รายงานโครงการอบรมให้ความรู้เรื่อง
“ความรู้การบริหารความเสี่ยง สำนักงานสาธารณสุขอำเภอแม่ลาน้อย”
วันที่ ๒๗ ,๓๐ มกราคม ๒๕๖๖ เวลา ๐๘.๓๐ น. –๑๖.๓๐ น.
ณ ห้องประชุม สำนักงานสาธารณสุขอำเภอแม่ลาน้อย

ผู้เข้ารับการอบรม

บุคลากรในสังกัดสำนักงานสาธารณสุขอำเภอแม่ลาน้อย ๗๔ คน

- ข้าราชการ จำนวน ๓๕ คน
- พนักงานราชการ จำนวน ๑ คน
- พนักงานกระทรวงสาธารณสุข จำนวน ๑๑ คน
- ลูกจ้างประจำ จำนวน ๒ คน
- ลูกจ้างเหมา จำนวน ๒๕ คน

กำหนดการประชุมประชุมวิชาการฟื้นฟูความรู้การบริหารความเสี่ยง สำนักงานสาธารณสุขอำเภอแม่ลาน้อย วันที่ ๒๗ , ๓๐ มกราคม ๒๕๖๖ ณ ห้องประชุมสำนักงานสาธารณสุขอำเภอแม่ลาน้อย

เวลา	รายละเอียดการประชุม	วิทยากร
๐๘.๓๐ น. – ๐๙.๐๐ น.	ลงทะเบียน	
๐๙.๐๐ น. – ๐๙.๑๕ น.	กล่าวเปิดประชุมวิชาการ	
๐๙.๑๕ น. – ๑๐.๓๐ น.	วิชาการการจัดการความเสี่ยง	นายบุญเลิศ
๑๐.๓๐ น. - ๑๐.๔๕ น.	รับประทานอาหารว่าง	
๑๐.๔๕ น. - ๑๒.๐๐ น.	ทบทวนการบันทึกความเสี่ยง ผ่านโปรแกรม HRMS	นายบุญเลิศ
๑๒.๐๐ น. - ๑๓.๐๐ น.	รับประทานอาหารกลางวัน	
๑๓.๐๐ น. - ๑๔.๓๐ น.	แบ่งกลุ่ม ทบทวนความเสี่ยง ทำ RCA	คกก.ความเสี่ยง
๑๔.๓๐ น. - ๑๔.๔๕ น.	รับประทานอาหารว่าง	
๑๔.๕๕ น. - ๑๖.๐๐ น.	นำเสนอการทบทวนความเสี่ยง	คกก.ความเสี่ยง
	ร่วมวางแนวทางการดำเนินการความเสี่ยง	
	สรุปข้อคิดเห็น	

การบริหารจัดการความเสี่ยงด้านสารสนเทศ
สำนักงานสาธารณสุขอำเภอแม่ลาน้อย

สำนักงานสาธารณสุขอำเภอแม่ลาน้อย เป็นหน่วยงานในสังกัดกระทรวงสาธารณสุข ซึ่งมีภารกิจในการดูแลรพ.สต.ต่างๆ ในอำเภอแม่ลาน้อย ตลอดจนการรวบรวมข้อมูลเพื่อใช้ในการนำเสนอสำนักงานสาธารณสุขจังหวัดแม่ฮ่องสอน การนำเทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานของสำนักงานฯ จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น การบริหารจัดการความเสี่ยงของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย โดยกลุ่มงานข้อมูลสารสนเทศและการสื่อสารมีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของสำนักงานฯ ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการ

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) **หมายถึง** เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) **หมายถึง** ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) **หมายถึง** กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) **หมายถึง** กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น ๔ แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) **หมายถึง** นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

๑. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
๒. การระบุความเสี่ยงต่าง ๆ (Event Identification)
๓. การประเมินความเสี่ยง (Risk Assessment)
๔. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
๕. กิจกรรมการบริหารความเสี่ยง (Control Activities)
๖. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
๗. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

วัตถุประสงค์

๑. เพื่อให้การจัดการภายในสำนักงานสาธารณสุขอำเภอแม่ลาน้อย มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

๒. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย

๓. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๕. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

สำนักงานสาธารณสุขอำเภอแม่ลาน้อย ได้กำหนดวัตถุประสงค์ให้สอดคล้องกับยุทธศาสตร์และทิศทางของจังหวัด โดยใช้หลัก SMART (ชัด-วัด-ปฏิบัติ-สม-เวลา)

- Specific = ชัดเจน
- Measurable = วัดได้
- Achievable = ปฏิบัติได้
- Reasonable = สมเหตุสมผล
- Time Constrained = มีกรอบเวลา

ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของกลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานสาธารณสุขอำเภอแม่ลาน้อย

การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย สามารถแยกประเภทความเสี่ยงด้านเป็น ๔ ประเภท ดังนี้

- **ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น
- **ความเสี่ยงจากผู้ปฏิบัติงาน** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
- **ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน** เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
- **ความเสี่ยงด้านการบริหารจัดการ** เป็นความเสี่ยงจากการวางแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
๒. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
๓. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่าย คอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๔. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๔	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๕. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๖. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๗. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
๘. ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
๙. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งสำนักงานสาธารณสุขอำเภอแม่ลาน้อย ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	๕ ครั้ง/ปี
๔	สูง	๔ ครั้ง/ปี
๓	ปานกลาง	๓ ครั้ง/ ปี
๒	น้อย	๒ ครั้ง/ปี
๑	น้อยมาก	ไม่เกิน ๑ ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	> ๑๐ ล้านบาท หรือ เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	> ๕ แสนบาท – ๑๐ ล้านบาท หรือ เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	> ๒.๕ แสนบาท – ๕ แสนบาท หรือ ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	> ๑ แสนบาท – ๒.๕ แสนบาท หรือ เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน ๑๐๐,๐๐๐ บาท หรือ เกิดเหตุร้ายที่ไม่มีความสำคัญ

การประมาณความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๑.ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล / เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล	๕	๔
๒.ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายสำนักงานสาธารณสุขอำเภอแม่ลาน้อย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย	๕	๓

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๓.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดันไฟฟ้าไม่คงที่	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๒
๔.ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๔	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- แฮ็คเกอร์ - แคร็กเกอร์ - การโจมตีการให้บริการ (denial of services/ DOS) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม - ไวรัส/เวิร์ม	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๒	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๕.ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔
๖.ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ		ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๑
๗.ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ		ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ	๕	๔

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ	ความถี่	ความรุนแรง
๘.ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ	๑	๕
๙.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การชุมนุมประท้วง - การจลาจล - การก่อการร้าย	ผู้ใช้งาน ผู้ดูแลระบบ	๑	๒
๑๐. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	- ความล้มเหลวทางเทคนิค - สัตว์กัดแทะประเภทหนู หรือแมลง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๓	๔
๑๑. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- การลักทรัพย์	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย	๑	๕

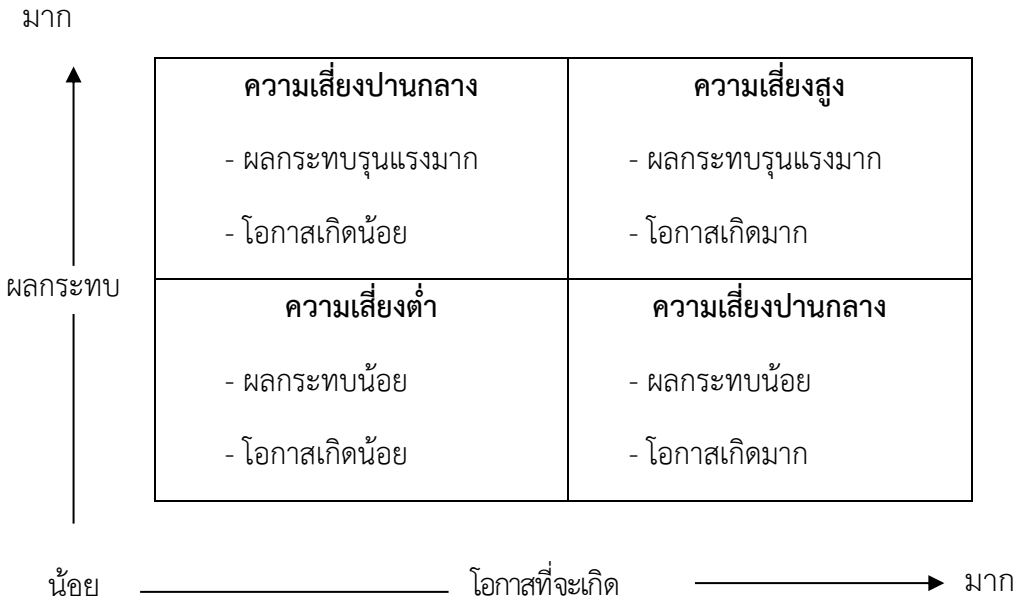
การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนด แผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ x ความรุนแรงของเหตุการณ์ต่างๆ ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

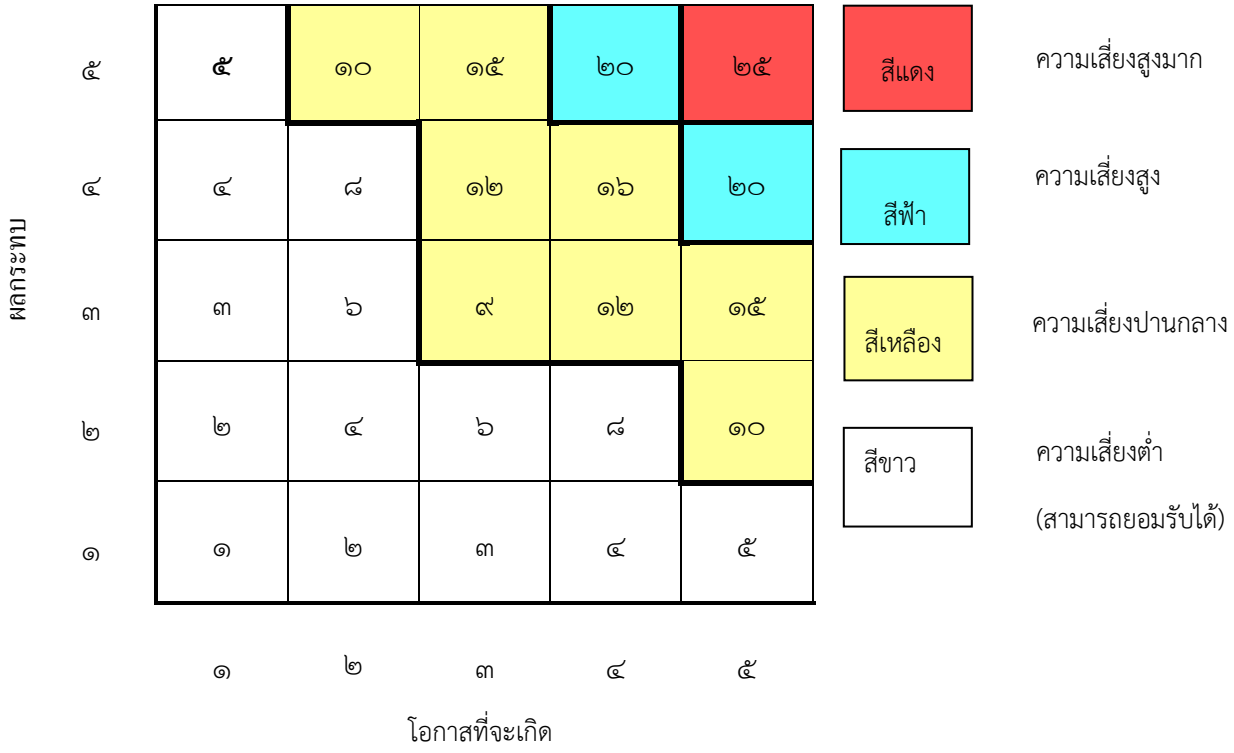
ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ – ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙ – ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ – ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



การประเมินความเสี่ยง



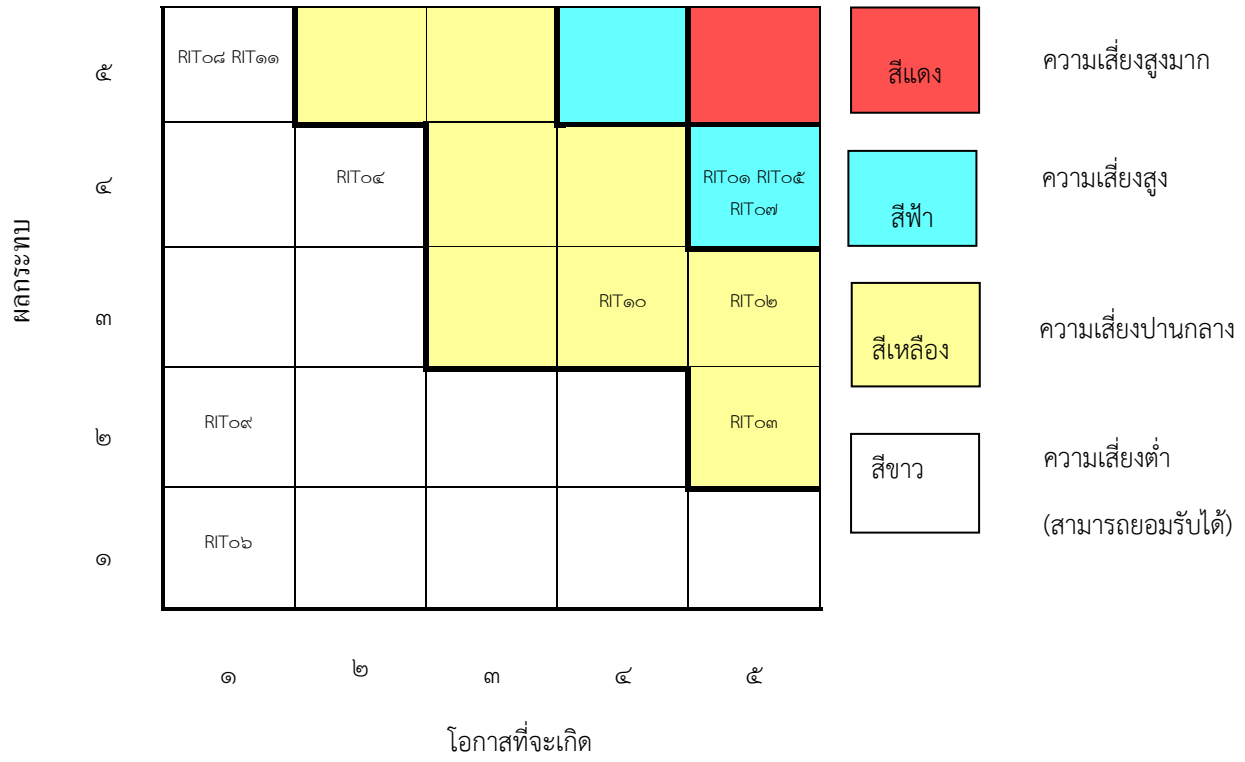
การประเมินค่าความเสี่ยงแสดงดังตารางต่อไปนี้

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๑.ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RIT๐๑	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๕	๔	๒๐
๒.ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RIT๐๒	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่าย สำนักงานสาธารณสุขอำเภอแม่ลาน้อย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย ทำให้เกิดช่องโหว่กับระบบรักษา	๕	๓	๑๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
			ความปลอดภัยของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย			
๓.ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับแรงดันไฟฟ้าไม่คงที่	RIT๐๓	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๕	๒	๑๐
๔.ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RIT๐๔	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	๒	๔	๘
๕.ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RIT๐๕	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๕	๔	๒๐
๖.ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RIT๐๖	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	๑	๑	๑
๗.ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RIT๐๗	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๕	๔	๒๐
๘.ความเสี่ยงจากการเกิดไฟไหม้ ผ่นดินไหว อาคารถล่ม	RIT๐๘	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	๑	๕	๕

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
๙.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RIT๐๙	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๑	๒	๒
๑๐.ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	RIT๑๐	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๓	๔	๑๒
๑๑.ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RIT๑๑	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๑	๕	๕

แผนภูมิความเสี่ยง



การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศ ในการบริหารจัดการได้อย่างมีประสิทธิภาพดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๒๐
๒	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๒๐
๓	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๒๐
๔	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายสำนักงานสาธารณสุขอำเภอแม่ลาน้อย โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่นๆที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย	๑๕
๕	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๑๒
๖	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้องไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๑๐

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๗	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	๘
๘	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	๕
๙	RIT๐๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๕
๑๐	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๒
๑๑	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	๑

การจัดการความเสี่ยง

นโยบายของสำนักงานสาธารณสุขอำเภอแม่ลาน้อย ระดับความเสี่ยงคงเหลือที่ยอมรับได้ ≤ ๙

สำนักงาน ก.พ.ร. กำหนดให้ ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๑๕ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๑๕ ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
๒	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	๒๐	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ปรับปรุงโครงสร้างศูนย์สารสนเทศและสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				- จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้
๓	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	**๒๐**	- ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศเพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ
๔	RIT๐๒ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๕	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย
๕	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- หาทางป้องกันสัตว์กัดแทะอุปกรณ์ - จัดหาเครื่องและอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนชั่วคราว เพื่อสามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ
๖	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑๐	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)
๗	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	๘	- ยอมรับความเสี่ยง	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
				- ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
๘	RIT๐๘ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	๕	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด
๙	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๕	- ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง
๑๐	RIT๐๙ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	- ยอมรับความเสี่ยง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้
๑๑	RIT๐๖ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	- ยอมรับความเสี่ยง	