหรือกระชาก (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้ไฟฟ้าสร้างความเสียหายต่อทรัพย์สิน IT => 1	1	**1**
	10.6 Criminal – Theft ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากโจรกรรม (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT => 1	1	**1**
	10.7 Criminal – Break-ins ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากการงัดแงะหรือย่องเบา (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT => 1	1	**1**
	10.8 Civil Unrest – Protest, Mob ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากเหตุจลาจล วัยรุ่นทะเลาะกัน (เลือก 0 หรือ 1) - มีระบบป้องกันไม่ให้มีผู้สร้างความเสียหายต่อทรัพย์สิน IT => 0	0	**5**

IT Components	Vulnerability		Score
11. Patient Risks due to IT Errors/Misuse			
ประเมินจุดอ่อนการใช้ IT ที่อาจทำให้เกินอันตรายต่อผู้ป่วย (เลือก 0 หรือ 1 แต่ละข้อ)			
เกณฑ์คะแนน 0 – 2 = 5 3 – 4 = 4 5 – 6 = 3 7 = 2 8 = 1	● **ระบบแจ้งเตือนเมื่อพบค่าวิกฤต** - มีระบบแจ้งเตือนเมื่อพบค่าวิกฤตของผู้ป่วย => 1 - มีการแจ้งเตือนผู้เกี่ยวข้องทันที => 1 - มีการตรวจสอบว่าระบบแจ้งเตือนทำงานได้ตามปกติ => 1	3	**2**
	● **ระบบตรวจสอบการสั่งการรักษาหรือไม่สั่งการรักษาที่เหมาะสม** - มีระบบตรวจสอบการไม่สั่งการรักษาที่เหมาะสมและแจ้งเตือน => 1 - มีระบบตรวจสอบการสั่งการรักษาที่เหมาะสม => 1	2	
	● **ระบบป้องกันความผิดพลาดในการบันทึกข้อมูล ตรวจสอบบุคคล หัวหน้าตรวจสอบ** - มีระบบป้องกันความผิดพลาดในการบันทึกข้อมูล => 1 - มีระบบตรวจสอบบุคคลแบบ double check => 1 - มีระบบหัวหน้ายืนยันการดำเนินการกรณีสำคัญยิ่งยวด => 0	2	

ผลการประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศ ปี พ.ศ.2568

IT Components	Probability (P)	Impact (I)	Risk = P x I
1. IT – Hardware			
1.1 Servers Crash or Failure	1 **2** 3 4 5	1 2 3 4 **5**	10
1.2 Network Switches Crash or Failure	**1** 2 3 4 5	1 2 3 **4** 5	4
1.3 Workstations Failure	1 2 **3** 4 5	**1** 2 3 4 5	3
2. IT – System Software			
2.1 Operating System Failure	**1** 2 3 4 5	1 **2** 3 4 5	2
3. IT – Applications			
3.1 Front Offices	**1** 2 3 4 5	**1** 2 3 4 5	1
3.2 Back Offices	**1** 2 3 4 5	1 2 3 **4** 5	4
4. IT – Communications, Connectivity			
4.1 Intranet	**1** 2 3 4 5	1 2 3 4 **5**	5
4.2 Internet	1 **2** 3 4 5	1 2 3 4 **5**	10
5. IT – Operational (Human) Error			
5.1 Backup Error	1 **2** 3 4 5	1 2 **3** 4 5	6
5.2 Data Loss Error	**1** 2 3 4 5	1 **2** 3 4 5	1
6. Data Loss and Privacy Breach			
6.1 Data Backup	**1** 2 3 4 5	1 2 **3** 4 5	3
6.2 Data Protection Policy and Regulations	1 2 **3** 4 5	1 **2** 3 4 5	6
6.3 PDPA Implementation	1 **2** 3 4 5	1 2 3 4 **5**	10
7. IT –Future Development			
7.1 No Data Dictionary	**1** 2 3 4 5	**1** 2 3 4 5	1
7.2 No System Blueprint	**1** 2 3 4 5	**1** 2 3 4 5	1
7.3 No Program Document or Comments	**1** 2 3 4 5	**1** 2 3 4 5	1
8. IT – Vendor and Outsource Failure			
8.1 Vendor Stop Support	**1** 2 3 4 5	**1** 2 3 4 5	1
9. IT – Hacking, Unauthorized Intrusions	1 2 **3** 4 5	1 2 3 4 **5**	15
10. Environment Factors			
10.1 Flooding – Internal	**1** 2 3 4 5	1 2 3 4 **5**	5
10.2 Flooding – External	**1** 2 3 4 5	1 2 3 4 **5**	5
10.3 Fire – Internal	**1** 2 3 4 5	1 2 3 4 **5**	5
10.4 Fire – External	**1** 2 3 4 5	1 2 3 4 **5**	5
10.5 Utilities – Electricity	**1** 2 3 4 5	1 2 3 4 **5**	5
10.6 Criminal – Theft	**1** 2 3 4 5	1 2 3 4 **5**	5
10.7 Criminal – Break-ins	**1** 2 3 4 5	1 2 3 4 **5**	5
10.8 Civil Unrest – Protest, Mob	1 2 3 4 **5**	1 2 3 4 **5**	25
11. Patient Risks due to IT Errors/Misuse	1 **2** 3 4 5	1 **2** 3 4 5	4
12. Other	1 2 3 4 5	1 2 3 4 5	

เมื่อคำนวณคะแนนความเสี่ยงแล้วนำคะแนนความเสี่ยงมาพิจารณาตามแผนผังประเมินความเสี่ยง ดังนี้

แผนผังประเมินความเสี่ยง

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

จากแผนผังประเมินความเสี่ยง จะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 17 ถึง 25 จะเป็นเหตุการณ์ที่เร่งต้องจัดการความเสี่ยงโดยเร่งด่วน (แสดงในตารางเป็นสีแดง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยง ตั้งแต่ 1-3 จะเป็นเหตุการณ์ที่ยังไม่ต้องเร่งรีบจัดการ (แสดงในตารางเป็นสีเหลือง)

การยอมรับความเสี่ยง (Risk Acceptance)

การยอมรับความเสี่ยง (Risk Acceptance) คือ การยินยอมให้ความเสี่ยงคงอยู่โดยไม่ดำเนินการควบคุมเพิ่มเติม

ตารางเกณฑ์ความสามารถในการยอมรับความเสี่ยง

ความ เสี่ยง	คะแนน	แถบสี	ความหมาย
ต่ำ	1-3		Acceptable or Limited Focus ระดับที่ยอมรับได้โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	4-9		Tolerable but caution or Management Discretion / Medium Risk ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	10-16		Intolerable or Attention Required/High Risk ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	17-25		Intolerable or Immediate Attention Require / High Risk ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการควบคุมให้อยู่ใน ระดับที่ยอมรับได้ทันที

ตารางรายการความเสี่ยงที่ยอมรับได้

ลำดับ	รายการความเสี่ยง	ระดับความเสี่ยง	เหตุผลในการยอมรับ	มาตรการเฝ้าระวัง/ติดตาม
1	เครื่องคอมพิวเตอร์ของเจ้าหน้าที่บางเครื่องทำงานช้า/ฮาร์ดดิสก์เต็ม	ต่ำ	ไม่กระทบระบบหลัก ใช้งานภายในรายบุคคล	ตรวจสอบรายเดือน พร้อมแนะนำอัปเกรด
2	เครื่องพิมพ์ในบางจุดไม่สามารถเชื่อมต่อได้ในช่วงเวลานอกเวลาราชการ	ต่ำ	ไม่มีผลกระทบต่อการบริการผู้ป่วยในเวลาราชการ	งานไอทีเข้าตรวจเช็คตามแผน
3	การใช้งาน USB Drive ในงานเวรหอผู้ป่วย	ต่ำ ระดับกลาง	เป็นการโอนข้อมูลภายในหน่วยงาน ไม่มีข้อมูลส่วนบุคคล	มีนโยบายการใช้ USB อย่างปลอดภัย (เช่น Scan ทุกครั้ง)
4	ยังไม่มีระบบสำรองอัตโนมัติในระบบย่อย (ระบบแจ้งเตือนภายในบางหน่วยงาน)	ต่ำ	ไม่ใช่ระบบ core, ข้อมูลไม่สำคัญมาก	บันทึก log การใช้งานและจัดเก็บข้อมูลมือ
5	บางเครื่องไม่สามารถอัปเดต Windows ทันทีได้	ต่ำ	ติดข้อจำกัดด้านเวอร์ชันของซอฟต์แวร์เฉพาะ	ทำ whitelist และบันทึกเพื่ออัปเดตในรอบเดือน

กระบวนการอนุมัติการยอมรับความเสี่ยง

1. ผู้ประเมินความเสี่ยง ทำการประเมินและเสนอรายการความเสี่ยงที่อยู่ในเกณฑ์สามารถยอมรับได้
2. หัวหน้ากลุ่มงาน IT ตรวจสอบความเหมาะสมและผลกระทบโดยรวม
3. คณะกรรมการบริหารความเสี่ยงโรงพยาบาล หรือ ผู้อำนวยการโรงพยาบาล พิจารณาอนุมัติ
4. บันทึกลงใน ทะเบียนความเสี่ยง (Risk Register) และติดตามอย่างน้อย ปีละ 1 ครั้ง

บทที่ 4
กลยุทธ์ในการแก้ไขความเสี่ยง

โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 17 จึงจัดทำแผนกลยุทธ์จัดการความเสี่ยงทางเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2568

IT - Hardware

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1.1 Server and Main Switches Crash or Failure	10			
		อุปกรณ์ในเครื่องแม่ข่ายเสียหาย	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีการรักษาความเย็นในห้อง Server ให้อยู่ใน 24 องศา ซึ่งยอมรับได้ถึง 26 องศา ถ้าเกินกว่านั้น ต้องรีบหาทางแก้ไข 2. หมั่นตรวจสอบเครื่องสำรองไฟ และเปลี่ยนแบตเตอรี่ทุก 2 ปี 3. จัดหาระบบมอนิเตอร์สถานะ Server
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. จัดทำระบบ DR-Site 2. มีเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันที 3. จัดทำแผนกู้คืนระบบ
1.2 Network Switches Crash or Failure	4			
		อุปกรณ์กระจายสัญญาณเสียหรือมีปัญหา	ลดโอกาสที่จะเกิดเหตุการณ์	1.จัดหาเครื่องสำรองไฟ
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.มีครุภัณฑ์สำรองอย่างน้อย 2 ตัว 2.ดำเนินการตามแผน BCP
		สาย CAT5, CAT6 ที่เชื่อมต่อภายภายในมีปัญหา	ลดโอกาสที่จะเกิดเหตุการณ์	1.จัดทำระบบสายสำรอง
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.จัดหาอุปกรณ์สำรองสำหรับซ่อมแซม 2.ดำเนินการตามแผน BCP
		สาย Fiber Optic เครือข่ายภายในขาดหรือใช้งานไม่ได้	ย้ายกระบวนการซ่อมไปอยู่ในความรับผิดชอบบริษัท	1. จัดทำระบบสายสำรอง 2. ทำสัญญากับบริษัทที่ดำเนินการติดตั้งสาย Fiber Optic ให้โรงพยาบาลดำเนินการแก้ไขภายใน 24 ชั่วโมง หรือน้อยกว่านั้น
			ลดโอกาสที่จะเกิดเหตุการณ์	1.จัดทำระบบสายสัญญาณสำรอง (Link Backup)
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.ดำเนินการตามแผน BCP

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1.3 Workstation and Printers Failure	3			
		เครื่องคอมพิวเตอร์	ลดโอกาสเกิดปัญหา	1. มีแผนการตรวจเช็คอุปกรณ์ ทำความสะอาดคอมพิวเตอร์อย่างน้อย 6 เดือนครั้ง 2. มีทดแทนอุปกรณ์เครื่องเก่าที่ใช้งานมานานเกิน 7 ปี 3. มีเครื่องสำรองไฟใช้กับเครื่องคอมพิวเตอร์ในห้องตรวจทุกเครื่อง
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องคอมพิวเตอร์สำรองพร้อมใช้งาน 2. มีอะไหล่สำรองแต่ละชนิดอย่างน้อย 3-5 ชิ้น
		อุปกรณ์ต่อพ่วงคอมพิวเตอร์ เช่น เครื่องพิมพ์	ลดผลเสียหายที่เกิดย้ายความเสี่ยงไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1.ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดต้องมีการสำรองเครื่องพิมพ์อย่างน้อย 10% ของจำนวนที่ทำสัญญาเช่า
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดให้มีการตรวจสอบเครื่องพิมพ์อย่างน้อย 1 เดือนครั้ง

IT – System Software

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
2.1 Operating System Failure	2			
		OS ในเครื่อง Server มีปัญหา	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันที 2. ดำเนินการ Veeam Restore 3. มีการดำเนินตามแผน DRP 4. มีการดำเนินการตามแผน BCP 5. พัฒนาศักยภาพของบุคลากรในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
		OS ในเครื่อง Client มีปัญหา	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องคอมพิวเตอร์สำรองพร้อมใช้งาน 2. มีอะไหล่สำรองแต่ละชนิดอย่างน้อย 3-5 ชิ้น

IT- Applications

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
3.2 Back Offices	4			
		โปรแกรม Back Offices มีปัญหา	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ดำเนินการตามแผน Backup & Restore 2. ดำเนินการทดสอบ Restore ข้อมูลทุกทุก 1 เดือน 3. มีการดำเนินตามแผน BCP

IT- Communication, Connectivity

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
4.1 Intranet	5			
		ระบบนำเสนอข้อมูลข่าวสารผ่านระบบอินทราเน็ตไม่สามารถใช้งานได้	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ดำเนินการตามแผน Backup & Restore 2. ดำเนินการทดสอบ Restore ข้อมูลทุกทุก 1 เดือน 3. มีการดำเนินตามแผน BCP
4.2 Internet	10			
		ระบบการสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ตไม่สามารถใช้งานได้	ลดโอกาสเกิดความเสียหาย	1. มีผู้ให้บริการอินเตอร์เน็ต อย่างน้อย 2 บริษัทที่ให้บริการในโรงพยาบาล
			ย้ายความเสี่ยงไปยังผู้ให้บริการอินเตอร์เน็ต	1. แจ้งผู้ให้บริการเพื่อดำเนินการแก้ไข

IT – Operational (Human) Error

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
5.1 Backup Error	6			
		ไม่ได้สำรองข้อมูล	ลดโอกาสเกิดเหตุการณ์	แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูล
		สำรองข้อมูลไม่สำเร็จ	ลดโอกาสเกิดเหตุการณ์	แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูลจัดทำระบบ ย้ายไฟล์อัตโนมัติ
		สำรองข้อมูลไม่ได้คุณภาพ	ยอมรับความเสี่ยงเหตุการณ์	มีการสุ่มตรวจสอบข้อมูลที่สำรองไว้ เดือนละ 1 ครั้ง
		พื้นที่ที่สำรองข้อมูลเต็ม	ลดโอกาสเกิดเหตุการณ์	แผนจัดทำระบบแจ้งเตือนอัตโนมัติเมื่อฮาร์ดดิสก์ใกล้เต็ม
5.2 Data Loss Error	2			
		การเข้าถึงข้อมูลและการเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ลดโอกาสเกิดเหตุการณ์	1.กำหนดสิทธิการใช้งาน
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.พัฒนาให้โปรแกรมสามารถเก็บประวัติการใช้งานได้ 2. แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูล 3. มีการเก็บข้อมูลทั้งในระบบเวชระเบียนและในระบบ HIS

Data Loss and Privacy Breach

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
6.2 Data Protection Policy and Regulations	6			
		การเข้าถึงข้อมูลที่บุคลากรไม่มีส่วนเกี่ยวข้อง	ลดโอกาสเกิดเหตุการณ์	1. กำหนดสิทธิการเขาถึงข้อมูลแยกตามหน่วยงาน
6.3 PDPA Implementation	10			
		การเข้าถึงข้อมูลส่วนบุคคล	ลดโอกาสเกิดเหตุการณ์	1. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบายระเบียบ และแนวปฏิบัติแก่บุคลากร ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล 2. จัดทำนโยบายระเบียบและแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการ และแนวปฏิบัติ

IT – Hacking Unauthorized Intrusions

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
9.1 Hacking Unauthorized Intrusions	15			
		การสวมรอยของผู้ใช้งาน	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีระเบียบปฏิบัติในการห้ามเผยแพร่รหัสผ่านของตนเอง และต้องออกจากระบบเมื่อเลิกใช้งาน 2. มีระบบ Auto logout 5 นาที เมื่อไม่มีการใช้งาน
		การเปิดช่องให้มีการเข้าถึงระบบได้จากภายนอก	ลดโอกาสเกิดเหตุการณ์	1. มีการยืนยันตัวตน หรือการใช้ Token เพื่อเป็นรหัสผ่านในการเข้าถึงข้อมูล 2. การเปิดช่องทางเฉพาะที่ต้องการใช้งานเท่านั้น 3. เปิดให้บริการ Web Service โดยกำหนดเวลา
		เครื่องคอมพิวเตอร์ติดไวรัส	ลดโอกาสที่จะเกิดเหตุการณ์	1. มีการติดตั้ง Antivirus ที่ไม่มีวันหมดอายุ และสามารถอัพเดต และจับไวรัสได้จริง 2. มี Firewall
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. แนะนำให้ผู้ใช้เก็บข้อมูลที่สำคัญในไดร์ฟอื่น

Environment Factors

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
10.1 Flooding – Internal	5			
		โอกาสเกิดน้ำรั่วในห้อง Server	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งพื้นยก (Raised Floor) เหนือจากพื้น 15 ซม.
10.2 Flooding – External	5			
		อำเภอสองพี่น้องเป็นพื้นที่มีโอกาสเกิดน้ำท่วม	ลดผลเสียหายเมื่อเกิดเหตุการณ์	วางแผนรับมือน้ำท่วมโดยทำการย้ายอุปกรณ์มายังจุดที่น้ำท่วมไม่ถึง
10.3 Fire – Internal	5			
		ไฟไหม้เครื่องแม่ข่าย และ ไฟไหม้อุปกรณ์กระจายสัญญาณ	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งอุปกรณ์ดักจับควัน 2. มีป้ายห้ามสูบบุหรี่ ห้ามนำวัสดุติดไฟง่ายเข้าใกล้เครื่องแม่ข่าย
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีถังดับเพลิงติดตั้งภานในห้อง Server 2. จัดทำระบบ DR-Site 3. ดำเนินการตามแผน DRP 4. ดำเนินการตามแผน BCP

10.4 Fire – External	5			
		การเกิดไฟไหม้ในพื้นที่	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1.
10.5 Utilities – Electricity	5			
		ไฟดับ ไฟกระชากทำให้ระบบ Server และระบบ Network ทำงานไม่ได้	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. มีเครื่องสำรองไฟสำหรับ server, switch, และ client ที่สำคัญ 2. หมั่นตรวจสอบเครื่องสำรองไฟ และเปลี่ยนแบตเตอรี่ทุก 2 ปี 3. จัดทำระบบ DR-Site 4. ดำเนินการตามแผน DRP 5. ดำเนินการตามแผน BCP
			ย้ายความเสี่ยงไปยังแผนกช่างไฟฟ้า	ระบบไฟฟ้าโรงพยาบาล สามารถทำงานเมื่อเกิดไฟฟ้าดับ ภายใน 10 วินาที
10.6 Criminal – Theft	5			
		การลักขโมย หรือโจรกรรม	ลดโอกาสที่จะเกิดเหตุการณ์	1. ล็อคประตูเมื่อไม่มีเจ้าหน้าที่อยู่ห้อง 2. มีระบบแสกนลายนิ้วมือเพื่อเปิดเข้าห้อง Server 3. มีการติดตั้งกล้องวงจรปิด
			ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. จัดทำระบบ DR-Site 2. ดำเนินการตามแผน DRP 3. ดำเนินการตามแผน BCP
10.7 Criminal – Break-ins	5			
		การงัดแงะหรือย่องเบา	ลดโอกาสที่จะเกิดเหตุการณ์	1. ล็อคประตูเมื่อไม่มีเจ้าหน้าที่อยู่ห้อง 2. มีระบบแสกนลายนิ้วมือเพื่อเปิดเข้าห้อง Server 3. มีการติดตั้งกล้องวงจรปิด
10.8 Civil Unrest – Protest, Mob	25			
		เมื่อมีการชุมนุมหรือเหตุจลาจล	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. จัดทำระบบ DR-Site 2. ดำเนินการตามแผน DRP 3. ดำเนินการตามแผน BCP

Patient Risks due to IT Errors/Misuse

เรื่อง	ระดับของความเสี่ยง	เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
11.1 Patient Risks due to IT Errors/Misuse	4			
		จุดอ่อนการใช้เทคโนโลยีที่ทำให้เกิดอันตรายต่อผู้ป่วย	ลดโอกาสที่จะเกิดเหตุการณ์	1. อบรมเจ้าหน้าที่ให้มีความรู้ด้านเทคโนโลยีสารสนเทศ นิยามและความสำคัญของการรู้สารสนเทศ

ตารางการจัดการความเสี่ยง (Risk Treatment Table)

ลำดับ	ความเสี่ยง (Risk)	ความรุนแรง (Impact)	โอกาสเกิด (Likelihood)	ระดับความเสี่ยง	วิธีการจัดการ (Treatment)	ผู้รับผิดชอบ	ระยะเวลา
1.	ระบบ HIS ล่ม	สูง	กลาง	สูง	จัดทำ DR Site และสำรองข้อมูลอัตโนมัติ	หัวหน้า IT	ภายใน 2570
2.	มัลแวร์/ไวรัสโจมตี	สูง	สูง	สูง	ติดตั้ง Endpoint Protection, อัปเดต Patch ระบบ	IT Support	ต่อเนื่อง
3.	การเข้าถึงข้อมูลผู้ป่วยโดยไม่ได้รับอนุญาต	สูง	กลาง	สูง	จำกัดสิทธิ์ผู้ใช้ตามบทบาท, Audit Log	Admin & Security	ต่อเนื่อง
4	ข้อมูลสูญหายจากฮาร์ดแวร์ชำรุด	กลาง	กลาง	กลาง	สำรองข้อมูลรายวัน, ตรวจสอบ Hardware	จพ.เครื่องคอมพิวเตอร์	รายวัน
5	ไฟฟ้าดับกระทันหัน	กลาง	สูง	กลาง	ติดตั้ง UPS และเครื่องปั่นไฟ	งานอาคารสถานที่	เสร็จแล้ว
6	การโจมตีจากภายนอก (DDoS)	สูง	ต่ำ	กลาง	ใช้ Firewall/IPS และระบบเฝ้าระวัง	Network Admin	2569
7	ความรู้ไม่เพียงพอของเจ้าหน้าที่	กลาง	สูง	กลาง	จัดอบรมความรู้ด้าน IT Security เป็นประจำ	HR ร่วมกับ IT	2569

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ชื่อกลุ่มงาน กลุ่มงานเทคโนโลยีสารสนเทศ **วันที่จัดทำ** 1 กุมภาพันธ์ 2568

เรื่อง	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
เครื่องแม่ข่าย (Server) ล่ม หรือมีปัญหา	- อุปกรณ์ในเครื่องแม่ข่ายเสียหาย	1. จัดทำ DR-Site ภายในโรงพยาบาล 2. จัดทำ DR-Site ต่างโรงพยาบาล 3. จัดหาระบบมอนิเตอร์สถานะ Server	กง.เทคโนโลยีสารสนเทศ	500,000 2,000,000 -	ปีงบประมาณ 2569 ปีงบประมาณ 2570 ปีงบประมาณ 2568
ระบบเครือข่ายล่มหรือมีปัญหา	- อุปกรณ์กระจายสัญญาณเสียหรือมีปัญหา - สาย Lan ที่เชื่อมต่อภายภายในมีปัญหา	1.จัดหา Switch สำรอง 2.ปรับปรุงระบบเครือข่าย (Main Switch) 3. ปรับปรุงสาย CAT5 เป็น CAT6 ทั้งหมด	กง.เทคโนโลยีสารสนเทศ	500,000 500,000	ปีงบประมาณ 2568 ปีงบประมาณ 2569
เครื่องคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงในหน่วยงานมีปัญหา	- เครื่องคอมพิวเตอร์มีปัญหา - เครื่องพิมพ์มีปัญหา	1. จัดหาคอมพิวเตอร์ทดแทนเครื่องที่ใช้งานเกิน 5 ปี และจัดหาเครื่องสำรองอย่างน้อย 5 ตัว 2. ทำแผนจัดหาอะไหล่สำรอง * อยู่ในแผนจัดหาวัสดุ ปี 2568 1.มีสำรอง 10 เครื่องจากการเช่า	กง.เทคโนโลยีสารสนเทศ	128,800 458,120	ปีงบประมาณ 2568 ปีงบประมาณ 2568

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ชื่อกลุ่มงาน กลุ่มงานเทคโนโลยีสารสนเทศ **วันที่จัดทำ** 1 กุมภาพันธ์ 2568

เรื่อง	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
ระบบปฏิบัติการมีปัญหา	- OS ในเครื่อง Server มีปัญหา - OS ในเครื่อง Client มีปัญหา	1. พัฒนาศักยภาพของบุคคลากรในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อดูแลและแก้ไขปัญหาได้ 2. ทำแผนจัดหาอะไหล่สำรอง * อยู่ในแผนจัดหาวัสดุ ปี 2568	กง.เทคโนโลยีสารสนเทศ	- 458,120	ปีงบประมาณ 2568 ปีงบประมาณ 2569
โปรแกรมสำหรับให้บริการทางการแพทย์ โปรแกรม HIS	- โปรแกรม HIS มีปัญหา ไม่สามารถใช้งานได้	1. พัฒนาศักยภาพของบุคลากรในกง.เทคโนโลยีสารสนเทศโดยการส่งไปอบรมเกี่ยวกับกำกับดูแลเครื่องแม่ข่าย (Server)	กง.เทคโนโลยีสารสนเทศ	30,000	ปีงบประมาณ 2569
การสำรองข้อมูลผิดพลาด	- ไม่ได้สำรองข้อมูล - พื้นที่ที่สำรองข้อมูลเต็ม - ข้อมูลมีการสูญหายหรือข้อผิดพลาด	1. แผนจัดทำระบบสำรองข้อมูลอัตโนมัติและลดระยะเวลาในการสำรองข้อมูล 2. มีการสุ่มตรวจสอบข้อมูลที่สำรองไว้ ทุก 1 เดือน 3. แผนจัดทำระบบแจ้งเตือนอัตโนมัติเมื่อฮาร์ดดิสก์ที่ใช้งานมาก 90%	กง.เทคโนโลยีสารสนเทศ	-	ปีงบประมาณ 2569
ระบบการสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ตไม่สามารถใช้งานได้	- อุปกรณ์กระจายสัญญาณเสียหรือมีปัญหา - สาย Fiber Optic เครือข่ายขาดหรือใช้งานไม่ได้	1. มีผู้ให้บริการอินเตอร์เน็ต อย่างน้อย 2 บริษัทที่ให้บริการในโรงพยาบาล	กง.เทคโนโลยีสารสนเทศ	15,600	ดำเนินการแล้ว
ผู้ให้บริการหยุด ให้บริการ	- ผู้ให้บริการระบบ Server หรือ Network หยุดให้การบริการ	1. พัฒนาศักยภาพของบุคคลากรในศูนย์คอมพิวเตอร์ให้สามารถดูแลระบบได้	กง.เทคโนโลยีสารสนเทศ	-	ปีงบประมาณ 2570

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ชื่อกลุ่มงาน กง.เทคโนโลยีสารสนเทศ **วันที่จัดทำ** 1 กุมภาพันธ์ 2568

เรื่อง	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
การเข้าถึงข้อมูลส่วนบุคคล	- ข้อมูลส่วนบุคคลรั่วไหล	1. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบายระเบียบ และแนวปฏิบัติแก่บุคลากรตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล 2.จัดทำนโยบายระเบียบและแนวปฏิบัติ ในการจัดการข้อมูลส่วนบุคคลรวมถึงทบทวนมาตรการและแนวปฏิบัติ	กง.เทคโนโลยีสารสนเทศ		ปีงบประมาณ 2568
การถูกโจมตีจากภายนอก	- เครื่องคอมพิวเตอร์ติดไวรัส	1. จัดหาโปรแกรมป้องกันไวรัส	กง.เทคโนโลยีสารสนเทศ	280,000	ดำเนินการแล้ว
อัคคีภัย	- ไฟไหม้เครื่องแม่ข่าย และ ไฟไหม้อุปกรณ์กระจายสัญญาณ	1. แผนอัคคีภัยของโรงยาบาล 2. จัดทำ DR-Site ภายในโรงพยาบาล 3. จัดทำ DR-Site ต่างโรงพยาบาล	กง.เทคโนโลยีสารสนเทศ	500,000 2,000,000 2,000,000	ปีงบประมาณ 2568 ปีงบประมาณ 2568 ปีงบประมาณ 2570
โจรกรรม – ลักขโมย	- การลักขโมย	1. จัดทำ DR-Site ภายในโรงพยาบาล 2. จัดทำ DR-Site ต่างโรงพยาบาล	กง.เทคโนโลยีสารสนเทศ	2,000,000 2,000,000	ปีงบประมาณ 2568 ปีงบประมาณ 2570