แผนบริหารความเสี่ยง
ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ

ประจำปีงบประมาณ 2566

สำนักงานสาธารณสุข อำเภอหนองหญ้าไซ	แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ปีงบประมาณ 2566 (Information Technology Plan)	ฉบับที่ : ....1/2566 ..... แก้ไขครั้งที่ : .....-..... วันที่มีผลบังคับใช้ : ..... 20 มี.ค. 2566

หน่วยงาน : สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ

รายชื่อคณะกรรมการ :

1. นายปภากร เผ่าเวียงคำ	ประธาน
2. นายอำนาจ แก้วสุข	รองประธาน
3. นางสาววรวีภัสส์ ภวิศจารุสกุล	กรรมการ
4. นายกาญจน์ณภัทร ธนวัฒน์ธนเดโช	กรรมการ
5. นางสาวบุษราคัม บุญหนองเหล่า	กรรมการ
6. นายศรราม สุขตะกั่ว	กรรมการ
7. นางวิลาวรรณ บุญประเสริฐ	กรรมการ
8. นายวิสาข์ บุญประเสริฐ	กรรมการ
9. นายเมธาสิทธิ์ อภิสกุลโรจน์	กรรมการและเลขาฯ

ผู้จัดทำ : นายเมธาสิทธิ์ อภิสกุลโรจน์

ผู้จัดทำ

เมธาสิทธิ์

.....

(นายเมธาสิทธิ์ อภิสกุลโรจน์)
นักวิชาการคอมพิวเตอร์

20 / มีค / 2566

ผู้เห็นชอบ/อนุมัติ

.....

(นายปภากร เผ่าเวียงคำ)
นักวิชาการสาธารณสุขชำนาญการ รักษาราชการแทน
สาธารณสุขอำเภอหนองหญ้าไซ

20 / มีค / 2566

คำนำ

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสาธารณสุขอำเภอหนองหญ้าไซ ปีงบประมาณ 2566 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความ เสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนด แนวทางหรือมาตรการควบคุม เพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจ ประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้ และอยู่ใน ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ผู้จัดทำ หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของ สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ ฉบับนี้จะช่วยให้ผู้ใช้งาน ใช้เป็นแนวทางในการ ลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อ กระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขอำเภอหนองหญ้าไซ ต่อไป

แผนบริหารความเสี่ยง
ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ
ประจำปีงบประมาณ 2566

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ ประจำปีงบประมาณ 2566

สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ ได้นำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในการปฏิบัติงานหลายด้าน ดังนั้น สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อหาวิธีการป้องกันปัญหาที่อาจจะเกิดขึ้น อันส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร อีกทั้ง เป็นการนำเทคโนโลยีสารสนเทศมาสนับสนุนการ ปฏิบัติงานให้เกิดประโยชน์สูงสุดและลดโอกาสความเสียหายที่อาจจะเกิดขึ้น

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารมีวัตถุประสงค์เพื่อเป็น แนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงเกิดขึ้นจริง และสามารถนำแนวทางจัดการความเสี่ยงนี้ ไปใช้ในการดำเนินการได้

1. ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิ บัติงาน การเงินและ การบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้ อย่างถูกต้อง

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

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับ

ที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การด าเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะและการควบคุมเพื่อการแก้ไข

ทรัพย์สิน (Asset) หมายถึง ทรัพย์สินต่างๆ ขององค์กรแบ่งเป็น 5 หมวด ได้แก่ หมวดข้อมูล หมวดบุคลากร หมวดฮาร์ดแวร์ หมวดซอฟต์แวร์ และหมวดบริการ

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยง ตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Treadway Commission) มีดังนี้

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

2.วัตถุประสงค์

1. เพื่อให้การจัดการภายในสำนักงานสาธารณสุขอำเภอหนองหญ้าไซ มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสาธารณสุขอำเภอหนองหญ้าไซ

3. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

4. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

5. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบายแล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการ กับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

3. ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของงานเทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ

คณะกรรมการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ชื่อ - สกุล	ตำแหน่ง	ความรับผิดชอบ
1	นายปภากร เผ่าเวียงคำ	รักษาราชการแทนสาธารณสุขอำเภอหนองหญ้าไซ	ประธาน
2	นายอำนาจ แก้วสุข	ผู้ช่วยสาธารณสุขอำเภอหนองหญ้าไซ	รองประธาน
3	นางสาววรวีภัสส์ ภวิศจารุสกุล	นักวิชาการสาธารณสุขชำนาญการ	กรรมการ
4	นายกาญจน์ณภัทร ธนวัฒน์ธนเดโช	นักวิชาการสาธารณสุขปฏิบัติการ	กรรมการ
5	นางสาวบุษราคัม บุญหนองเหล่า	นักวิชาการสาธารณสุขปฏิบัติการ	กรรมการ
6	นายศรราม สุขตะกั่ว	เจ้าพนักงานสาธารณสุขปฏิบัติงาน	กรรมการ
7	นางวิลาวรรณ บุญประเสริฐ	นักวิชาการเงินและบัญชี	กรรมการ
8	นายวิสาข์ บุญประเสริฐ	เจ้าพนักงานธุรการ	กรรมการ
9	นายเมธาสิทธิ์ อภิสกุลโรจน์	นักวิชาการคอมพิวเตอร์	กรรมการและเลขาฯ

4. การประเมินความเสี่ยง (Risk assessment) การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของกรมสามารถแยกประเภทความเสี่ยงเป็น 4 ประเภท ดังนี้

- **ความเสี่ยงด้านเทคนิค** เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Crackเป็นต้น
- **ความเสี่ยงจากผู้ปฏิบัติงาน** เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือใช้ข้อมูลต่างๆ ของกรมฯ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
- **ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน** เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
- **ความเสี่ยงด้านการบริหารจัดการ** เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

ทั้งนี้ ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตารางที่ 1

ตารางที่ 1 รายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม
1. ความเสี่ยงจากการเกิด อัคคีภัย อุทกภัย	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	ความเสียหายของเครื่องคอมพิวเตอร์และอุปกรณ์ หรือ เครือข่าย ทำให้หน่วยงานใช้งานระบบ หรือ อุปกรณ์ไม่ได้	- ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ - น้ำรั่ว และความชื้นในอากาศ - สัตว์กัดแทะ เช่น หนูหรือแมลง - อุปกรณ์เสื่อมสภาพ
2. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	1.โปรแกรมหรือข้อมูลถูกทำลาย 2.ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ	- ไวรัส/มัลแวร์ - การดักจับข้อมูล - การถูกโจมตีระบบจากภายนอก
3. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	1. เกิดความเสียหายของระบบอุปกรณ์ภายใน Hardware 2.เกิดความเสียหายกับระบบข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์	- แหล่งกำเนิดไฟฟ้าขัดข้อง - เครื่องสำรองไฟฉุกเฉินไม่ทำงาน - การซ่อมบำรุงหยุดจ่ายระบบไฟฟ้า
4. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตและอินทราเน็ตขัดข้อง	ความเสี่ยงด้านเทคนิค	1. ไม่สามารถใช้งานระบบงานของหน่วยงานผ่านเครือข่ายอินเตอร์เน็ตได้ 2. ไม่สามารถเชื่อมต่อระบบงานภายนอกผ่านเครือข่ายอินเตอร์เน็ตได้	- การดำเนินการของหน่วยงานภายนอกที่มีผลกระทบต่อระบบเครือข่าย - การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ
5. ความเสี่ยงข้อมูลสารสนเทศรั่วไหล	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน/ความเสี่ยงจากภัยคุกคามทางไซเบอร์	1.โปรแกรมหรือข้อมูลเสียหาย 2.ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ 3.ข้อมูลสำคัญของหน่วยงานเสียหาย	- ถูกโจรกรรมข้อมูลของผู้ป่วย - ไวรัสเรียกค่าไถ่ (Ransomware) - ถูกเผยแพร่สาธารณะบนอินเตอร์เน็ต - ไวรัส/เวิร์ม

5. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

พิจารณาจาก การประเมินระดับโอกาสในการเกิดเหตุการณ์(Likelihood)และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง(Impact) โดยใช้ตาราง risk matrix

Likelihood/ระดับโอกาสในการเกิดเหตุการณ์

ระดับ	โอกาสที่จะเกิด	**ผลกระทบ**
1	น้อยมาก	5 ปีต่อครั้ง
2	น้อย	2-5 ปีต่อครั้ง
3	ปานกลาง	1 ปีต่อครั้ง
4	สูง	2-6 เดือนต่อครั้งไม่เกิน5
5	สูงมาก	1 เดือนต่อครั้งหรือมากกว่า

ระดับความรุนแรงของผลกระทบ(Impact)

ระดับความสำคัญ	**ระดับความรุนแรง**	**ผลกระทบ**
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ

Risk Matrix คือ การนำระดับโอกาสในการเกิดเหตุการณ์ (Likelihood) และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง (Impact) มาวิเคราะห์และจัดลำดับความสำคัญของเหตุการณ์เพื่อใช้ประกอบการตัดสินใจดำเนินการแก้ไข

ตารางแสดง Risk Matrix สำนักงานสาธารณสุขอำเภอหนองหญ้าไซ

โอกาสที่จะเกิด Likelihood	**ระดับความรุนแรงของผลกระทบ**(Impact)				
	1	2	3	4	5
5	Low	Significant	High	High	High
4	Low	Significant	Significant	High	High
3	Low	Low	Significant	High	High
2	Very Low	Low	Significant	Significant	Significant
1	Very Low	Very Low	Low	Low	Significant

จากตาราง risk matrix สามารถแบ่งระดับความสำคัญของความเสี่ยงเป็น 4 ระดับ จากระดับความสำคัญจากน้อยไปมาก ดังนี้

1. Very low risk level หมายถึง ระดับความเสี่ยงที่หน่วยงานสามารถยอมรับได เนื่องจากมีมาตรการควบคุมแล้ว
2. Low risk level หมายถึง ระดับความเสี่ยงที่หน่วยงานสามารถยอมรับได้ แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ
3. Significant risk level หมายถึง ระดับความเสี่ยงไม่สามารถยอมรับได้หน่วยงานต้องวางแผนบริหารจัดการ
4. High risk level หมายถึง ระดับความเสี่ยงที่หน่วยงานไม่สามารถยอมรับได้ จำเป็นต้องบริหารจัดการหน่วยงานเพื่อลดระดับความสำคัญลงให้ต่ำกว่า high risk level

ตารางที่ 2 ประเด็นความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ความเสี่ยง	โอกาสที่จะเกิด	ผลกระทบ	คะแนน
1	ความเสี่ยงจากการเกิด อัคคีภัย อุทกภัย	2	2	4
2	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	3	3	9
3	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	2	2	4
4	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตและอินทราเน็ตขัดข้อง	3	3	9
5	ความเสี่ยงข้อมูลสารสนเทศรั่วไหล	2	5	10

6. การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและ ผลกระทบที่เกิดขึ้นและขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ (ความถี่) X ความรุนแรงของเหตุการณ์ต่างๆ (ผลกระทบ)

ซึ่งใช้เกณฑ์ในการจัดแบ่ง ดังนี้

ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 - 7	ต่ำ	สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	เขียว
8 - 14	ปานกลาง	ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	เหลือง
15 - 20	สูง	ความเสี่ยงไม่สามารถยอมรับได้ (หน่วยงานต้องวางแผนบริหารจัดการ)	ส้ม
20 - 25	สูงมาก	ไม่สามารถยอมรับได้ (บริหารจัดการระดับโรงพยาบาล)	แดง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
1	ความเสี่ยงจากการเกิด อัคคีภัย อุทกภัย	**4**	สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) **-** มีการตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - สำรองข้อมูล ทั้งภายในและภายนอกอาคาร
2	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	**9**	ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการติดตั้งระบบปฏิบัติการ Windows ถูกลิขสิทธิ์ - ปรับปรุงระบบฐานข้อมูลของระบบสแกนไวรัสคอมพิวเตอร์ และปรับปรุงระบบปฏิบัติการ Windows ให้เป็นปัจจุบัน
3	ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	**4**	สามารถยอมรับความเสี่ยง (มีมาตรการควบคุมแล้ว)	**-** มีการติดตั้งระบบสำรองไฟฟ้าให้มีความครอบคลุมกับระบบคอมพิวเตอร์และตรวจสอบประสิทธิภาพของระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนดตามแผนบำรุงรักษาคอมพิวเตอร์ที่หน่วยงานได้กำหนดไว้
4	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตและอินทราเน็ตขัดข้อง	**9**	ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	**-** จัดหาระบบเครือข่ายอินเทอร์เน็ตสำรองเพื่อเป็นช่องทางให้ระบบอินเทอร์เน็ตใช้งานได้อย่างต่อเนื่อง - มีแผนบริหารจัดการบำรุงรักษาอุปกรณ์
5	ความเสี่ยงข้อมูลสารสนเทศรั่วไหล	**10**	ยอมรับความเสี่ยงได้ (แต่ต้องเฝ้าระวังมาตรการควบคุมสม่ำเสมอ)	- มีการติดตั้งอุปกรณ์ firewall ป้องกัน การโจมตีระบบจากภายนอกและตรวจสอบการใช้งานอินเตอร์ที่มีความเสี่ยง - มีการสำรองข้อมูล - มีการตั้งรหัสผ่านในการเข้าถึงข้อมูล

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ของสำนักงานสาธารณสุขอำเภอหนองหญ้าไซ บรรลุเป้าประสงค์ของการบริหารความเสี่ยง

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา
1. ความเสี่ยงจากการเกิด อัคคีภัย อุทกภัย	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - สำรองข้อมูล	- ปีละ 2 ครั้ง - เดือนละ 1 ครั้ง
2. ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	- การตรวจจับไวรัสคอมพิวเตอร์ - ประชาสัมพันธ์ให้ความรู้กับบุคลากรในเรื่องของความมั่นคงปลอดภัยสารสนเทศ	- ปีละ 1 ครั้ง
3. ความเสี่ยงจากการเกิดระบบกระแสไฟฟ้าขัดข้อง	- ตรวจเช็คการเก็บประจุไฟฟ้าของเครื่องสำรองไฟฟ้าคอมพิวเตอร์	- ทุกเดือน
4. ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตและอินทราเน็ตขัดข้อง	- เตรียมความพร้อมด้านอุปกรณ์เครือข่ายกรณีอุปกรณ์เครือข่ายขัดข้อง -มีแผนตรวจเช็คอุปกรณ์เครือข่าย	- ปีละ 1 ครั้ง -เดือนละ 2 ครั้ง
5. ความเสี่ยงข้อมูลสารสนเทศรั่วไหล	- มีการอัพเดทระบบ Firewall - มีแผน maintenance ระบบ Firewall	-ทุกเดือน -ปีละ 1 ครั้ง