การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

ตุลาคม พ.ศ.2565

คำนำ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินงาน เป็นอุปสรรคต่อพันธกิจองค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม

เพื่อให้ผลการดำเนินงานขององค์กรเป็นไปตามวัตถุประสงค์และเป้าหมายที่วางไว้ และเพื่อให้เกิดการรับรู้ ตระหนัก และเข้าใจถึงความเสี่ยงด้านต่างๆ ที่เกิดขึ้นกับองค์กร โดยสามารถเลือกวิธีบริหารจัดการที่เหมาะสมในการลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ จึงได้นำหลักการ แนวคิด กระบวนการบริหารความเสี่ยง มาเป็นเครื่องมือในการพัฒนา ปลูกฝังให้เป็นส่วนหนึ่งของการดำเนินงานตามภารกิจ จนเป็นวัฒนธรรมองค์กร ก่อให้เกิดประโยชน์ต่อการบรรลุเป้าหมายการดำเนินงานขององค์กรต่อไป

งานเทคโนโลยีสารสนเทศ
คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

สารบัญ

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

การบริหารจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามา มีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยง จากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

1.2 คำจำกัดความและความหมายที่เกี่ยวข้องกับการบริหารความเสี่ยง

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

ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุของความเสี่ยงซึ่งจะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม 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 เพื่อสร้างคุณค่าเพิ่มให้กับองค์กรนอกเหนือจากแผนงานและโครงการที่ได้กำหนดไว้แล้ว

การควบคุมภายใน (Internal Control) หมายถึง กระบวนการปฏิบัติงานที่บุคลากรในองค์กร โดยคณะกรรมการบริหาร ผู้บริหารทุกระดับ และพนักงานทุกคนมีบทบาทร่วมกันในการจัดให้มีขึ้น เพื่อสร้าง ความเชื่อมั่นอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ของการควบคุมภายใน

การบริหารจัดการความเสี่ยง (Risk Management) หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ใน การบ่งชี้ 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 ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหาย ความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์และความต้องการของผู้มีผลประโยชน์ร่วม

1.4 ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้องค์กสามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิดความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

1) **เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี** การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ในการกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น
2) **สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร** การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ รวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานใน การตอบสนองต่อเป้าหมายและภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้
3) **ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด** การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบในเชิงลบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล
4) **เป็นเครื่องมือที่สำคัญในการบริหารงาน** การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงานและการตัดสินใจในด้านต่างๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของโรงพยาบาลโรงพยาบาลมหาราชนครเชียงใหม่เป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่องค์กร
5) **ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน** การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจ ในกลยุทธ์ วัตถุประสงค์ขององค์กร และระดับความเสี่ยงอย่างชัดเจน
6) **ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล** การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำและกิจกรรมที่มีความเสี่ยงสูง ย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ทรัพยากรแตกต่างกัน 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)*

1. **สภาพแวดล้อมภายในองค์กรด้านเทคโนโลยีสารสนเทศ (Internal Environment)** ได้แก่

- ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น เว็บไซต์คณะแพทยศาสตร์ และหน่วยงานในสังกัดคณะแพทยศาสตร์ ภายใต้อินเทอร์เน็ตโดเมน med.cmu.ac.th และฐานข้อมูลเว็บไซต์ดังกล่าว เป็นต้น
- ระบบฐานข้อมูลบริหารงานภายใน ได้แก่ ฐานข้อมูลระบบสารสนเทศโรงพยาบาล ระบบสารสนเทศทางการบริหาร และระบบสารสนเทศทางการศึกษา เป็นต้น
- ระบบให้บริการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์คณะแพทยศาสตร์ (Web Application Program) เป็นต้น

- อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์คณะแพทยศาสตร์ (Web Server) เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์คอมพิวเตอร์ (Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

2. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง (Objective Setting)

1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

2) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3) เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. การบ่งชี้หรือการระบุความเสี่ยง (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบ ผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

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** เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุม

ความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบ และมิติ โอกาสของความเสี่ยงที่จะเกิดขึ้น

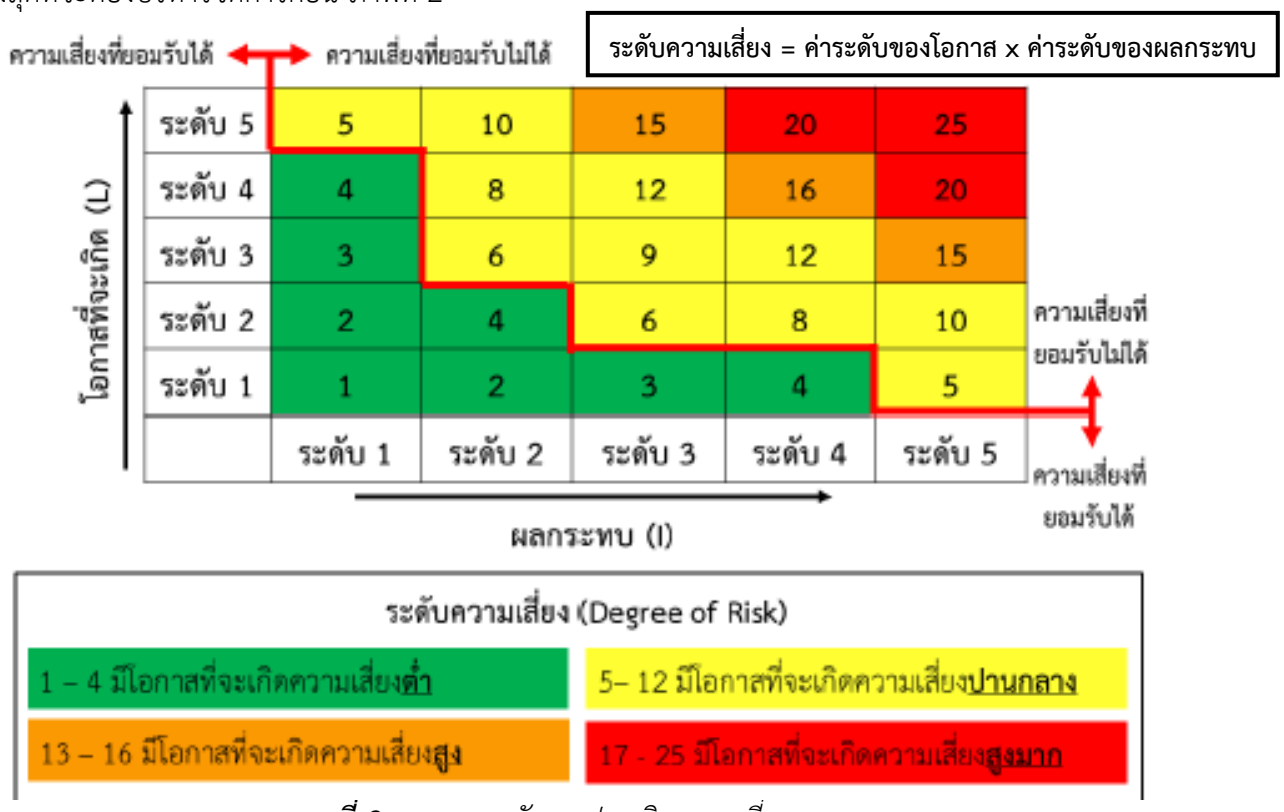
เกณฑ์การประเมินผลกระทบ มีดังนี้

ระดับ	การประเมิน
1	น้อยมาก
2	น้อย
3	ปานกลาง
4	สูง
5	สูงมาก

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง มีดังนี้

ระดับ	การประเมิน
1	โอกาสเกิดขึ้นน้อยมาก
2	โอกาสเกิดขึ้นน้อย
3	โอกาสเกิดขึ้นปานกลาง
4	โอกาสเกิดขึ้นสูง
5	โอกาสเกิดขึ้นสูงมาก

3) **การวิเคราะห์ความเสี่ยง** เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ภาพที่ 2



ภาพที่ 2 *แสดงแผนผังการประเมินความเสี่ยง*

4) **การจัดลำดับความเสี่ยง** เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

5. การตอบสนองความเสี่ยง (Risk Response)

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการ จะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

- **การหลีกเลี่ยง (Terminate/Avoidance)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะ ไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้
- **การยอมรับ (Take/Acceptance)** เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง
- **การควบคุมหรือการลด (Treat/Reduction)** เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิด ความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น
- **การถ่ายโอน (Transfer/Sharing)** การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

6. กิจกรรมการควบคุมความเสี่ยง (Control Activities)

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

- **ควบคุมเพื่อการป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้ เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึง เอกสาร เป็นต้น

- **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุมเพื่อค้น ข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น
- **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้น ให้เกิดความสำเร็จตามวัตถุประสงค์
- **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไข ข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก ใช้ขั้นตอนดังนี้
    - นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น
    - พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
    - ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

7. ข้อมูลสารสนเทศและการติดต่อสื่อสาร (Information & Communication)

เป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมินและการบริหารจัดการความเสี่ยง ดังนั้น โรงพยาบาลมหาราชนครเชียงใหม่ ได้รวบรวมและบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งภายนอก และภายใน ตลอดจนเปิดเผยและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

8. การติดตาม (Monitoring)

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธี ซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลดการควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดย พิจารณาจาก

1) พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

3) กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

4) ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ มาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุ วัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยง ด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหาร เพื่อทราบและสั่งการ

2.2 ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

งานเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็น 8 ประเภท ดังนี้

1) **ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)**

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2) **ความเสี่ยงด้านบุคลากร (Human Risk)**

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

3) **ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)**

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือ จากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

4) **ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)**

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัปเดตให้ทันสมัยเพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งคณะฯ อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

5) **ความเสี่ยงด้านระบบข้อมูล (Database Risk)**

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญเนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและ เทคโนโลยี

2.3 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของงานเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ รายละเอียดดังนี้

ปัจจัยภายนอก ได้แก่

- ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ
- การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)
- ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง
- ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ
- การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

ปัจจัยภายใน ได้แก่

- ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร
- เจ้าหน้าที่หรือบุคลการของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ
- อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

2.4 การประเมินความเสียหาย

ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่การถูกเจาะเข้าระบบ ฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

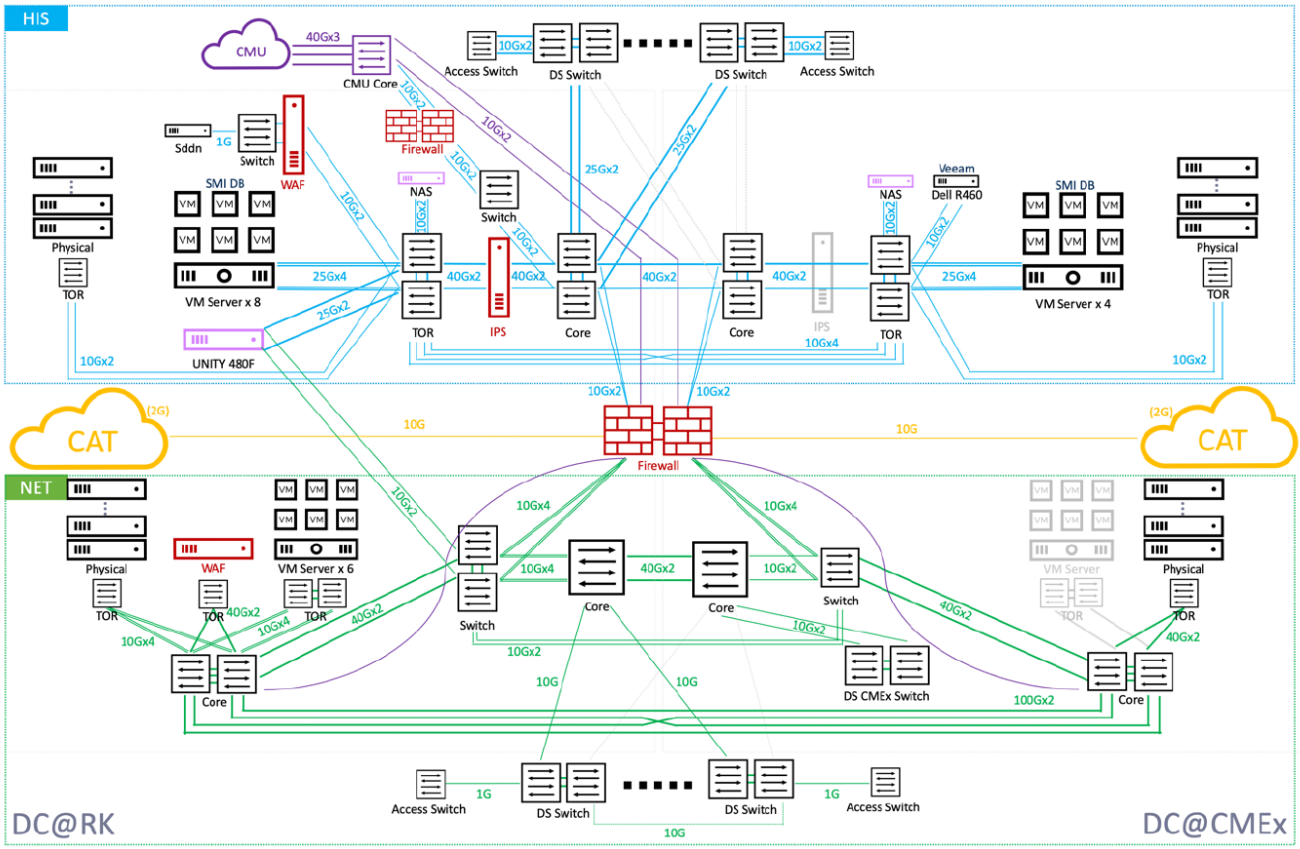
2.5 ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และเครือข่ายเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ตั้งอยู่ที่งานเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ชั้น M อาคารเรียนรวมราชนครินทร์ ที่อยู่ 110 ถนนอินทวโรส ตำบลศรีภูมิ อำเภอเมือง จังหวัดเชียงใหม่

ระบบคอมพิวเตอร์และเครือข่าย คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวดเป็นไปตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems : ISMS) โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย ในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการควบคุม (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ควบคุมและคัดกรอง (Filter Package) ข้อมูลที่ผ่านเข้ามาภายในระบบเครือข่ายคณะฯ โรงพยาบาล และจากเครือข่ายภายนอก เช่น เครือข่ายของมหาวิทยาลัย เครือข่ายอินเทอร์เน็ต เครือข่ายโรงพยาบาล ด้าน Website หรือ Web Application มีการกำหนดมาตรการควบคุมผ่านอุปกรณ์ Web Application Firewall (WAF) เพื่อใช้ในการ

ควบคุมและคัดกรองข้อมูลที่ผ่านเข้ามาในระบบเครือข่าย ส่วน Database HIS มีการกำหนดมาตรการควบคุมผ่านอุปกรณ์ Intrusion Prevention System (IPS) เพื่อใช้ในการควบคุมและคัดกรองข้อมูลที่ผ่านเข้ามาในระบบเครือข่าย เครื่องแม่ข่ายและเครื่องลูกข่ายมีการติดตั้งโปรแกรมระบบปฏิบัติการและป้องกันไวรัสที่มีลิขสิทธิ์ถูกต้อง เครื่องแม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัย เช่น Firewall, WAF, IPS, Core Switch ทั้งหมดส่ง Log และ Event มาที่ SIEM (Security Information and Event Management) เพื่อวิเคราะห์และค้นหาปัญหา ภัยคุกคาม หรือการโจมตีที่เกิดขึ้นในระบบคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของคณะแพทยศาสตร์ มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของคณะแพทยศาสตร์มีการทำ Network Segmentation โดยแบ่ง Subnet และ VLAN ให้เป็นกลุ่มย่อยเฉพาะกลุ่ม ทั้งเครือข่ายของคณะฯ และโรงพยาบาล เพื่อเพิ่มความปลอดภัย โดยสามารถกำหนด Security Profile ให้เหมาะสมกับกลุ่มย่อยได้ เห็นถึงพฤติกรรมของอุปกรณ์ในเครือข่ายที่ซับซ้อนได้งานขึ้น สามารถติดตาม จำกัดความเสียหายหรือการแพร่กระจายของภัยคุกคามให้อยู่ในวงจำกัดในกรณีเกิดปัญหาการใช้งาน สำหรับการใช้งานเครือข่ายคณะฯ เพื่อใช้งานอินเทอร์เน็ตจำเป็นจะต้องมีการยืนยันตัวตนก่อนเข้าใช้งาน การใช้งานเครือข่ายโรงพยาบาลต้องเป็นเครื่องที่ลงทะเบียนการใช้งานกับงานเทคโนโลยีสารสนเทศเท่านั้น

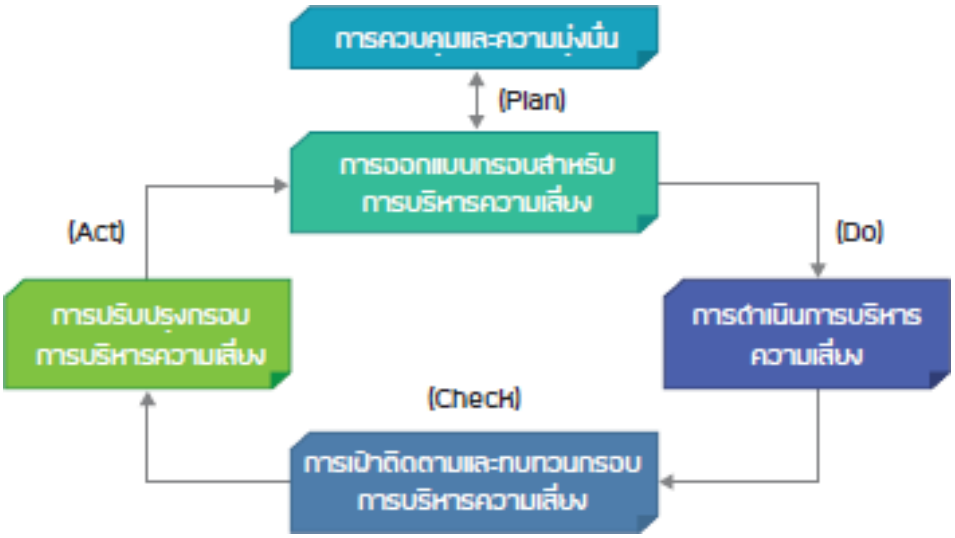
ระบบเครือข่ายหลักของคณะแพทยศาสตร์ (Core Network) เป็นศูนย์กลางการเชื่อมต่อระบบเครือข่ายภายในทั้งหมด โดยมี Firewall เป็นศูนย์กลางเชื่อมเครือข่ายคณะฯ และโรงพยาบาลเข้าด้วยกัน ความเร็วระหว่าง Core Switch ไปยัง Distribution Switch อยู่ที่ 10G และ 50G ตามลำดับ อุปกรณ์ถูกออกแบบและติดตั้งจำนวน 2 ชุดขึ้นไปและทำงานพร้อมกัน ทำให้ได้ประสิทธิภาพเต็มที่ เพื่อป้องกันเหตุระบบเครือข่ายไม่สามารถใช้งานได้ ลักษณะงานต้องรองรับการใช้งานแบบ 24x7 เพื่อให้ระบบสารสนเทศทั้งหมดใช้งานได้อย่างเต็มประสิทธิภาพ



ภาพที่ 3 *แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของคณะแพทยศาสตร์*

2.6 กรอบการบริหารจัดการความเสี่ยง

กรอบการบริหารจัดการความเสี่ยง (Framework for Managing Risk) ตามมาตรฐานการ บริหารจัดการความเสี่ยงสากล ISO 31000 แบ่งออกเป็น 4 ส่วน โดยขับเคลื่อนผ่านวงจร PDCA ประกอบด้วย 1) การวางแผน (Plan) 2) การลงมือทำ (Do) 3) การตรวจสอบ (Check) 4) การปรับปรุงแก้ไข (Act)



ภาพที่ 4 *กรอบการบริหารความเสี่ยง ตามมาตรฐาน ISO31000*

2.6.1 การออกแบบกรอบเพื่อการบริหารความเสี่ยง (Plan)

เป็นขั้นตอนการทำความเข้าใจสภาพแวดล้อมขององค์กร การบริหารความเสี่ยงขององค์กรจะเริ่มต้นจากการทำความเข้าใจในสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร โครงสร้างองค์กร การกำหนดนโยบายความต่อเนื่องทางธุรกิจ (Business continuity policy) รวมถึงวัตถุประสงค์ เป้าหมาย กระบวนการ และวิธีการปฏิบัติงานที่เกี่ยวข้องกับการจัดการกับความเสี่ยง เพื่อให้สามารถสร้างผลลัพธ์ที่สอดคล้องกับนโยบายและวัตถุประสงค์โดยรวมขององค์กร

2.6.2 การดำเนินการบริหารความเสี่ยง (Do)

การดำเนินการตามกรอบการบริหารความเสี่ยง จะเป็นการลงมือดำเนินการตามนโยบาย การควบคุม กระบวนการ และวิธีปฏิบัติ กำหนดช่วงเวลาและกลยุทธ์ที่เหมาะสมสำหรับการดำเนินการ การนำนโยบายและกระบวนการบริหารจัดการความเสี่ยงมาใช้ในกระบวนการต่างๆ การจัดทำเอกสาร การฝึกอบรม การสื่อสารองค์กร ดำเนินการเพื่อให้มั่นใจว่ากระบวนการบริหารความเสี่ยงต่างๆ ได้รับการนำไปปฏิบัติในทุกระดับและหน้าที่งานที่เกี่ยวข้องในองค์กร โดยเป็นส่วนหนึ่งของการปฏิบัติงานขององค์กรและกระบวนการทางธุรกิจ

2.6.3 การเฝ้าติดตามและทบทวนกรอบการบริหารความเสี่ยง (Check)

ในขั้นตอนนี้จะเป็นการประเมิน และการวัดผลการดำเนินงานของแต่ละกระบวนการ วัดความก้าวหน้าเทียบกับแผนการบริหารความเสี่ยงเป็นระยะๆ การทบทวนถึงกรอบการบริหารความเสี่ยง นโยบายและแผนงานอย่างสม่ำเสมอ การจัดทำรายงานความเสี่ยง ความก้าวหน้าของแผนการบริหารความเสี่ยง และการดำเนินการสอดคล้องกับนโยบายการบริหารความเสี่ยง การรายงานผลลัพธ์ที่ได้เพื่อนำไปสู่การทบทวนโดยฝ่ายบริหารต่อไป

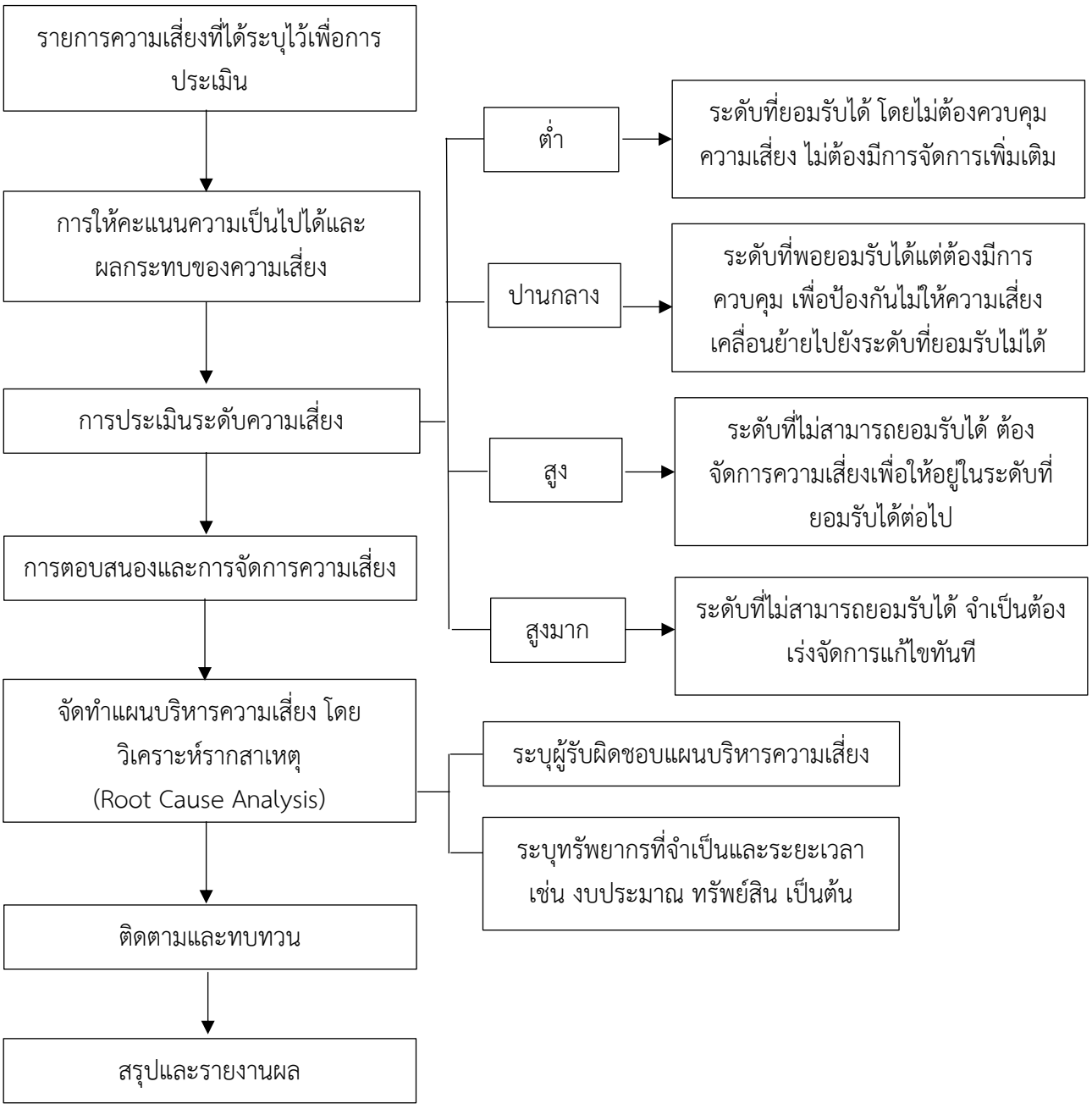
2.6.4 การปรับปรุงกรอบการบริหารความเสี่ยง (Act)

เป็นการดำเนินการปฏิบัติการแก้ไขและป้องกันจากผลของการทบทวน โดยฝ่ายบริหาร รวมถึงการดำเนินการปรับปรุงระบบการจัดการความเสี่ยง (Risk Management) ด้วย

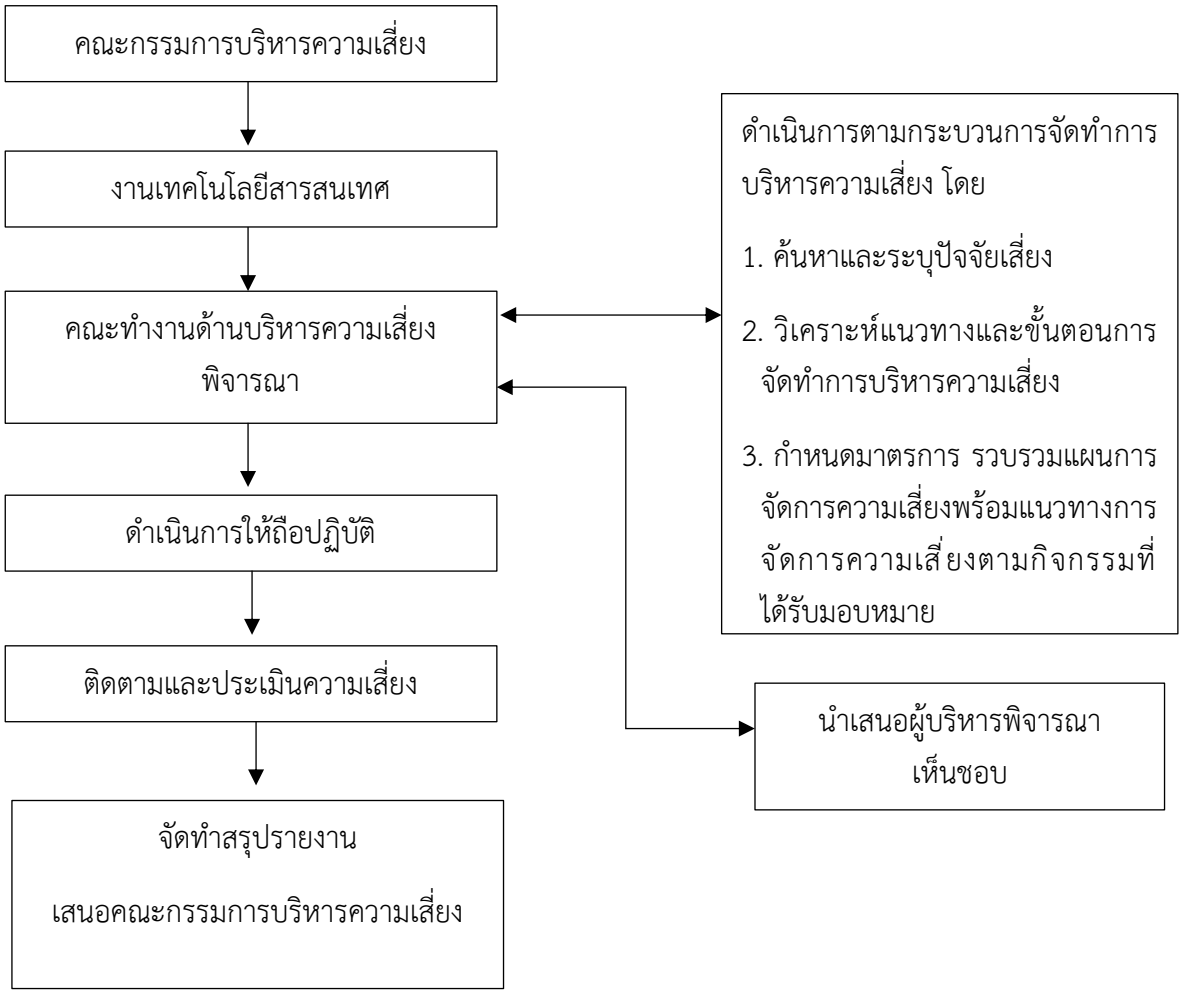
บทที่ 3
กระบวนการบริหารความเสี่ยง

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ งานเทคโนโลยีสารสนเทศจึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงาน ด้านกิจกรรมนั้นๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ ออกเป็นกิจกรรมต่างๆ ดังต่อไปนี้

3.1 แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



3.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้

3.3.1 ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) กำหนดเกณฑ์ไว้ 5 ระดับ ดังนี้

Likelihood Table

ระดับโอกาสเกิด		โอกาสในการเกิด		
5	สูงมาก	โอกาสเกิดเหตุการณ์มากกว่า	1 ครั้ง ภายใน 30 วัน (1 เดือน)	มากกว่า 12 ครั้ง/ปี
4	สูง	โอกาสเกิดเหตุการณ์น้อยกว่าหรือเท่ากับ	1 ครั้ง ภายใน 30 วัน (1 เดือน)	12 ครั้ง/ปี
3	ปานกลาง	โอกาสเกิดเหตุการณ์อย่างน้อย	1 ครั้ง ภายใน 90 วัน (3 เดือน)	4 ครั้ง/ปี
2	น้อย	โอกาสเกิดเหตุการณ์อย่างน้อย	1 ครั้ง ภายใน 180 วัน (6 เดือน)	2 ครั้ง/ปี
1	น้อยมาก	โอกาสเกิดเหตุการณ์อย่างน้อย	1 ครั้ง ภายใน 365 วัน (1 ปี)	1 ครั้ง/ปี

3.3.2 ระดับความรุนแรงของผลกระทบ (Impact) กำหนดผลกระทบไว้ 4 ด้าน แต่ละด้านกำหนดเกณฑ์ไว้ 5 ระดับ ดังนี้

3.3.2.1 ผลกระทบเชิงปริมาณ ด้านการเงิน (Financial)

Financial Impact Table

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
5	สูงมาก	มีมูลค่าความเสียหาย > 6,000,000 บาท
4	สูง	มีมูลค่าความเสียหาย > 2,000,001 ≤ 6,000,000 บาท
3	ปานกลาง	มีมูลค่าความเสียหาย > 800,000 ≤ 2,000,000 บาท
2	น้อย	มีมูลค่าความเสียหาย > 300,000 ≤ 800,000 บาท
1	น้อยมาก	มีมูลค่าความเสียหาย ≤ 300,000 บาท

3.3.2.2 ผลกระทบเชิงคุณภาพ ด้านการดำเนินงานการให้บริการ (Operation)

Operation Impact Table

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
5	สูงมาก	การให้บริการหยุดชะงัก ใช้เวลาดำเนินการแก้ไข > 4 ชั่วโมง
4	สูง	การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน > 1 ชั่วโมง ≤ 4 ชั่วโมง
3	ปานกลาง	การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน > 30 นาที ≤ 1 ชั่วโมง
2	น้อย	การให้บริการยังดำเนินการได้ แต่มีแนวโน้มจะหยุดชะงัก ดำเนินการแก้ไขได้ภายใน > 15 ≤ 30 นาที
1	น้อยมาก	การให้บริการยังดำเนินการได้ แต่มีแนวโน้มจะหยุดชะงัก ดำเนินการแก้ไขได้ภายใน 15 นาที

3.3.2.3 ผลกระทบเชิงคุณภาพ ด้านภาพลักษณ์องค์กร (Reputation)

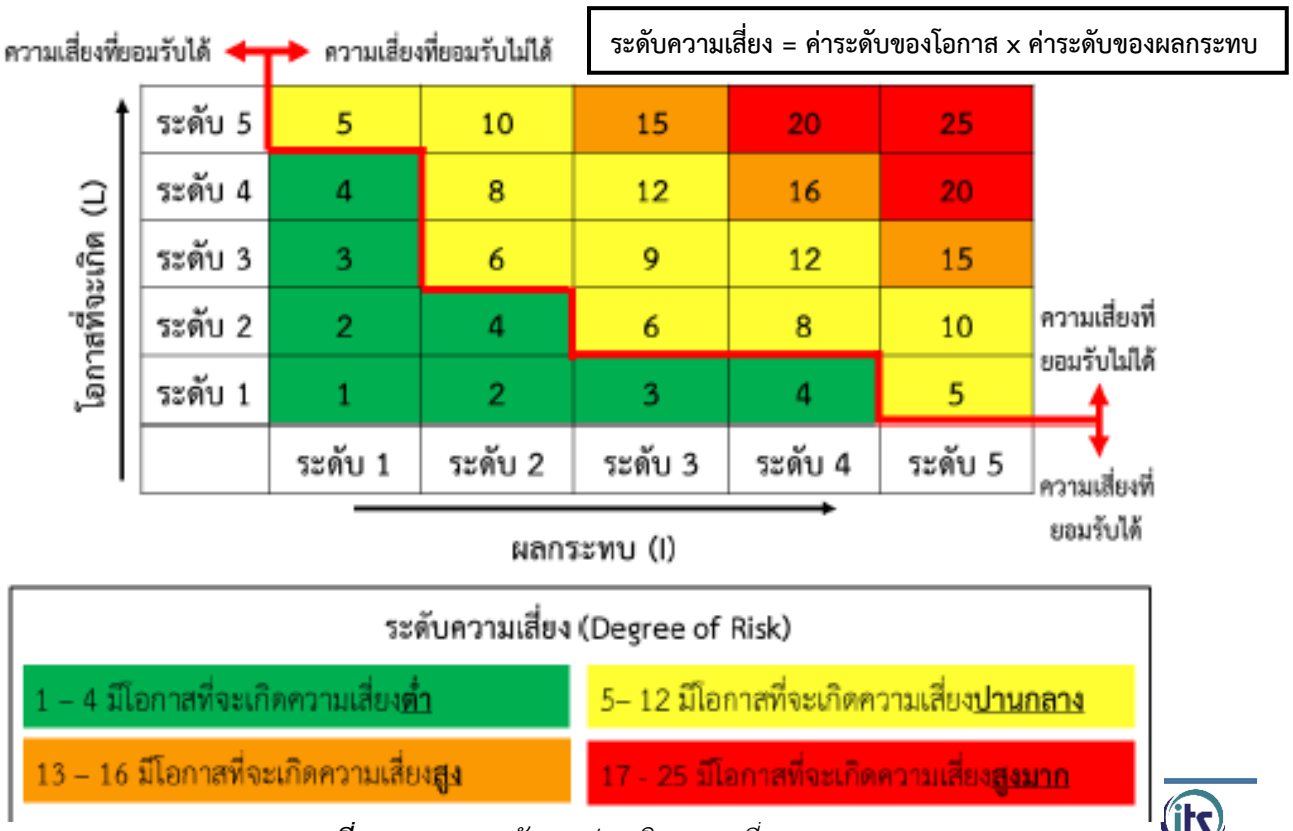
Reputation Impact Table

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
5	สูงมาก	มีการเผยแพร่ข่าวภายนอกมหาวิทยาลัยเชียงใหม่ และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัยเชียงใหม่
4	สูง	มีการเผยแพร่ข่าวทั่วทั้งมหาวิทยาลัยเชียงใหม่ และมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัยเชียงใหม่
3	ปานกลาง	มีการเผยแพร่ข่าวในระดับมหาวิทยาลัยเชียงใหม่ และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของมหาวิทยาลัยเชียงใหม่
2	น้อย	มีการเผยแพร่ข่าวในวงจำกัดภายในคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของคณะแพทยศาสตร์
1	น้อยมาก	มีการเผยแพร่ข่าวในวงจำกัดภายในงานเทคโนโลยีสารสนเทศ และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของคณะแพทยศาสตร์

3.3.2.4 ผลกระทบเชิงคุณภาพ ด้านพนักงาน (Employee)

Employee Impact Table

ระดับคะแนน	ระดับความรุนแรง	ผลกระทบ
5	สูงมาก	เกิดเหตุการณ์ ก่อให้เกิดการเสียชีวิต/สูญเสียอวัยวะ/ทุพพลภาพ
4	สูง	เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บสาหัส พักงาน > 1 เดือน
3	ปานกลาง	เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บ พักงาน ≤ 1 เดือน
2	น้อย	เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บเล็กน้อยหรือพักงาน ≤ 3 วัน
1	น้อยมาก	เกิดเหตุการณ์ แต่ไม่ก่อให้เกิดการบาดเจ็บ



ภาพที่ 5 *แสดงแผนผังการประเมินความเสี่ยง*

ตารางที่ 1 เกณฑ์การประเมินระดับความรุนแรงของความเสี่ยง

ระดับความเสี่ยง	ค่าความเสี่ยง (โอกาส x ผลกระทบ)	เกณฑ์การประเมิน
สูงมาก	17-25	อยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการแก้ไขทันที
สูง	13-26	อยู่ในระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ ยอมรับได้ต่อไป
ปานกลาง	5-12	ระดับที่พอยอมรับได้แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ	1-4	อยู่ในระดับที่ยอมรับได้ ไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ตารางที่ 2 รายละเอียดการประเมินในแต่ละประเด็นความเสี่ยง ปี พ.ศ.2565

ลำดับ	ประเด็นความเสี่ยง	โอกาสเกิด	ผลกระทบ (ผลลัพธ์คิดจากคะแนนสูงสุดที่ได้)				ระดับความเสี่ยง
			การเงิน (F)	การดำเนินงาน (O)	ภาพลักษณ์ (R)	พนักงาน (E)	
1	การบุกรุกโจมตีจากภายนอก	3	5	5	5	1	สูง 3x5=15
2	ไวรัสคอมพิวเตอร์/Malware	3	4	3	2	1	ปานกลาง 3x4=12
3	การถูกโจรกรรมฐานข้อมูล	2	5	5	5	1	ปานกลาง 2x5=10
4	การถูกโจมตีเครื่องแม่ข่าย (Server) ทำให้ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	2	5	4	4	**1**	ปานกลาง 2x5=10
5**	การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)	2	4	1	4	1	ปานกลาง 2x4=8
6	การไม่สามารถใช้งานโปรแกรม (Software) ข้อมูลหลักของโรงพยาบาล (ระบบสารสนเทศโรงพยาบาล HIS) ได้	2	2	3	2	1	ปานกลาง 2x3=6
7	เจ้าหน้าที่ใช้คอมพิวเตอร์/ระบบเครือข่ายผิดวัตถุประสงค์	2	3	1	1	1	ปานกลาง 2x3=6
8	การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์	3	1	1	2	1	ปานกลาง 3x2=6
9	ระบบกระแสไฟฟ้าขัดข้อง	3	1	1	2	1	ปานกลาง 3x2=6
10	ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	1	2	**1**	5	**1**	ปานกลาง 1x5=5
11	อัคคีภัย	1	5	4	2	1	ปานกลาง 1x5=5
12	แผ่นดินไหว	1	5	5	3	3	ปานกลาง 1x5=5
13	อุทกภัย	1	5	3	3	1	ปานกลาง 1x5=5
14	แมลงหรือสัตว์กัดแทะอุปกรณ์คอมพิวเตอร์ หรือสายไฟฟ้า/สายสัญญาณ	1	5	4	2	1	ปานกลาง 1x5=5
15	การไม่สำรองข้อมูล/การสำรองข้อมูลขาดการอัปเดต	2	2	2	2	1	ต่ำ 2x2=4

ลำดับ	ประเด็นความเสี่ยง	โอกาสเกิด	ผลกระทบ (ผลลัพธ์คิดจากคะแนนสูงสุดที่ได้)				ระดับความเสี่ยง
			การเงิน (F)	การดำเนินงาน (O)	ภาพลักษณ์ (R)	พนักงาน (E)	
16**	การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	2	2	2	2	1	ต่ำ 2x2=4
17	ระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1	2	3	2	1	ต่ำ 1x3=3
18**	การใช้ Wireless เข้าเครือข่ายอินทราเน็ตทั้งหมด	1	2	1	1	1	ต่ำ 1x2=2
19	การเชื่อมต่อระบบอินเทอร์เน็ต/อินทราเน็ตขัดข้อง	1	2	**1**	**2**	**1**	ต่ำ 1x2=2
20	มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1	2	**1**	**1**	**1**	ต่ำ 1x2=2
21**	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	1	2	**1**	**1**	**1**	ต่ำ 1x2=2
22	การถูก Black List จาก Search Engine	1	2	**1**	**1**	**1**	ต่ำ 1x2=2

ตารางที่ 3 เปรียบเทียบการประเมินความเสี่ยง พ.ศ.2563 ถึง พ.ศ.2566

ลำดับ	ประเด็นความเสี่ยง	ระดับความเสี่ยง			
		ปี 2563	ปี 2564	ปี 2565	ปี 2566
1	การบุกรุกโจมตีจากภายนอก	สูงมาก 4x5=20	สูงมาก 4x5=20	สูง 3x5=15	สูง 3x5=15
2	ไวรัสคอมพิวเตอร์/Malware	สูง 4x4=16	สูง 4x4=16	ปานกลาง 3x4=12	ปานกลาง 3x4=12
3	การถูกโจรกรรมฐานข้อมูล	สูง 3x5=15	ปานกลาง 2x5=10	ปานกลาง 2x5=10	ปานกลาง 2x5=10
4	การถูกโจมตีเครื่องแม่ข่าย (Server) ทำให้ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	สูง 3x5=15	ปานกลาง 2x5=10	ปานกลาง 2x5=10	ปานกลาง 2x5=10
5*	การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)	N/A	N/A	ปานกลาง 2x4=8	ปานกลาง 2x4=8
6	การไม่สามารถใช้งานโปรแกรม (Software) ข้อมูลหลักของโรงพยาบาล (ระบบสารสนเทศโรงพยาบาล HIS) ได้	ปานกลาง 3x3=9	ปานกลาง 2x3=6	ปานกลาง 2x3=6	ปานกลาง 2x3=6
7	เจ้าหน้าที่ใช้คอมพิวเตอร์/ระบบเครือข่ายผิดวัตถุประสงค์	ปานกลาง 3x3=9	ปานกลาง 2x3=6	ปานกลาง 2x3=6	ปานกลาง 2x3=6
8	การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์	ปานกลาง 3x2=6	ปานกลาง 3x2=6	ปานกลาง 3x2=6	ปานกลาง 3x2=6
9	ระบบกระแสไฟฟ้าขัดข้อง	ปานกลาง 4x2=8	ปานกลาง 4x2=8	ปานกลาง 3x2=6	ปานกลาง 3x2=6

ลำดับ	ประเด็นความเสี่ยง	ระดับความเสี่ยง			
		ปี 2563	ปี 2564	ปี 2565	ปี 2566
10	ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	ปานกลาง 2x5=10	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5
11	อัคคีภัย	ปานกลาง 2x5=10	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5
12	แผ่นดินไหว	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5
13	อุทกภัย	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5
14	แมลงหรือสัตว์กัดแทะอุปกรณ์คอมพิวเตอร์ หรือสายไฟฟ้า/สายสัญญาณ	ปานกลาง 2x5=10	ปานกลาง 1x5=5	ปานกลาง 1x5=5	ปานกลาง 1x5=5
15	การไม่สำรองข้อมูล/การสำรองข้อมูลขาดการอัปเดต	ปานกลาง 3x2=6	ต่ำ 2x2=4	ต่ำ 2x2=4	ต่ำ 2x2=4
16**	การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	N/A	ปานกลาง 3x2=6	ต่ำ 2x2=4	ต่ำ 2x2=4
17	ระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	ปานกลาง 2x3=6	ต่ำ 1x3=3	ต่ำ 1x3=3	ต่ำ 1x3=3
18**	การใช้ Wireless เข้าเครือข่ายอินทราเน็ตทั้งหมด	N/A	ต่ำ 1x2=2	ต่ำ 1x2=2	ต่ำ 1x2=2
19	การเชื่อมต่อระบบอินเทอร์เน็ต/อินทราเน็ตขัดข้อง	ปานกลาง 3x2=6	ต่ำ 1x2=2	ต่ำ 1x2=2	ต่ำ 1x2=2
20	มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	ต่ำ 2x2=4	ต่ำ 1x2=2	ต่ำ 1x2=2	ต่ำ 1x2=2
21**	การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	N/A	ต่ำ 1x2=2	ต่ำ 1x2=2	ต่ำ 1x2=2
22	การถูก Black List จาก Search Engine	ต่ำ 2x2=4	ต่ำ 1x2=2	ต่ำ 1x2=2	ต่ำ 1x2=2

หมายเหตุ: * คือ ความเสี่ยงที่เกิดขึ้นตั้งแต่ปี พ.ศ.2565

** คือ ความเสี่ยงที่เกิดขึ้นตั้งแต่ปี พ.ศ.2564

3.4 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
ความเสี่ยงสูง							
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร (Hardware and Data Communication Risk)	1. การบุกรุกโจมตีจากภายนอก	1. เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	● ทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย ● ถูกแก้ไขหรือเปลี่ยน แปลงข้อมูล หรือรูปภาพ บน Web Site ของคณะแพทยศาสตร์ ● ถูกโจรกรรมข้อมูลที่ เป็นความลับ	สูง 3x5=15	1. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย 2. จัดทำแผนหรือขั้นตอนการปฏิบัติที่จำเป็น เพื่อป้องกันการถูกบุกรุกตามลำดับ 3. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	การลดความเสี่ยง (Reduction)	หน่วยระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
ความเสี่ยงปานกลาง							
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร (Hardware and Data Communication Risk)	1. จากการติดไวรัสคอมพิวเตอร์หรือ Malware	1. โปรแกรมหรือข้อมูล ถูกทำลาย 2. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3. การถูกขโมยข้อมูล	● ใช้คอมพิวเตอร์ไม่ได้ ● ใช้ระบบงานไม่ได้ ● ข้อมูลที่สำคัญสูญหาย	ปานกลาง 3x4=12	1. ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์กับเครื่องแม่ข่าย และเครื่องลูกข่าย ทุกเครื่อง 2. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ	การลดความเสี่ยง (Reduction)	หน่วยระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร	2. จากการถูกโจรกรรมฐานข้อมูล	1. เสี่ยงต่อการสูญหายของข้อมูล	● ข้อมูลสูญหาย ● สูญเสียรายได้	ปานกลาง 2x5=10	1. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย	การลดความเสี่ยง (Reduction)	หน่วยระบบเครือข่ายและความมั่นคง

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
(Hardware and Data Communication Risk)					2. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ		ปลอดภัยสารสนเทศ
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร (Hardware and Data Communication Risk)	3. จากการโจมตีเครื่องแม่ข่ายของคณะฯ ทำให้ไม่สามารถให้บริการได้ (Denial of Service-DoS)	1.โปรแกรมหรือข้อมูลถูกทำ-ลาย 2.ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3.การถูกขโมยข้อมูล	● ข้อมูลสูญหาย ● สูญเสียรายได้	ปานกลาง 2x5=10	1. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย 2. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ	การลดความเสี่ยง (Reduction)	หน่วยระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
● ด้านบุคลากร (Human Risk)	4. การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA)	การดำเนินการที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	● ข้อมูลส่วนบุคคลถูกละเมิดอาจก่อให้เกิดอันตรายทั้งต่อร่างกายหรือต่อทรัพย์สิน	ปานกลาง 2x4=8	1. แต่งตั้งคณะกรรมการอำนวยการ และคณะกรรมการดำเนินการที่เกี่ยวข้องกับ พรบ. ข้อมูลส่วนบุคคล 2. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบาย ระเบียบ และแนวปฏิบัติแก่บุคลากร ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล 3. จัดทำนโยบาย ระเบียบ และแนวปฏิบัติ ในการ	การลดความเสี่ยง (Reduction)	หน่วยบริหารจัดการคุณภาพและความเสี่ยงด้าน IT

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					จัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการและแนวปฏิบัติ ปีละ 1 ครั้ง 4. พัฒนาสถาปัตยกรรมขององค์กร (Enterprise Architecture: EA) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถพิจารณาความเชื่อมโยงของระบบและข้อมูลได้ และสามารถตอบสนองได้หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น 5. พัฒนาความรู้ของบุคลากร ทั้งผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลส่วนบุคคล ให้เกิดการตระหนัก มีความรู้ และ		

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					ทักษะในการจัดการข้อมูลส่วนบุคคล 6. จัดให้มีการซ้อมกระบวนการตอบสนองในกรณีเกิดการละเมิดข้อมูลส่วนบุคคลขึ้นอย่างน้อย 1 ครั้งต่อปี		
● ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	5. จากการไม่สามารถใช้งานโปรแกรม (Software) ข้อมูลหลักของโรงพยาบาล (ระบบสารสนเทศโรงพยาบาล HIS)	1. เสี่ยงต่อการให้บริการระบบสำคัญหยุดชะงัก	● ผู้ป่วยรอนาน ● ผู้ไม่พึงพอใจ ● การให้บริการหยุดชะงัก ● สูญเสียรายได้	ปานกลาง 2x3=6	ดำเนินการตามแผน Manual System	การลดความเสี่ยง (Reduction)	หน่วยสารสนเทศโรงพยาบาล
● ด้านบุคลากร (Human Risk)	6. เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1. เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การฟังวิทยุหรือดูโทรทัศน์ออนไลน์ เป็นต้น 2. การใช้ Resource ทำผิดกฎหมาย เช่น การ	● สูญเสีย Bandwidth ในเครือข่าย ทำให้ต้องจัดเพิ่ม Bandwidth ให้ มากขึ้นทุกๆ ปี ● อาจถูกร้องเรียนหรือ ฟ้องร้องจากบุคคลภายนอก	ปานกลาง 2x3=6	1. บริหารจัดการด้วยข้อแนะนำ Ten Ways to Protect Your Network From Insider Threats เพื่อลดความเสี่ยง	การลดความเสี่ยง (Reduction)	งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		ดาวน์โหลดโปรแกรม ภาพยนตร์หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น			2. กำหนด Policy ของ Firewall ให้ เหมาะสม อย่างสม่ำเสมอ เปิด Port เท่าที่จำเป็น 3. การมีข้อตกลงที่ผู้ใช้งานต้องเป็น ผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ไปใช้ในทางที่ผิด รวมถึงการบันทึก การใช้งานและรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา		
● ด้านกายภาพ และสิ่งแวดล้อม (Physical and Environment Risk)	7. จากการโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์	เสี่ยงต่อการสูญหายของอุปกรณ์คอมพิวเตอร์และข้อมูลที่มีความสำคัญ	● เสียงบประมาณในการจัดหาอุปกรณ์ ทดแทน ● เสียภาพลักษณ์ของคณะฯ	ปานกลาง 3x2=6	1. ควบคุมการเข้าออกอาคาร 2. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออกอาคารตลอดเวลา 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การลดความเสี่ยง (Reduction)	- งานเทคโนโลยีสารสนเทศ - งานอาคารสถานที่

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
● ด้านกายภาพ และสิ่งแวดล้อม (Physical and Environment Risk)	8. จากระบบกระแสไฟฟ้าขัดข้อง	1. ไม่สามารถใช้งานเครื่องแม่ข่าย และระบบเครือข่ายได้ 2. ความเสี่ยงต่อการ Crash ของเครื่อง แม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) และระบบฐานข้อมูล(RDBMS) เนื่องจาก เครื่องไม่ได้ถูกทำการShutdown อย่างเหมาะสม	● ข้อมูลเสียหาย ● ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูล เสียหาย ต้องมีการติดตั้งใหม่	ปานกลาง 3x2=6	1. ตรวจสอบระบบสำรองไฟฟ้า (UPS) 2. ตรวจสอบการทำงานของเครื่องกำเนิดไฟฟ้า (Electrical Generator)	การถ่ายโอนความเสี่ยง (Sharing)	- งานเทคโนโลยีสารสนเทศ - งานซ่อมบำรุง
● ด้านระบบข้อมูล (Database Risk)	9. ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	1. ข้อมูลที่สำคัญมีการรั่วไหล จากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือแผ่น DVD/ CD	● ข้อมูลที่อยู่ในชั้น ความลับรั่วไหล ทำให้ เสียหายต่อความเชื่อถือของคณะฯ ● ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้	ปานกลาง 1x5=5	มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้	การลดความเสี่ยง (Reduction)	- งานเทคโนโลยีสารสนเทศ
● ด้านกายภาพ และสิ่งแวดล้อม	10. จากการเกิดอัคคีภัย	1.คอมพิวเตอร์และเครือข่ายถูกทำลาย 2.ข้อมูลถูกทำลาย	● เสียงบประมาณใน การจัดหาระบบทดแทน	ปานกลาง 1x5=5	1. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	การลดความเสี่ยง (Reduction)	- งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
(Physical and Environment Risk)		3.การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	● การไม่สามารถใช้งาน ระบบระหว่างที่มีการ จัดหาระบบทดแทน		2. วางแผนจัดหาและติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง 3. มีแผนในการเคลื่อนย้ายอุปกรณ์ ตามลำดับความสำคัญ		- งานอาคารสถานที่
● ด้านกายภาพ และสิ่งแวดล้อม (Physical and Environment Risk)	11. จากการเกิดแผ่นดินไหว	1. ความเสียหายด้านโครงสร้างอาจทำลายระบบเครื่องและข้อมูล	● ไม่สามารถใช้ระบบงาน หรือข้อมูลได้เป็นปกติ	ปานกลาง 1x5=5	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน 2. จัดทำแผนสำรองฉุกเฉินเพื่อรับมือว่ามีขั้นตอนปฏิบัติอย่างไร และจะใช้เครื่องทดแทนจากที่ใดเพื่อ สามารถจะใช้งานได้อย่างต่อเนื่อง	การลดความเสี่ยง (Reduction)	- งานเทคโนโลยีสารสนเทศ - งานอาคารสถานที่
● ด้านกายภาพ และสิ่งแวดล้อม (Physical and Environment Risk)	12. จากการเกิดอุทกภัย	1. ความเสียหายของเครื่องคอมพิวเตอร์ และอุปกรณ์	● การให้บริการระบบขาดความต่อเนื่อง	ปานกลาง 1x5=5	1. มีแผนในการเคลื่อนย้ายอุปกรณ์ ตามลำดับความสำคัญ	การลดความเสี่ยง (Reduction)	- งานเทคโนโลยีสารสนเทศ - งานอาคารสถานที่

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
● ด้านกายภาพ และสิ่งแวดล้อม (Physical and Environment Risk)	13. จากแมลงหรือสัตว์กัดแทะอุปกรณ์คอมพิวเตอร์ หรือสายไฟฟ้า/สายสัญญาณ	1. เสี่ยงต่อการไม่สามารถใช้งานได้ปกติ	● เสียงบประมาณใน การซ่อมแซมหรือจัดหา ทดแทน ● ไม่สามารถให้บริการ ระบบได้อย่างต่อเนื่อง	ปานกลาง 1x5=5	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุด ทางเข้าตู้ Rack 2. ไม่นำอาหารหรือเครื่องดื่มมาทาน หรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การลดความเสี่ยง (Reduction)	- งานเทคโนโลยีสารสนเทศ - งานอาคารสถานที่
ความเสี่ยงต่ำ							
● ด้านระบบข้อมูล (Database Risk)	1. จากการไม่สำรองข้อมูล/การสำรองข้อมูลขาดการอัปเดต	1.เสี่ยงต่อการสูญหายของข้อมูลในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินงานได้ตามปกติ 2.เสี่ยงต่อการมีข้อมูลที่ ไม่ถูกต้องกับความเป็นจริง	● เสียค่าใช้จ่ายในการกู้คืนข้อมูล หรือการจัดทำ ขึ้นมาใหม่ ● ไม่สามารถนำข้อมูลที่มีอยู่ไปใช้งานได้ เนื่องจากขาดความมั่นใจในข้อมูล	ต่ำ 2x2=4	1. มีการบริหารจัดการในการทำการสำรองข้อมูล (Backup) เป็นประจำอย่างสม่ำเสมอ 2. มีการทดสอบการนำข้อมูลกลับคืนสู่ระบบ (Restore)	การยอมรับความเสี่ยง (Acceptance)	งานเทคโนโลยีสารสนเทศ
● ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	2. จากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	1.การสูญหายของ ข้อมูล 2.การถูกฟ้องร้อง เสื่อมเสียชื่อเสียง และความน่าเชื่อถือของคณะฯ	● การใช้งานอาจไม่ได้ประสิทธิภาพตามความสามารถของซอฟต์แวร์นั้นๆ	ต่ำ 2x2=4	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมาย มาใช้งานตามความจำเป็น 2 . การรณรงค์ขอความร่วมมือบุคลากรการใช้	การยอมรับความเสี่ยง (Acceptance)	งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
			● คณะฯ อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์ นั้นๆ ● ความไม่สะดวกหากไม่ใช้งานด้วยซอฟต์แวร์ที่ไม่จำเป็นต้องมีลิขสิทธิ์(Open Source)		งานซอฟต์แวร์ที่ถูกกฎหมาย		
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	3. จากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย	1.ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ 2.เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล	● การใช้งานระบบงาน ไม่สามารถใช้ได้ตามปกต	ต่ำ 1x3=3	1.ตรวจสอบระบบคอมพิวเตอร์แม่ ข่ายและสำรองฐานข้อมูล 2.จัดตั้งศูนย์สำรองข้อมูล (Backup Site)	การยอมรับความเสี่ยง (Acceptance)	หน่วยระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	4. จากการใช้ Wireless เข้าเครือข่ายอินทราเน็ต	เสี่ยงต่อผู้ที่ไม่มีสิทธิ์ เข้าถึงข้อมูลเข้าใช้ เครือข่ายอินทราเน็ต ผ่านทาง WiFi	● ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ประโยชน์ อันจะนำมาซึ่งการขาด ความเชื่อถือของคณะฯ	ต่ำ 1x2=2	1.ควบคุมการเข้าใช้เครือข่าย 2. เพิ่มความปลอดภัยในการใช้งาน เพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)	การยอมรับความเสี่ยง (Acceptance)	หน่วยระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
● ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	5. จากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ตขัดข้อง	1.ไม่สามารถใช้งานระบบงานของคณะฯ ผ่านเครือข่ายอินทราเน็ตได้	● ขัดขวางการปฏิบัติงานของผู้บริหารงาน และเจ้าหน้าที่	ต่ำ 1x2=2	ตรวจสอบระบบเครือข่ายสื่อสารหลัก	การยอมรับความเสี่ยง (Acceptance)	หน่วยระบบเครือข่ายและความมั่นคง

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
(Hardware and Data Communication Risk)		2. ไม่สามารถเชื่อมต่อภายนอกคณะฯ ผ่านเครือข่ายอินเทอร์เน็ตได้	● บุคคลภายนอกไม่ สามารถเข้าใช้ Web Server หรือค้นหาข้อมูลที่ต้องการได้				ปลอดภัยสารสนเทศ
● ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	6. มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร	1. การถูกขโมยข้อมูล 2. โปรแกรมเสียหาย 3. การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง	● ลดความน่าเชื่อถือต่อ คณะฯ หากข้อมูลถูก ขโมยไปและนำไปเผยแพร่ ● กรณีที่เป็นข้อมูลลับ อาจสร้างความเสียหาย ต่อคณะฯ เป็นอย่างยิ่ง	ต่ำ 1x2=2	1. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง 2. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ 3. ตรวจสอบช่องโหว่ และดำเนินการปิดช่องโหว่	การยอมรับความเสี่ยง (Acceptance)	งานเทคโนโลยีสารสนเทศ
● ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	7. การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง	1. เสี่ยงต่อการถูก ขโมยข้อมูล 2.เสี่ยงต่อการทำความเสียหายแก่ โปรแกรม 3.ไม่สามารถแก้ไขข้อบกพร่องได้เอง	● ลดความน่าเชื่อถือต่อ คณะฯ หากข้อมูลถูก ขโมยไปและนำไปเผยแพร่ ● กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหาย ต่อคณะฯ เป็นอย่างยิ่ง	ต่ำ 1x2=2	1. การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level 2. การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล ER Diagram	การยอมรับความเสี่ยง (Acceptance)	งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
		4. ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว 5. เสียค่าใช้จ่ายสูง	● จัดหางบประมาณ เพื่อทำการบำรุงรักษา โปรแกรมและข้อมูล พร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการ อัปเดตอยู่ เสมอ		3. ให้มีการส่งมอบ Source Code ในรูปแบบอิเล็กทรอนิกส์ไฟล์ ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้ 4. หากมีการพัฒนา Library ด้วย ตนเอง ต้องส่ง Source Code Library ที่สามารถแก้ไขได้ 5. มีการถ่ายทอดความรู้เทคโนโลยี ในการพัฒนาระบบให้กับเจ้าหน้าที่ 6. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม 7. จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง		

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					8. มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัปเดต เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น		
● ด้านบุคลากร (Human Risk) ● ด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware and Data Communication Risk)	8. ความเสี่ยงจากการถูก Black List โดย Search Engine	1.ผู้ใช้งานที่ต้องการ ข้อมูลของคณะฯ หรือประชาชนทั่วไปไม่สามารถเข้าใช้งาน Web Server ได้ 2. ไม่สามารถใช้งานเครือข่ายได้	● ลดความน่าเชื่อถือ หรือข้อมูลของคณะฯ ● คณะฯ อาจถูก ฟ้องร้องโดยผู้มีส่วนได้ส่วนเสีย	ต่ำ 1x2=2	1. ติดตั้งโปรแกรมเพื่อตรวจสอบให้แน่ใจว่าไม่มีอุปกรณ์ใดในเครือข่ายคณะฯ ได้ส่ง Spam ออกไปยังเครือข่ายอินเทอร์เน็ต 2. ติดตั้งระบบการตรวจสอบแฟ้มข้อมูลก่อนการอัปโหลดข้อมูลขึ้น Web Server หรือ FTP Server	การยอมรับความเสี่ยง (Acceptance)	หน่วยระบบเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประเภทความเสี่ยง	ความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	กิจกรรมควบคุม	วิธีจัดการความเสี่ยง	ผู้รับผิดชอบ
					3. มีการอัปเดตตัวโปรแกรมและ Signature อย่างสม่ำเสมอ และการทำการบำรุงรักษา (Maintenance) ทั้งฮาร์ดแวร์และซอฟต์แวร์ พร้อมทั้ง Update		

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

งานเทคโนโลยีสารสนเทศ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่
ระดับความเสี่ยงที่จัดทำแผนการบริหารความเสี่ยง: ปานกลาง - สูง
วัตถุประสงค์: เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของคณะแพทยศาสตร์ บรรลุเป้าประสงค์ของการบริหารความเสี่ยง
ผู้รับผิดชอบ: งานเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
1. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก (ระดับ สูง)	1. ติดตั้งระบบตรวจจับป้องกัน และเตือนภัยการถูกบุกรุก - WAF - SIEM - SOAR			↔	↔							10 ล้านบาท	ระดับความเสี่ยงลดลง จาก 20 (สูงมาก) เหลือ 15 (สูง)
	2. จัดทำแผนหรือขั้นตอนการปฏิบัติที่จำเป็น เพื่อป้องกันการถูกบุกรุกตามลำดับ	ทุก 3 เดือน	↔	↔	↔	↔	↔	↔	↔	↔	↔		
	3. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย	ทุกวัน	↔	↔	↔	↔	↔	↔	↔	↔	↔		

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
2. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware (ปานกลาง)	ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์กับเครื่องแม่ข่าย และเครื่องลูกข่าย ทุกเครื่อง	ทุกครั้งที่ติดตั้งเครื่องใหม่	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 16 (สูง) เหลือ 12 (ปานกลาง)
	2.อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ	ทุกวัน	←	—	—	—	—	—	—	—	→		
3. ความเสี่ยงจากการถูกโจรกรรมฐานข้อมูล (ปานกลาง)	1.ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่ายทุกเครื่อง	ทุกครั้งที่ติดตั้งเครื่องใหม่	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 15 (สูง) เหลือ 10 (ปานกลาง)
	2.อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ	ทุกวัน	←	—	—	—	—	—	—	—	→		
4. ความเสี่ยงจากการโจมตี เครื่องแม่ข่ายของคณะฯ ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS) (ปานกลาง)	1.ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย	ทุกครั้งที่ติดตั้งเครื่องใหม่	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 15 (สูง) เหลือ 10 (ปานกลาง)
	2.อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ	ทุกวัน	←	—	—	—	—	—	—	—	→		

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
5. การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) (ปานกลาง)	1. แต่งตั้งคณะกรรมการอำนวยการ และคณะกรรมการดำเนินการ ที่เกี่ยวข้องกับ พรบ.ข้อมูลส่วนบุคคล	ทบทวนทุกปี	◂▸										ระดับความเสี่ยงยังคงอยู่ที่ระดับ 8 (ปานกลาง)
	2. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบาย ระเบียบ และแนวปฏิบัติ แก่บุคลากร ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล	ปีละ 1 ครั้ง		◂▸			◂▸			◂▸			
	3. จัดทำนโยบาย ระเบียบ และแนวปฏิบัติ ในการจัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการและแนวปฏิบัติ ปีละ 1 ครั้ง	ทบทวนทุกปี	◂▸			◂▸			◂▸				

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
	4. พัฒนาสถาปัตยกรรมขององค์กร (Enterprise Architecture: EA) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถเชื่อมโยงระบบและข้อมูลได้ และสามารถตอบสนองได้ หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น	ทุกครั้งที่มีการพัฒนาระบบ	←	—	—	—	—	—	—	—	→		
	5. พัฒนาความรู้ของบุคลากร ทั้งผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลส่วนบุคคล ให้เกิดการตระหนัก มีความรู้และทักษะในการจัดการข้อมูลส่วนบุคคล	พัฒนาอย่างต่อเนื่อง	←	—	—	—	—	—	—	—	→		

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
	6. จัดให้มีการซ้อมกระบวนการตอบสนองในกรณีเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น อย่างน้อย 1 ครั้งต่อปี	ปีละ 1 ครั้ง			◆▶			◆▶			◆▶		
6. การไม่สามารถใช้งานโปรแกรม (Software) ข้อมูลหลักของโรงพยาบาล (ระบบสารสนเทศโรงพยาบาล HIS) (ปานกลาง)	1. ดำเนินการตามแผน Manual System โดยซ้อมแผน ปีละ 1 ครั้ง	ปีละ 1 ครั้ง			◆▶			◆▶			◆▶		ระดับความเสี่ยงอยู่ที่ 6 (ปานกลาง)
7. เจ้าหน้าที่ใช้คอมพิวเตอร์/ เครือข่ายผิดวัตถุประสงค์ (ปานกลาง)	1. ให้ความรู้การใช้งานระบบคอมพิวเตอร์อย่างปลอดภัย	ปีละ 1 ครั้ง			◆▶			◆▶			◆▶		ระดับความเสี่ยงลดลง จาก 9 (ปานกลาง) เหลือ 6 (ปานกลาง)
	2. การมีข้อตกลงที่ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการนำอุปกรณ์เครื่องคอมพิวเตอร์ หรือ Resources ต่างๆ ไป	ตลอดเวลา	◀		▶								

ประเภทความเสี่ยง/กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
	ใช้ในทางที่ผิด รวมถึงการบันทึก การใช้งาน และรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา												
8. การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์ (ปานกลาง)	1. ควบคุมการเข้าออกอาคาร	ตลอดเวลา	←								→		ระดับความเสี่ยงอยู่ที่ระดับ 6 (ปานกลาง)
	2. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์	ตลอดเวลา	←								→		
	3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	ตลอดเวลา	←								→		
9. ระบบกระแสไฟฟ้าขัดข้อง (ปานกลาง)	1. ตรวจสอบระบบสำรอง ไฟฟ้า (UPS)	ทุกวัน	←								→		ระดับความเสี่ยงลดลง จาก 8 (ปานกลาง) เหลือ 6 (ปานกลาง)
	2. ตรวจสอบการทำงานของเครื่องกำเนิดไฟฟ้า (Electrical Generator)	ทุกวัน		←							→		

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
10. ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้ (ปานกลาง)	มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว	ตลอดเวลา	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 10 (ปานกลาง) เหลือ 5 (ปานกลาง)
11. อัคคีภัย (ปานกลาง)	1. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	ทุกวัน	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 10 (ปานกลาง) เหลือ 5 (ปานกลาง)
	2. ติดตั้งระบบตรวจจับควัน ระบบดับเพลิง และแจ้งเตือนการเกิดอัคคีภัย	ตลอดเวลา	←	—	—	—	—	—	—	—	→		
	3. จัดทำและซ้อมแผนสำรองฉุกเฉิน	ปีละ 1 ครั้ง		◆			◆			◆			
12. แผ่นดินไหว (ปานกลาง)	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน	ตลอดเวลา	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงอยู่ที่ระดับ 5 (ปานกลาง)
	2. จัดทำและซ้อมแผนสำรองฉุกเฉิน	ปีละ 1 ครั้ง		◆			◆			◆			
13. อุทกภัย (ปานกลาง)	จัดทำและซ้อมแผนสำรองฉุกเฉิน	ปีละ 1 ครั้ง		◆			◆			◆			ระดับความเสี่ยงอยู่ที่ระดับ 5 (ปานกลาง)

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2566			2567			2568			งบประมาณ	ผลลัพธ์ ความก้าวหน้า
			1-4	5-8	9-12	1-4	5-8	9-12	1-4	5-8	9-12		
14. แมลงหรือสัตว์กัดแทะอุปกรณ์คอมพิวเตอร์หรือสายไฟฟ้า/สายสัญญาณ	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack	ตลอดเวลา	←	—	—	—	—	—	—	—	→		ระดับความเสี่ยงลดลง จาก 10 (ปานกลาง) เหลือ 5 (ปานกลาง)
	2. ไม่นำอาหารหรือเครื่องดื่มมาทาน หรือเก็บไว้ในบริเวณที่มีความเสี่ยง	ตลอดเวลา	←	—	—	—	—	—	—	—	→		

บทที่ 4
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กร ลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในคณะแพทยศาสตร์ ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือสูญหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการความเสี่ยงในองค์กร นั่นเอง

1. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (**Risk identification**) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงในระดับสูงและปานกลาง ดังต่อไปนี้

ความเสี่ยง	แนวทางปฏิบัติ
1. การบุกรุกโจมตีจากภายนอก	1. ติดตั้งระบบเครือข่ายเพื่อป้องกัน และเตือนภัย (WAF, SIEM, SOAR)
	2. จัดทำแผนทบทวน ขั้นตอนปฏิบัติที่จำเป็นตามลำดับ
	3. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย
2. การติดไวรัสคอมพิวเตอร์หรือ Malware	1. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ
3. การถูกโจรกรรมฐานข้อมูล	1. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย
	2. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ
4. การโจมตี เครื่องแม่ข่ายของคณะฯ ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)	1. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย
	2. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ
5. การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)	1. แต่งตั้งคณะกรรมการอำนวยการ และคณะกรรมการดำเนินการ ที่เกี่ยวข้องกับ พรบ. ข้อมูลส่วนบุคคล
	2. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบาย ระเบียบ และแนวปฏิบัติ แก่บุคลากร ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล
	3. จัดทำนโยบาย ระเบียบ และแนวปฏิบัติ ในการจัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการและแนวปฏิบัติ ปีละ 1 ครั้ง

	4. พัฒนาสถาปัตยกรรมขององค์กร (Enterprise Architecture: EA) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถพิจารณาความเชื่อมโยงของระบบและข้อมูลได้ และสามารถตอบสนองได้ หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น
	5. พัฒนาความรู้ของบุคลากร ทั้งผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลส่วนบุคคล ให้เกิดการตระหนัก มีความรู้ และทักษะในการจัดการข้อมูลส่วนบุคคล
	6. จัดให้มีการซ้อมกระบวนการตอบสนองในกรณีเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น อย่างน้อย 1 ครั้งต่อปี
6. การไม่สามารถใช้งานโปรแกรม (Software) ข้อมูลหลักของโรงพยาบาล (ระบบสารสนเทศโรงพยาบาล HIS)	1. ดำเนินการตามแผน Manual System โดยซ้อมแผนปีละ 1 ครั้ง
7. เจ้าหน้าที่ใช้คอมพิวเตอร์/ เครือข่ายผิดวัตถุประสงค์	1. ให้ความรู้การใช้งานระบบคอมพิวเตอร์อย่างปลอดภัย
8. การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์	1. ควบคุมการเข้าออกอาคาร
	2. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์
	3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ที่มี เครื่องคอมพิวเตอร์และ อุปกรณ์ติดตั้งอยู่
9. ระบบกระแสไฟฟ้าขัดข้อง	1. ตรวจสอบระบบสำรอง ไฟฟ้า (UPS)
	2. ตรวจสอบการทำงานของเครื่องกำเนิดไฟฟ้า (Electrical Generator)
10. ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้	1. บริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้ว หากทำได้
11. การเกิดอัคคีภัย	1. ติดตั้งและตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง
	2. ติดตั้งระบบตรวจจับควัน ระบบ ดับเพลิง และการแจ้งเตือนการเกิดอัคคีภัย
	3. มีแผนในการเคลื่อนย้ายอุปกรณ์ ตามลำดับความสำคัญ
12. การเกิดแผ่นดินไหว	1. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน
	2. จัดทำแผนสำรองฉุกเฉิน

13. การเกิดอุทกภัย	1. จัดทำแผนสำรองฉุกเฉิน
14. แมลงหรือสัตว์กัดแทะอุปกรณ์คอมพิวเตอร์ หรือ สายไฟฟ้า/สายสัญญาณ	1. ร้อยท่อสายไฟฟ้าหรือสายสัญญาณตลอดเส้นทาง จนถึงจุด ทางเข้าตู้ Rack
	2. ไม่นำอาหารหรือเครื่องดื่มมาทาน หรือเก็บไว้ในบริเวณที่มีความเสี่ยง

2. สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

- เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ
- เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศ ให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
- ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3. ข้อเสนอแนะ

- การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุม โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้
  1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน
  2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น
  3) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้
- การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ เป็นไปตามหลักการ PDCA