



# การบริหารจัดการ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จังหวัดมหาสารคาม

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด  
สำนักงานจังหวัดมหาสารคาม

ประจำปี 2567



## คำนำ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักงานจังหวัดมหาสารคาม จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น และส่งผลกระทบต่อการทำงาน เป็นอุปสรรคต่อพันธกิจในองค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม

เพื่อให้ผลการดำเนินงานขององค์กรเป็นไปตามวัตถุประสงค์และเป้าหมายที่วางไว้ และเพื่อให้เกิดการรับรู้ตระหนัก และเข้าใจถึงความเสี่ยงด้านต่างๆ ที่เกิดขึ้นกับองค์กร โดยสามารถเลือกวิธีบริหารจัดการที่เหมาะสมในการลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ จึงได้นำหลักการ แนวคิด กระบวนการบริหารความเสี่ยงมาเป็นเครื่องมือในการพัฒนา ปลูกฝังให้เป็นส่วนหนึ่งของการดำเนินงานตามภารกิจ จนเป็นวัฒนธรรมองค์กรก่อให้เกิดประโยชน์ต่อการบรรลุเป้าหมายการดำเนินงานขององค์กรต่อไป

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด  
สำนักงานจังหวัดมหาสารคาม  
๑๐ มกราคม ๒๕๖๗

## สารบัญ

|                                                               | หน้า |
|---------------------------------------------------------------|------|
| คำนำ                                                          |      |
| หลักการและเหตุผล                                              | ๑    |
| วัตถุประสงค์                                                  | ๑    |
| เป้าหมาย                                                      | ๑    |
| ขอบเขตการดำเนินงาน                                            | ๒    |
| คำจำกัดความและความหมายที่เกี่ยวข้องกับการบริหารความเสี่ยง     | ๒    |
| ประโยชน์ของการบริหารความเสี่ยง                                | ๓    |
| <b>บทที่ ๒</b> แนวทางการบริหารความเสี่ยง                      | ๔    |
| ๑. หลักการบริหารความเสี่ยง                                    | ๔    |
| ๒. ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ                      | ๙    |
| ๓. ปัจจัยเสี่ยง                                               | ๑๐   |
| ๔. การประเมินความเสียหาย                                      | ๑๐   |
| ๕. ระบบรักษาความปลอดภัยบนเครือข่าย                            | ๑๐   |
| ๖. กรอบการบริหารความเสี่ยง                                    | ๑๒   |
| ๗. นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต             | ๑๙   |
| ๘. นโยบายการรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก      | ๒๑   |
| <b>บทที่ ๓</b> กระบวนการบริหารความเสี่ยง                      | ๑๓   |
| ๑. แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง                 | ๑๓   |
| ๒. การบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ | ๑๔   |
| ๓. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ          | ๑๕   |
| ๔. ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ       | ๒๐   |
| <b>แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ</b>            | ๓๓   |
| <b>บทที่ ๔</b> สรุปและข้อเสนอแนะ                              | ๔๒   |

## บทที่ ๑

### บทนำ

#### ๑.๑ หลักการและเหตุผล

การบริหารจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตาม ควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสีย และโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศ ที่เข้ามา มีบทบาท สำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งาน อุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ ต่าง ๆ ภายใต้สภาวะการ ดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อ การดำเนินงานหรือ เป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามี ปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาส และผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนด แนวทางในการจัดการความเสี่ยง โดยต้อง คำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

#### ๑.๒ วัตถุประสงค์

๑. เพื่อให้การจัดการภายในสำนักงานจังหวัดมหาสารคาม มีประสิทธิภาพ และมีความยืดหยุ่น ในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาส ที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศและการสื่อสาร

๒. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ ของสำนักงานจังหวัดมหาสารคาม

๓. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการ เผยแพร่ ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๕. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้นก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผนสำนักงาน จังหวัดมหาสารคาม ได้กำหนดวัตถุประสงค์ให้สอดคล้องกับยุทธศาสตร์และทิศทางโดยใช้หลัก SMART

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

#### ๑.๓ เป้าหมาย

สำนักงานจังหวัดมหาสารคาม มีแผนสำหรับดำเนินการเพื่อจัดการความเสี่ยง ดังนี้

๑. มีแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๒. มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๓. มีแผนบริหารความต่อเนื่องการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔. สามารถนำแผนบริหารจัดการความเสี่ยงไปใช้เพื่อเป็นกรอบแนวทางในการดำเนินงานขององค์กรได้

#### ๑.๔. ขอบเขตการดำเนินงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการภายในความรับผิดชอบของกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สำนักงานจังหวัดมหาสารคาม ซึ่งจะมีการรวบรวมและวิเคราะห์ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานจังหวัดมหาสารคาม

#### ๑.๕ คำจำกัดความและความหมายที่เกี่ยวข้องกับการบริหารความเสี่ยง

**ความเสี่ยง (Risk)** หมายถึง เหตุการณ์/การกระทำใดๆ ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบ ในเชิงลบต่อวัตถุประสงค์หรือเป้าหมายขององค์กร หรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบรรลุเป้าหมาย และวัตถุประสงค์ของแผนงาน/โครงการที่จะก้าวสู่พันธกิจ และวิสัยทัศน์ ที่กำหนดไว้

**ปัจจัยเสี่ยง (Risk Factor)** หมายถึง สาเหตุของความเสี่ยงซึ่งจะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการความเสี่ยงในภายหลังได้อย่างถูกต้อง

**การประเมินความเสี่ยง (Risk Assessment)** หมายถึง กระบวนการระบุความเสี่ยงและการวิเคราะห์ ความเสี่ยงเพื่อจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบต่อการบรรลุเป้าหมายขององค์กร (Impact)

**ระดับของความเสี่ยง (Degree of Risk)** หมายถึง สถานะของความเสี่ยงที่ได้จากประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงแบ่งเป็น ๕ ระดับ คือ ความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงปานกลาง ความเสี่ยงต่ำ และความเสี่ยงต่ำมาก

**โอกาส (Opportunity)** หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบ ในเชิงบวกต่อวัตถุประสงค์หรือเป้าหมายขององค์กร ซึ่งผู้บริหารและผู้ที่เกี่ยวข้องควรจะได้ทบทวนถึงกลยุทธ์และแผนงานที่เหมาะสมใหม่ เพื่อสร้างคุณค่าเพิ่มให้กับองค์กรนอกเหนือจากแผนงานและโครงการที่ได้กำหนดไว้แล้ว

**การควบคุมภายใน (Internal Control)** หมายถึง กระบวนการปฏิบัติงานที่บุคลากรในองค์กร โดยคณะกรรมการบริหาร ผู้บริหารทุกระดับ ข้าราชการ พนักงานราชการ และลูกจ้างทุกคนมีบทบาทร่วมกัน ในการจัดให้มีขึ้นเพื่อสร้างความเชื่อมั่นอย่างสมเหตุสมผลว่าการปฏิบัติงานจะบรรลุวัตถุประสงค์ของการควบคุมภายใน

**การบริหารจัดการความเสี่ยง (Risk Management)** หมายถึง กลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ ติดตาม และสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหน่วยงาน/ฝ่ายงาน หรือ กระบวนการดำเนินงานขององค์กรเพื่อช่วยลดความสูญเสียในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุด และเพิ่มโอกาสแก่องค์กรมากที่สุด

**การบริหารความเสี่ยงโดยองค์กรรวม (Enterprise Risk Management : EMR)** หมายถึง การบริหาร ความเสี่ยงโดยมีโครงสร้างองค์กรกระบวนการ และวัฒนธรรมองค์กรประกอบเข้าด้วยกัน และเป็นกลไกส่วนหนึ่ง ของการขับเคลื่อนไปสู่การกำกับดูแลกิจการที่ดี เพื่อบรรลุวัตถุประสงค์และการเติบโตอย่างยั่งยืนขององค์กร และเป็นที่พอใจของผู้มีผลประโยชน์ร่วม โดยครอบคลุมความเสี่ยงทั่วทั้งองค์กร ไม่ว่าจะเป็น ความเสี่ยงเกี่ยวกับกลยุทธ์ การดำเนินงาน การปฏิบัติตามกฎระเบียบ และการเงิน ซึ่งความเสี่ยงเหล่านี้อาจทำให้เกิดความเสียหาย ความไม่แน่นอน และโอกาส รวมถึงการมีผลกระทบต่อวัตถุประสงค์และความต้องการของผู้มีผลประโยชน์ร่วม

## ๑.๖ ประโยชน์ของการบริหารความเสี่ยง

การดำเนินการบริหารความเสี่ยงจะช่วยให้ผู้บริหารมีข้อมูลที่ใช้ในการตัดสินใจได้ดียิ่งขึ้น และทำให้องค์กร สามารถจัดการกับปัญหาอุปสรรคและอยู่รอดได้ในสถานการณ์ที่ไม่คาดคิดหรือสถานการณ์ที่อาจทำให้องค์กรเกิด ความเสียหาย

ประโยชน์ที่คาดหวังว่าจะได้รับจากการดำเนินการบริหารความเสี่ยง มีดังนี้

๑) เป็นส่วนหนึ่งของหลักการบริหารกิจการบ้านเมืองที่ดี การบริหารความเสี่ยงจะช่วยคณะทำงานบริหารความเสี่ยงและผู้บริหารทุกระดับตระหนักถึงความเสี่ยงหลักที่สำคัญ และสามารถทำหน้าที่ใน การกำกับดูแลองค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

๒) สร้างฐานข้อมูลที่มีประโยชน์ต่อการบริหารและการปฏิบัติงานในองค์กร การบริหารความเสี่ยงจะเป็นแหล่งข้อมูลสำหรับผู้บริหารในการตัดสินใจด้านต่างๆ รวมถึงการบริหารความเสี่ยง ซึ่งตั้งอยู่บนสมมุติฐานในการตอบสนองต่อเป้าหมายและภารกิจหลักขององค์กรรวมถึงระดับความเสี่ยงที่ยอมรับได้

๓) ช่วยสะท้อนให้เห็นภาพรวมของความเสี่ยงต่างๆ ที่สำคัญได้ทั้งหมด การบริหารความเสี่ยงจะทำให้บุคลากรภายในองค์กรมีความเข้าใจถึงเป้าหมายและภารกิจหลักขององค์กร และตระหนักถึงความเสี่ยงสำคัญที่ส่งผลกระทบต่อองค์กรได้อย่างครบถ้วน ซึ่งครอบคลุมความเสี่ยงธรรมาภิบาล

๔) เป็นเครื่องมือที่สำคัญในการบริหารงาน การบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยให้ผู้บริหารสามารถมั่นใจได้ว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมและทันเวลา รวมทั้งเป็นเครื่องมือที่สำคัญของผู้บริหารในการบริหารงาน และการตัดสินใจในด้านต่าง ๆ เช่น การวางแผนการกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ซึ่งส่งผลให้การดำเนินงานของสำนักงานจังหวัดมหาสารคามเป็นไปตามเป้าหมายที่กำหนด และสามารถปกป้องผลประโยชน์รวมทั้งเพิ่มมูลค่าแก่องค์กร

๕) ช่วยให้การพัฒนาองค์กรเป็นไปในทิศทางเดียวกัน การบริหารความเสี่ยงทำให้รูปแบบการตัดสินใจ ในระดับการปฏิบัติงานขององค์กรมีการพัฒนาไปในทิศทางเดียวกัน เช่น การตัดสินใจโดยที่ผู้บริหารมีความเข้าใจ ในกลยุทธ์วัตถุประสงค์ขององค์กร และระดับความเสี่ยงอย่างชัดเจน

๖) ช่วยให้การพัฒนาการบริหารและจัดสรรทรัพยากรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การจัดสรรทรัพยากรเป็นไปอย่างเหมาะสม โดยพิจารณาถึงระดับความเสี่ยงในแต่ละกิจกรรม และการเลือกใช้มาตรการในการบริหารความเสี่ยง เช่น การใช้ทรัพยากรสำหรับกิจกรรมที่มีความเสี่ยงต่ำ และกิจกรรมที่มีความเสี่ยงสูง ย่อมแตกต่างกัน หรือการเลือกใช้มาตรการแต่ละประเภทย่อมใช้ ทรัพยากรแตกต่างกัน เป็นต้น

## บทที่ ๒ แนวทางการบริหารความเสี่ยง

### ๒.๑ หลักการบริหารความเสี่ยง

หลักการบริหารความเสี่ยงโดยใช้กระบวนการบริหารความเสี่ยงตามมาตรฐานของ COSO (The Committee of Sponsoring Organization of the Tread way Commission) ซึ่งกำหนดกรอบการจัดการความเสี่ยงในแนวทาง COSO : ERM (Enterprise Risk Management) ประกอบด้วยหลักการสำคัญ ๘ องค์ประกอบ เพื่อให้เกิดการบรรลุวัตถุประสงค์ของการบริหารความเสี่ยง ดังภาพที่ ๑



ภาพที่ ๑ COSO : ERM (Enterprise Risk Management)

#### ๑. สภาพแวดล้อมภายในองค์กรด้านเทคโนโลยีสารสนเทศ (Internal Environment)

๑) ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น เว็บไซต์จังหวัดมหาสารคาม หน่วยงานภายในสังกัดสำนักงานจังหวัดมหาสารคามภายใต้อินเทอร์เน็ตโดเมน mahasarakham.go.th ฐานข้อมูลเว็บไซต์ดังกล่าว และเว็บไซต์จากระบบคลาวด์กลางภาครัฐที่สำนักงานจังหวัดมหาสารคามขอใช้บริการ เป็นต้น

๒) ระบบฐานข้อมูลบริหารงานภายใน ได้แก่ ฐานข้อมูลระบบออกเลขหนังสือสำนักงานจังหวัดมหาสารคาม ฐานข้อมูลระบบจัดเก็บเอกสารสำนักงานจังหวัดมหาสารคาม ฐานข้อมูลระบบจัดเก็บเลขพัสดุสำนักงานจังหวัดมหาสารคาม และฐานข้อมูลระบบบริหารบุคคลสำนักงานจังหวัดมหาสารคาม

๓) ระบบให้บริการเครือข่าย ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์จังหวัดมหาสารคาม (Web Application Program) เป็นต้น

๔) อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บ และสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) เครื่องคอมพิวเตอร์ป้องกันการโจรกรรมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์คอมพิวเตอร์ (Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

## ๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง (Objective Setting)

- ๑) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานจังหวัดมหาสารคาม กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
- ๒) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน
- ๓) เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทัน่วงที่ กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

## ๓. การบ่งชี้หรือการระบุความเสี่ยง (Event Identification)

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร

วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

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

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความเสี่ยงที่เกิดขึ้นในรูปของความถี่ของการเกิดความเสี่ยงและความรุนแรงของความเสี่ยง รวมทั้งข้อมูลการดำเนินการใดๆ เพื่อลดความเสี่ยงที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

## ๔. การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วย ๔ ขั้นตอน คือ

๑) การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree- of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็น เกณฑ์ ๕ ระดับ (สูงมาก สูง ปานกลาง น้อย และน้อยมาก)

๒) การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่า ความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยง

จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุม ความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่ มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

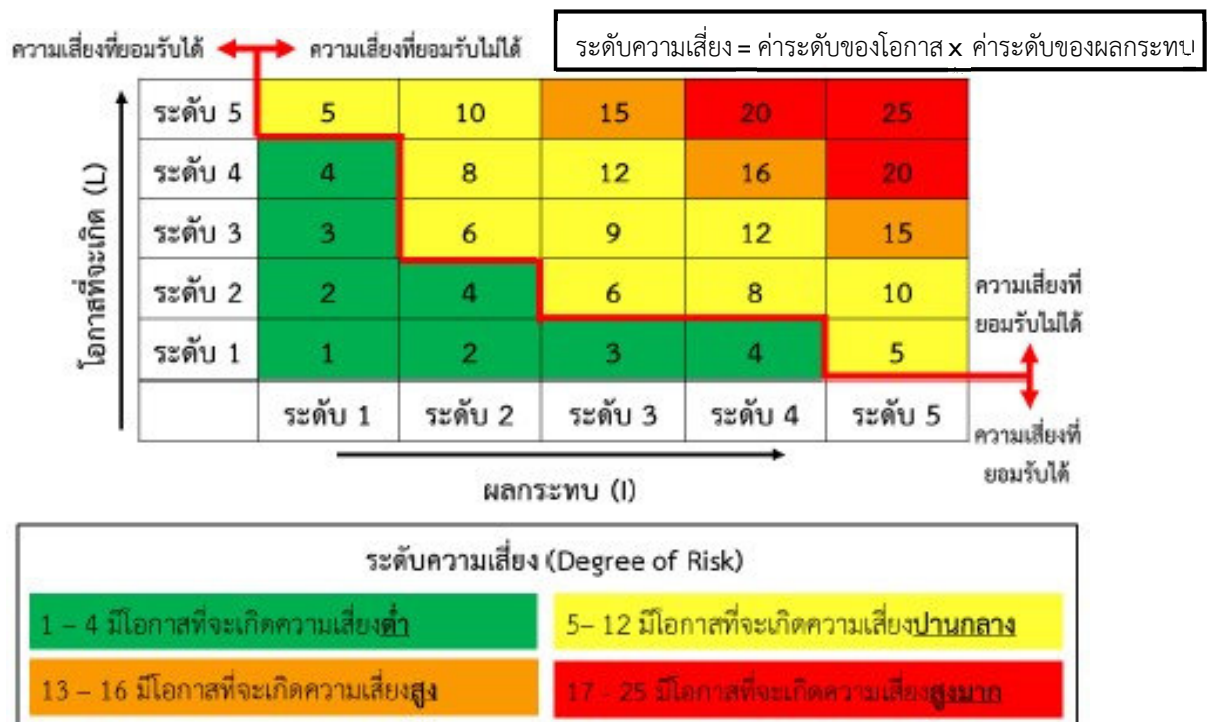
เกณฑ์การประเมินผลกระทบ มีดังนี้

| ระดับ | การประเมิน |
|-------|------------|
| ๑     | น้อยมาก    |
| ๒     | น้อย       |
| ๓     | ปานกลาง    |
| ๔     | สูง        |
| ๕     | สูงมาก     |

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง มีดังนี้

| ระดับ | การประเมิน           |
|-------|----------------------|
| ๑     | โอกาสเกิดขึ้นน้อยมาก |
| ๒     | โอกาสเกิดขึ้นน้อย    |
| ๓     | โอกาสเกิดขึ้นปานกลาง |
| ๔     | โอกาสเกิดขึ้นสูง     |
| ๕     | โอกาสเกิดขึ้นสูงมาก  |

๓) การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยง สูงสุดที่จะต้องบริหารจัดการก่อน ภาพที่ ๒



ภาพที่ 2 แสดงแผนผังการประเมินความเสี่ยง

**๔) การจัดลำดับความเสี่ยง** เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

## **๕. การตอบสนองความเสี่ยง (Risk Response)**

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้อง คำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพ ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลด ระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

**๑) การหลีกเลี่ยง (Terminate/Avoidance)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือการเลือกที่จะไม่รับความเสี่ยงไว้เลยอาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่เกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับ กิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมีได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

**๒) การยอมรับ (Take/Acceptance)** เป็นการยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิด ความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือ ป้องกันความเสี่ยง

**๓) การควบคุมหรือการลด (Treat/Reduction)** เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรง ของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธี ควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสีย หลังเกิด ความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความ สูญเสียก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

**๔) การถ่ายโอน (Transfer/Sharing)** การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

## **๖. กิจกรรมการควบคุมความเสี่ยง (Control Activities)**

การวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้ง เจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๑) **ควบคุมเพื่อป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึง เอกสาร เป็นต้น

๒) **การควบคุมเพื่อให้อุบัติการณ์ (Detective Control)** เป็นวิธีการควบคุมเพื่อค้น ข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓) **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๔) **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับ ความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก ใช้ขั้นตอนดังนี้

- ☐ นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น
- ☐ พิจารณา หรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
- ☐ ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

## ๗. ข้อมูลสารสนเทศและการติดต่อสื่อสาร (Information & Communication)

เป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ประเมินและการบริหารจัดการความเสี่ยง ดังนั้น สำนักงานจังหวัดมหาสารคาม ได้รวบรวมและบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งภายนอกและภายใน ตลอดจนเปิดเผยและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

## ๘. การติดตาม (Monitoring)

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงในโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุม ความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธี ซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยัง เหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่าย แต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

๑) พิจารณาวายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๒) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๓) กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔) ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการ มาบริหาร

ความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์ และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงาน ผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ถ้าไม่มีเหลืออยู่ มีอยู่ใน ระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

## ๒.๒ ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

งานเทคโนโลยีสารสนเทศ สำนักงานจังหวัดมหาสารคาม ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็น ๕ ประเภท ดังนี้

### ๑) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์สร้างขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ไฟผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

### ๒) ความเสี่ยงด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่ เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

### ๓) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

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

### ๔) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

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

### ๕) ความเสี่ยงด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสียหาย แก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญเนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญ สำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของ

ระบบ ข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและ จำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและ เทคโนโลยี

### ๒.๓ ปัจจัยเสี่ยง

ปัจจัยที่จะก่อให้เกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของงานเทคโนโลยีสารสนเทศ สำนักงานจังหวัดมหาสารคาม 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
- ☐ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ
- ☐ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสาร เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

### ๒.๔ การประเมินความเสียหาย

ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหาย จากไวรัส ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วคราว ได้แก่การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

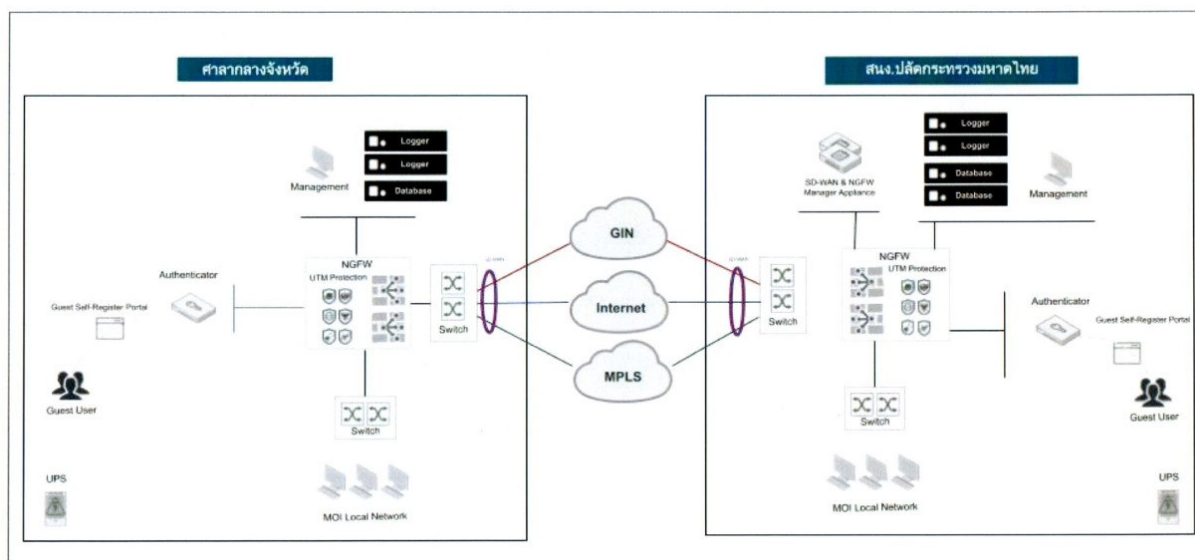
### ๒.๕ ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบคอมพิวเตอร์และเครือข่ายของสำนักงานจังหวัดมหาสารคาม ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบคอมพิวเตอร์และระบบเครือข่ายเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ตั้งอยู่ที่ศาลากลางจังหวัดมหาสารคาม สำนักงานจังหวัดมหาสารคาม ชั้น ๔ ที่อยู่ ถนนเลี้ยวเมืองมหาสารคาม – ร้อยเอ็ด ตำบลแวงน่าง อำเภอเมืองมหาสารคาม จังหวัดมหาสารคาม

ระบบคอมพิวเตอร์และเครือข่ายของสำนักงานจังหวัดมหาสารคาม มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวดเป็นไปตามมาตรฐาน ISO/IEC 27001:2022 ซึ่งเป็น มาตรฐานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems : ISMS) โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่าย

ในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการควบคุม (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ควบคุมและคัดกรอง (Filter Package) ข้อมูลที่ผ่านเข้ามาภายในระบบเครือข่ายสำนักงานจังหวัดมหาสารคาม และจากเครือข่ายภายนอก เช่น เครือข่ายอินเทอร์เน็ต เครือข่ายของสำนักงานจังหวัดมหาสารคาม เครือข่ายของผู้มาขอใช้บริการภายในบริเวณศาลากลางจังหวัดมหาสารคาม มีการกำหนดมาตรการควบคุมผ่านอุปกรณ์ Next Generation Firewall (NGFW) เพื่อในการควบคุมและคัดกรองข้อมูลที่ผ่านเข้ามาในระบบเครือข่าย ส่วนของระบบฐานข้อมูล Database มีการกำหนดมาตรการควบคุมผ่านอุปกรณ์ Intrusion Prevention System (IPS) เพื่อใช้ในการควบคุมและคัดกรองข้อมูลที่ผ่านเข้ามาในระบบ เครือข่าย เครื่องแม่ข่ายและเครื่องลูกข่ายมีการติดตั้งโปรแกรมระบบปฏิบัติการและป้องกันไวรัสที่มีลิขสิทธิ์ถูกต้อง เครื่องแม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัย เช่น Firewall, WAF, IPS, Core Switch ทั้งหมดส่ง Log เพื่อวิเคราะห์ และค้นหาปัญหา ภัยคุกคาม หรือการโจมตีที่เกิดขึ้นในระบบคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของสำนักงานจังหวัดมหาสารคาม มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเข้มงวด เพื่อให้มีความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบันเครือข่ายของสำนักงานจังหวัดมีการทำ Network Segmentation โดยแบ่ง Subnet และ VLAN ให้เป็นกลุ่มย่อยเพื่อเพิ่มความปลอดภัย โดยสามารถกำหนด Security Profile ให้เหมาะสมกับกลุ่มย่อยได้ เห็นถึงพฤติกรรมของอุปกรณ์ในเครือข่ายที่ซับซ้อนได้งานขึ้น สามารถติดตาม จำกัดความเสียหาย หรือการแพร่กระจายของภัยคุกคามให้อยู่ในวงจำกัดในกรณีเกิดปัญหาการใช้งาน สำหรับการใช้งานเครือข่ายสำนักงานจังหวัดมหาสารคามเพื่อใช้งานอินเทอร์เน็ตจำเป็นต้องมีการยืนยันตัวตนก่อนเข้าใช้งาน การใช้งานเครือข่ายสำนักงานจังหวัดมหาสารคามต้องเป็นเครื่องที่ลงทะเบียนการใช้งานกับงานเทคโนโลยีสารสนเทศเท่านั้น

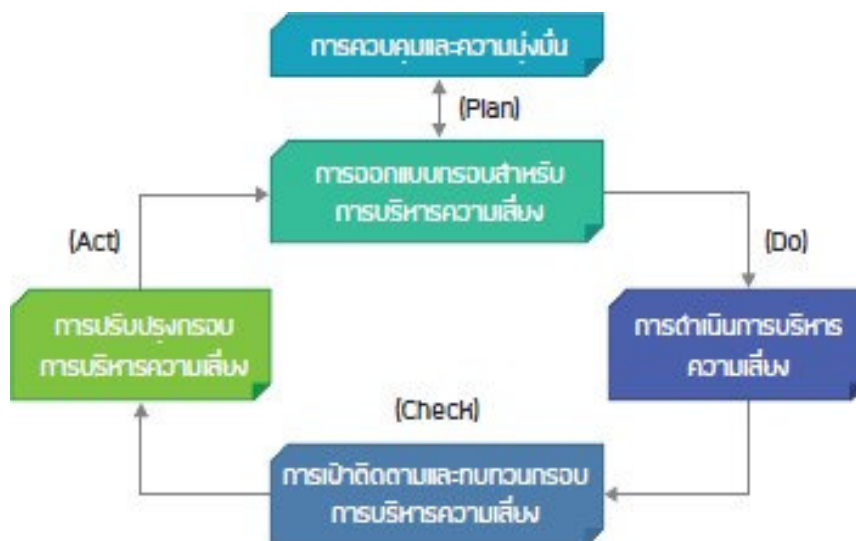
ระบบเครือข่ายหลักของสำนักงานจังหวัดมหาสารคาม จะเชื่อมโยงเครือข่ายโดยตรงจากสำนักงานปลัดกระทรวงมหาดไทยโดยใช้เทคโนโลยี MPLS (Multiprotocol Label Switching) ซึ่งเป็นเทคโนโลยีสำหรับการบริหารจัดการเส้นทางและควบคุมคุณภาพของสัญญาณเชื่อมต่อบนเครือข่าย ATM รวมทั้งใช้งานเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ GIN (Government Information Network) ที่สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยอุปกรณ์ถูกออกแบบและติดตั้งจำนวน ๒ ชุดขึ้นไปและทำงานในรูปแบบ HA (High Availability) ซึ่งเมื่ออุปกรณ์หลักเกิดชำรุดอุปกรณ์สำรองจะสามารถดำเนินการได้ทันที เพื่อป้องกันเหตุระบบเครือข่ายไม่สามารถใช้งานได้ลักษณะงานนั้นสามารถรองรับการใช้งานแบบ ๒๔ x ๗ เพื่อให้ระบบสารสนเทศทั้งหมดสามารถใช้งานได้อย่างเต็มประสิทธิภาพ



ภาพที่ ๓ แสดงโครงข่ายคอมพิวเตอร์สารสนเทศของสำนักงานจังหวัดมหาสารคาม

๒.๖ กรอบการบริหารจัดการความเสี่ยง

กรอบการบริหารจัดการความเสี่ยง (Framework for Managing Risk) ตามมาตรฐานการ บริหารจัดการ ความเสี่ยงสากล ISO31000 แบ่งออกเป็น ๔ ส่วน โดยขับเคลื่อนผ่านวงจร PDCA ประกอบด้วย ๑) การวางแผน (Plan) ๒) การลงมือทำ (Do) ๓) การตรวจสอบ (Check) ๔) การปรับปรุงแก้ไข (Act)



ภาพที่ ๔ กรอบการบริหารความเสี่ยง ตามมาตรฐาน ISO31000

๑) การออกแบบกรอบเพื่อการบริหารความเสี่ยง (Plan)

เป็นขั้นตอนการทำความเข้าใจสภาพแวดล้อมขององค์กร การบริหารความเสี่ยงขององค์กรจะเริ่มต้นจากการทำความเข้าใจในสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร โครงสร้างองค์กร การกำหนดนโยบาย ความต่อเนื่องทางธุรกิจ (Business continuity policy) รวมถึงวัตถุประสงค์ เป้าหมาย กระบวนการ และวิธีการ ปฏิบัติงานที่เกี่ยวข้องกับการจัดการกับความเสี่ยง เพื่อให้สามารถสร้างผลลัพธ์ที่สอดคล้องกับนโยบาย และวัตถุประสงค์โดยรวมขององค์กร

๒) การดำเนินการบริหารความเสี่ยง (Do)

การดำเนินการตามกรอบการบริหารความเสี่ยง จะเป็นการลงมือดำเนินการตามนโยบาย การควบคุม กระบวนการ และวิธีปฏิบัติ กำหนดช่วงเวลาและกลยุทธ์ที่เหมาะสมสำหรับการดำเนินการ การนำ นโยบายและกระบวนการบริหารจัดการความเสี่ยงมาใช้ในกระบวนการต่าง ๆ การจัดทำเอกสาร การฝึกอบรม การ สื่อสารองค์กร ดำเนินการเพื่อให้มั่นใจว่ากระบวนการบริหารความเสี่ยงต่าง ๆ ได้รับการนำไปปฏิบัติในทุกระดับและหน้าที่งานที่เกี่ยวข้องในองค์กร โดยเป็นส่วนหนึ่งของการปฏิบัติงานขององค์กร และกระบวนการทางธุรกิจ

๓) การเฝ้าติดตามและทบทวนกรอบการบริหารความเสี่ยง (Check)

ในขั้นตอนนี้จะเป็นการประเมิน และการวัดผลการดำเนินงานของแต่ละกระบวนการ วัดความก้าวหน้าเทียบกับแผนการบริหารความเสี่ยงเป็นระยะๆ การทบทวนถึงกรอบการบริหารความเสี่ยง นโยบาย และแผนงานอย่างสม่ำเสมอ การจัดทำรายงานความเสี่ยง ความก้าวหน้าของแผนการบริหาร ความเสี่ยง และการ ดำเนินการสอดคล้องกับนโยบายการบริหารความเสี่ยง การรายงานผลลัพธ์ที่ได้เพื่อนำไปสู่ การทบทวนโดยฝ่าย บริหารต่อไป

#### ๔) การปรับปรุงกรอบการบริหารความเสี่ยง (Act)

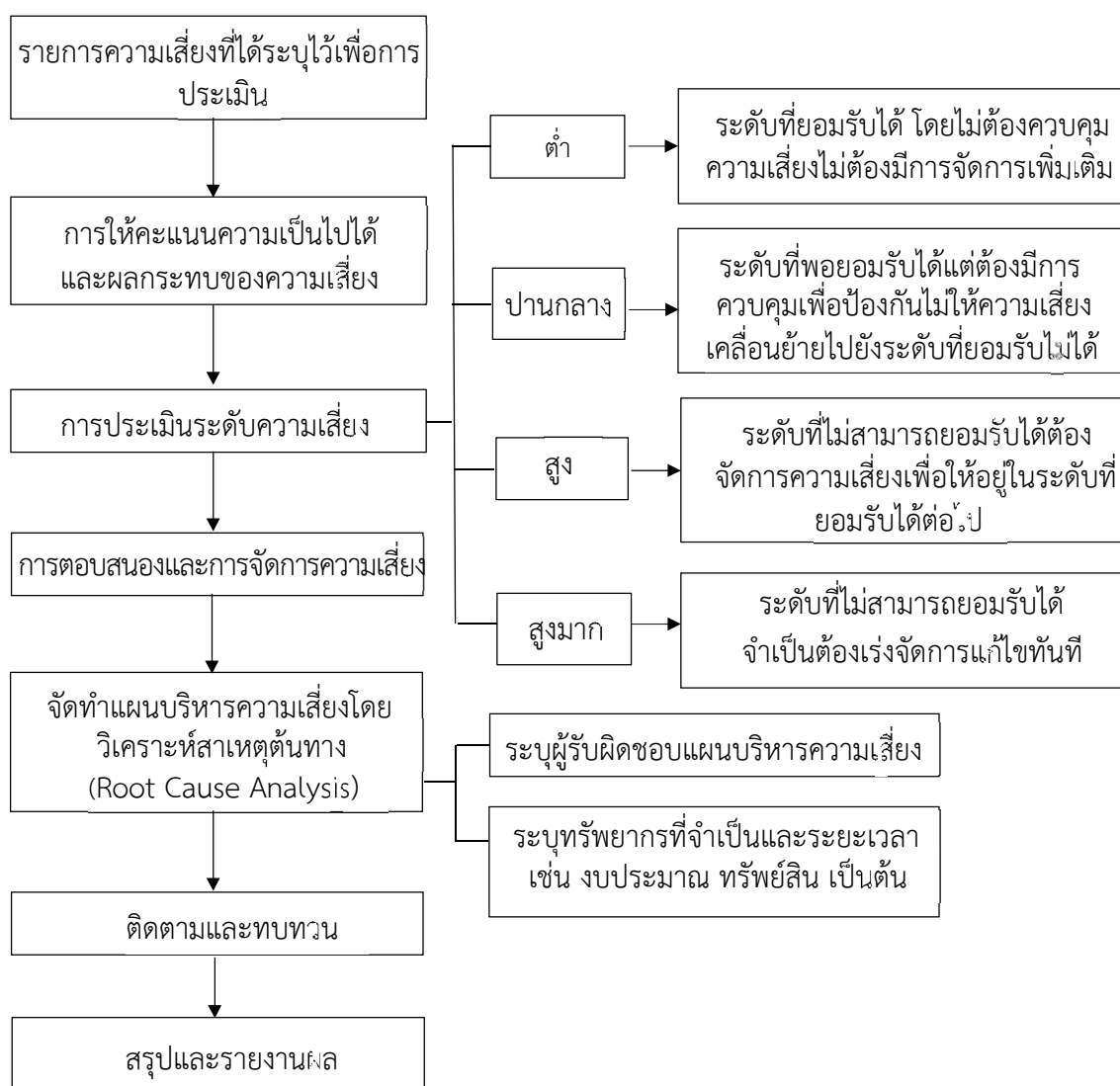
เป็นการดำเนินการปฏิบัติการแก้ไขและป้องกันจากผลของการทบทวน โดยฝ่ายบริหาร รวมถึงการดำเนินการปรับปรุงระบบการจัดการความเสี่ยง (Risk Management) ด้วย

#### บทที่ ๓

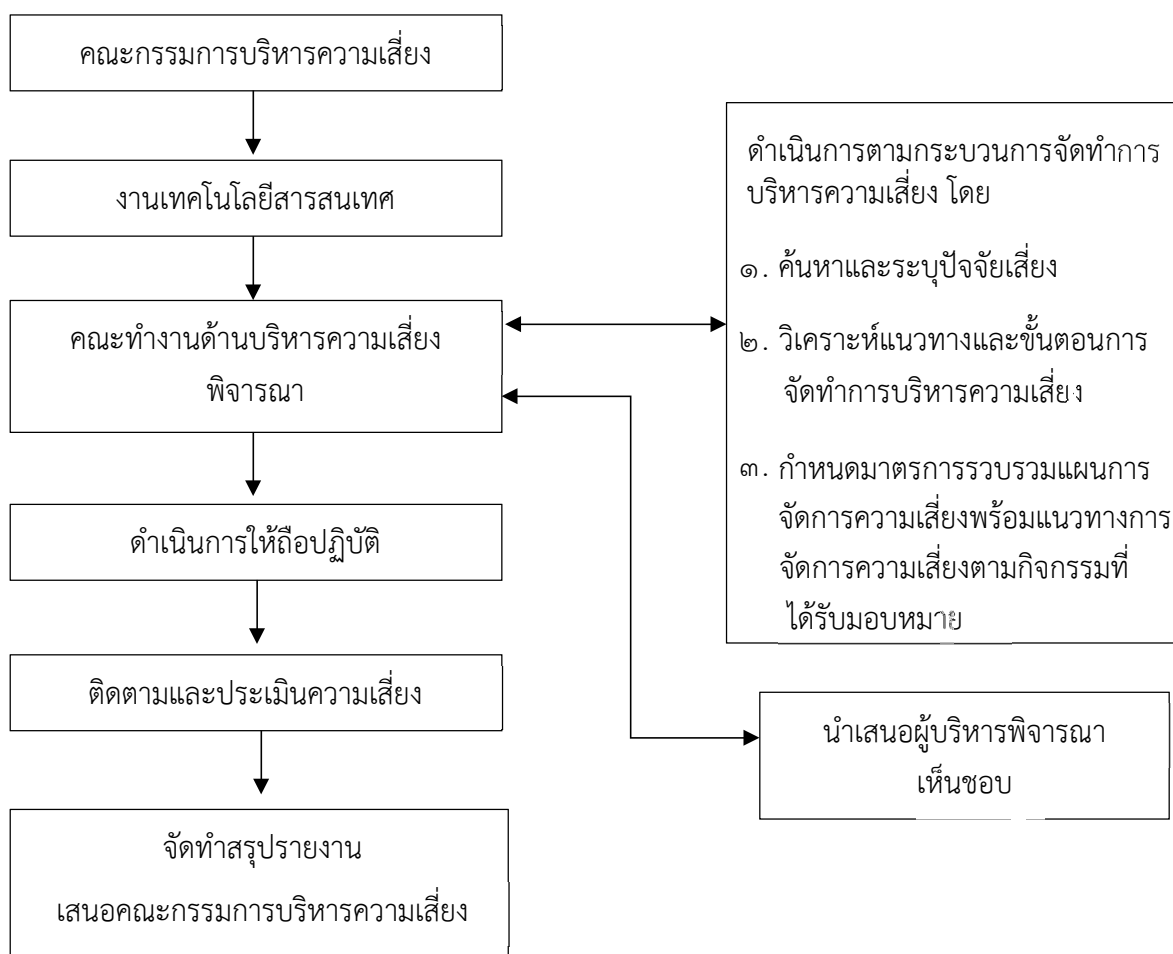
#### กระบวนการบริหารความเสี่ยง

สำนักงานจังหวัดมหาสารคามได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ งานเทคโนโลยีสารสนเทศจึงจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนการที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูลระดับความ คิดเห็นร่วมกับผู้ปฏิบัติงาน ด้านกิจกรรมนั้น ๆ ดังตารางการบริหารจัดการความเสี่ยงที่ได้จัดทำ การวิเคราะห์โดยแยกการวิเคราะห์ ออกเป็นกิจกรรมต่าง ๆ ดังต่อไปนี้

#### ๓.๑ แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



### ๓.๒ กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ



### ๓.๓ การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ ผลสรุปการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้

๑) ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) กำหนดเกณฑ์ไว้ ๕ ระดับ ดังนี้

Likelihood Table

| ระดับโอกาสเกิด |         | โอกาสในการเกิด                                                       |                     |
|----------------|---------|----------------------------------------------------------------------|---------------------|
| ๕              | สูงมาก  | โอกาสเกิดเหตุการณ์มากกว่า ๑ ครั้ง ภายใน ๓๐ วัน (๑ เดือน)             | มากกว่า ๑๒ ครั้ง/ปี |
| ๔              | สูง     | โอกาสเกิดเหตุการณ์น้อยกว่าหรือเท่ากับ ๑ ครั้ง ภายใน ๓๐ วัน (๑ เดือน) | ๑๒ ครั้ง/ปี         |
| ๓              | ปานกลาง | โอกาสเกิดเหตุการณ์อย่างน้อย ๑ ครั้ง ภายใน ๙๐ วัน (๓ เดือน)           | ๔ ครั้ง/ปี          |
| ๒              | น้อย    | โอกาสเกิดเหตุการณ์อย่างน้อย ๑ ครั้ง ภายใน ๑๘๐ วัน (๖ เดือน)          | ๒ ครั้ง/ปี          |
| ๑              | น้อยมาก | โอกาสเกิดเหตุการณ์อย่างน้อย ๑ ครั้ง ภายใน ๓๖๕ วัน (๑ ปี)             | ๑ ครั้ง/ปี          |

๒) ระดับความรุนแรงของผลกระทบ (Impact) กำหนดผลกระทบไว้ ๔ ด้าน แต่ละด้านกำหนดเกณฑ์ไว้ ๕ ระดับ ดังนี้

๒.๑) ผลกระทบเชิงปริมาณ ด้านการเงิน (Financial)

Financial Impact Table

| ระดับคะแนน | ระดับความรุนแรง | ผลกระทบ                                         |
|------------|-----------------|-------------------------------------------------|
| ๕          | สูงมาก          | มีมูลค่าความเสียหาย > ๖,๐๐๐,๐๐๐ บาท             |
| ๔          | สูง             | มีมูลค่าความเสียหาย > ๒,๐๐๐,๐๐๑ ≤ ๖,๐๐๐,๐๐๐ บาท |
| ๓          | ปานกลาง         | มีมูลค่าความเสียหาย > ๘๐๐,๐๐๐ ≤ ๒,๐๐๐,๐๐๐ บาท   |
| ๒          | น้อย            | มีมูลค่าความเสียหาย > ๓๐๐,๐๐๐ ≤ ๘๐๐,๐๐๐ บาท     |
| ๑          | น้อยมาก         | มีมูลค่าความเสียหาย ≤ ๓๐๐,๐๐๐ บาท               |

๒.๒) ผลกระทบเชิงคุณภาพ ด้านการดำเนินงานการให้บริการ (Operation)

Operation Impact Table

| ระดับคะแนน | ระดับความรุนแรง | ผลกระทบ                                                                                   |
|------------|-----------------|-------------------------------------------------------------------------------------------|
| ๕          | สูงมาก          | การให้บริการหยุดชะงัก ใช้เวลาดำเนินการแก้ไข > ๔ ชั่วโมง                                   |
| ๔          | สูง             | การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน > ๑ ชั่วโมง ≤ ๔ ชั่วโมง                      |
| ๓          | ปานกลาง         | การให้บริการหยุดชะงัก ดำเนินการแก้ไขได้ภายใน > ๓๐ นาที ≤ ๑ ชั่วโมง                        |
| ๒          | น้อย            | การให้บริการยังดำเนินการได้ แต่มีแนวโน้มจะหยุดชะงัก ดำเนินการแก้ไขได้ภายใน > ๑๕ ≤ ๓๐ นาที |
| ๑          | น้อยมาก         | การให้บริการยังดำเนินการได้ แต่มีแนวโน้มจะหยุดชะงัก ดำเนินการแก้ไขได้ภายใน ๑๕ นาที        |

## ๒.๓) ผลกระทบเชิงคุณภาพ ด้านภาพลักษณ์องค์กร (Reputation)

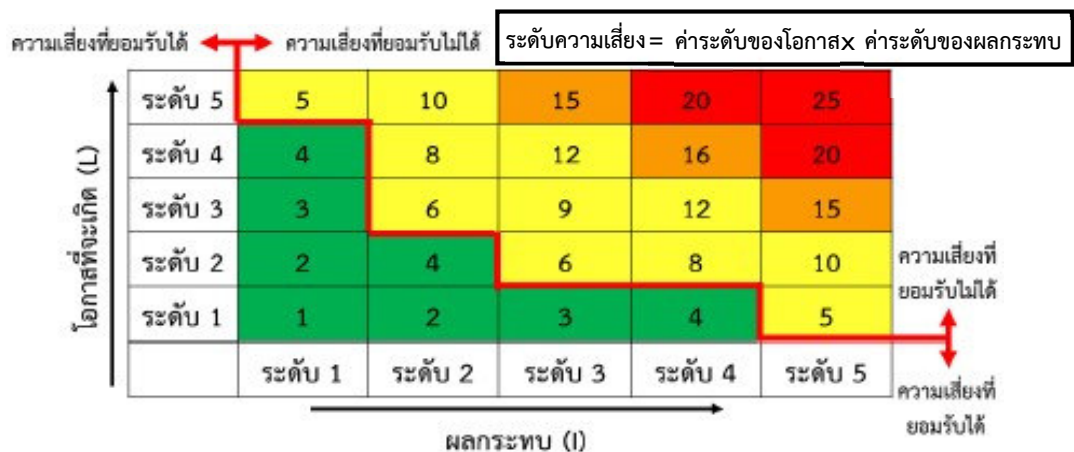
Reputation Impact Table

| ระดับ<br>คะแนน | ระดับความ<br>รุนแรง | ผลกระทบ                                                                                                                          |
|----------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------|
| ๕              | สูงมาก              | มีการเผยแพร่ข่าวภายนอกจังหวัดมหาสารคามและมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของจังหวัดมหาสารคาม                             |
| ๔              | สูง                 | มีการเผยแพร่ข่าวทั่วทั้งจังหวัดมหาสารคามและมีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของจังหวัดมหาสารคาม                           |
| ๓              | ปานกลาง             | มีการเผยแพร่ข่าวในระดับจังหวัดมหาสารคามและไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงจังหวัดมหาสารคาม                            |
| ๒              | น้อย                | มีการเผยแพร่ข่าวในวงจำกัดภายในสำนักงานจังหวัดมหาสารคาม และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของสำนักงานจังหวัดมหาสารคาม |
| ๑              | น้อยมาก             | มีการเผยแพร่ข่าวในวงจำกัดภายในงานเทคโนโลยีสารสนเทศ และไม่มีผลกระทบในทางลบต่อภาพลักษณ์และชื่อเสียงของสำนักงานจังหวัดมหาสารคาม     |

## ๒.๔) ผลกระทบเชิงคุณภาพ ด้านพนักงาน (Employee)

Employee Impact Table

| ระดับ<br>คะแนน | ระดับความรุนแรง | ผลกระทบ                                                      |
|----------------|-----------------|--------------------------------------------------------------|
| ๕              | สูงมาก          | เกิดเหตุการณ์ ก่อให้เกิดการเสียชีวิต/สูญเสียอวัยวะ/ทุพพลภาพ  |
| ๔              | สูง             | เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บสาหัส พักงาน > ๑ เดือน     |
| ๓              | ปานกลาง         | เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บ พักงาน ≤ ๑ เดือน          |
| ๒              | น้อย            | เกิดเหตุการณ์ ก่อให้เกิดการบาดเจ็บเล็กน้อยหรือพักงาน ≤ ๓ วัน |
| ๑              | น้อยมาก         | เกิดเหตุการณ์ แต่ไม่ก่อให้เกิดการบาดเจ็บ                     |



| ระดับความเสี่ยง (Degree of Risk)      |                                          |
|---------------------------------------|------------------------------------------|
| 1 – 4 มีโอกาสที่จะเกิดความเสี่ยงต่ำ   | 5– 12 มีโอกาสที่จะเกิดความเสี่ยงปานกลาง  |
| 13 – 16 มีโอกาสที่จะเกิดความเสี่ยงสูง | 17 – 25 มีโอกาสที่จะเกิดความเสี่ยงสูงมาก |

ภาพที่ ๕ แสดงแผนผังการประเมินความเสี่ยง

ตารางที่ ๑ เกณฑ์การประเมินระดับความรุนแรงของความเสี่ยง

| ระดับ<br>ความเสี่ยง | ค่าความเสี่ยง<br>(โอกาส x ผลกระทบ) | เกณฑ์การประเมิน                                                                                               |
|---------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------|
| สูงมาก              | ๑๗-๒๕                              | อยู่ในระดับที่ไม่สามารถยอมรับได้<br>จำเป็นต้องเร่งจัดการแก้ไขทันที                                            |
| สูง                 | ๑๓-๒๖                              | อยู่ในระดับที่ไม่สามารถยอมรับได้ต้องจัดการ<br>ความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป                  |
| ปานกลาง             | ๕-๑๒                               | ระดับที่พอยอมรับได้แต่ต้องมีการควบคุม<br>เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยัง<br>ระดับที่ยอมรับไม่ได้ |
| ต่ำ                 | ๑-๔                                | อยู่ในระดับที่ยอมรับได้ไม่ต้องควบคุมความเสี่ยง<br>ไม่ต้องการจัดการเพิ่มเติม                                   |

ตารางที่ ๒ รายละเอียดการประเมินในแต่ละประเด็นความเสี่ยง ปี พ.ศ.๒๕๖๖

| ลำดับ | ประเด็นความเสี่ยง                                                                                   | โอกาสเกิด | ผลกระทบ (ผลลัพธ์คิดจากคะแนนสูงสุดที่ได้) |                  |               |             | ระดับความเสี่ยง              |
|-------|-----------------------------------------------------------------------------------------------------|-----------|------------------------------------------|------------------|---------------|-------------|------------------------------|
|       |                                                                                                     |           | การเงิน (F)                              | การดำเนินงาน (O) | ภาพลักษณ์ (R) | พนักงาน (E) |                              |
| ๑     | การบุกรุกโจมตีจากภายนอก                                                                             | ๓         | ๕                                        | ๕                | ๕             | ๑           | สูง<br>$๓ \times ๕ = ๑๕$     |
| ๒     | ไวรัสคอมพิวเตอร์/Malware                                                                            | ๓         | ๔                                        | ๓                | ๒             | ๑           | ปานกลาง<br>$๓ \times ๔ = ๑๒$ |
| ๓     | การถูกโจรกรรมฐานข้อมูล                                                                              | ๒         | ๕                                        | ๕                | ๕             | ๑           | ปานกลาง<br>$๒ \times ๕ = ๑๐$ |
| ๔     | การถูกโจมตีเครื่องแม่ข่าย (Server) ทำให้ไม่สามารถให้บริการได้ (Denial of Service-DoS)               | ๒         | ๕                                        | ๔                | ๔             | ๑           | ปานกลาง<br>$๒ \times ๕ = ๑๐$ |
| ๕     | การถูกฟ้องร้องจาก<br>การละเมิดข้อมูลส่วนบุคคล<br>ตามพระราชบัญญัติคุ้มครอง<br>ข้อมูลส่วนบุคคล (PDPA) | ๒         | ๔                                        | ๑                | ๔             | ๑           | ปานกลาง<br>$๒ \times ๔ = ๘$  |
| ๖     | การไม่สามารถใช้งานโปรแกรม<br>สำนักงาน (Software) ได้                                                | ๒         | ๒                                        | ๓                | ๒             | ๑           | ปานกลาง<br>$๒ \times ๓ = ๖$  |
| ๗     | เจ้าหน้าที่ใช้คอมพิวเตอร์/<br>ระบบเครือข่ายผิดวัตถุประสงค์                                          | ๒         | ๓                                        | ๑                | ๑             | ๑           | ปานกลาง<br>$๒ \times ๓ = ๖$  |
| ๘     | การโจรกรรมอุปกรณ์<br>คอมพิวเตอร์/อุปกรณ์ต่อพ่วง<br>คอมพิวเตอร์                                      | ๓         | ๑                                        | ๑                | ๒             | ๑           | ปานกลาง<br>$๓ \times ๒ = ๖$  |
| ๙     | ระบบกระแสไฟฟ้าขัดข้อง                                                                               | ๓         | ๑                                        | ๑                | ๒             | ๑           | ปานกลาง<br>$๓ \times ๒ = ๖$  |
| ๑๐    | ข้อมูลรั่วไหลจากการ<br>เปลี่ยนมือผู้ใช้                                                             | ๑         | ๒                                        | ๑                | ๕             | ๑           | ปานกลาง<br>$๑ \times ๕ = ๕$  |
| ๑๑    | อัคคีภัย                                                                                            | ๑         | ๕                                        | ๔                | ๒             | ๑           | ปานกลาง<br>$๑ \times ๕ = ๕$  |
| ๑๒    | แผ่นดินไหว                                                                                          | ๑         | ๕                                        | ๕                | ๓             | ๓           | ปานกลาง<br>$๑ \times ๕ = ๕$  |
| ๑๓    | อุทกภัย                                                                                             | ๑         | ๕                                        | ๓                | ๓             | ๑           | ปานกลาง<br>$๑ \times ๕ = ๕$  |

| ลำดับ | ประเด็นความเสี่ยง                                            | โอกาสเกิด | ผลกระทบ (ผลลัพธ์คิดจากคะแนนสูงสุดที่ได้) |                  |               |             | ระดับความเสี่ยง             |
|-------|--------------------------------------------------------------|-----------|------------------------------------------|------------------|---------------|-------------|-----------------------------|
|       |                                                              |           | การเงิน (F)                              | การดำเนินงาน (O) | ภาพลักษณ์ (R) | พนักงาน (E) |                             |
| ๑๔    | แมลงหรือสัตว์กัดแทะอุปกรณ์คอมพิวเตอร์ หรือสายไฟฟ้า/สายสัญญาณ | ๑         | ๕                                        | ๔                | ๒             | ๑           | ปานกลาง<br>$๑ \times ๕ = ๕$ |
| ๑๕    | การไม่สำรองข้อมูล/การสำรองข้อมูลขาดการอัปเดต                 | ๒         | ๒                                        | ๒                | ๒             | ๑           | ต่ำ<br>$๒ \times ๒ = ๔$     |
| ๑๖    | การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์                             | ๒         | ๒                                        | ๒                | ๒             | ๑           | ต่ำ<br>$๒ \times ๒ = ๔$     |
| ๑๗    | ระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย                            | ๑         | ๒                                        | ๓                | ๒             | ๑           | ต่ำ<br>$๑ \times ๓ = ๓$     |
| ๑๘    | การใช้ Wireless เข้าเครือข่ายอินเทอร์เน็ตทั้งหมด             | ๑         | ๒                                        | ๑                | ๑             | ๑           | ต่ำ<br>$๑ \times ๒ = ๒$     |
| ๑๙    | การเชื่อมต่อระบบอินเทอร์เน็ต/อินเทอร์เน็ตขัดข้อง             | ๑         | ๒                                        | ๑                | ๒             | ๑           | ต่ำ<br>$๑ \times ๒ = ๒$     |
| ๒๐    | มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร              | ๑         | ๒                                        | ๑                | ๑             | ๑           | ต่ำ<br>$๑ \times ๒ = ๒$     |
| ๒๑    | การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง | ๑         | ๒                                        | ๑                | ๑             | ๑           | ต่ำ<br>$๑ \times ๒ = ๒$     |
| ๒๒    | การถูก Black List จาก Search Engine                          | ๑         | ๒                                        | ๑                | ๑             | ๑           | ต่ำ<br>$๑ \times ๒ = ๒$     |

## ๓.๔ ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

| ประเภทความเสี่ยง                                                                     | ความเสี่ยง                            | ปัจจัยความเสี่ยง                                                                                        | ผลกระทบ                                                                                                                                                                                                                                                                            | ระดับความเสี่ยง   | กิจกรรมควบคุม                                                                                                                                                                                 | วิธีการจัดการความเสี่ยง     | ผู้รับผิดชอบ                                    |
|--------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-------------------------------------------------|
| <b>ความเสี่ยงสูง</b>                                                                 |                                       |                                                                                                         |                                                                                                                                                                                                                                                                                    |                   |                                                                                                                                                                                               |                             |                                                 |
| ด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร<br>(Hardware and Data Communication Risk) | การบุกรุกโจมตีจากภายนอก               | เสี่ยงต่อการถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต                                                  | <input type="checkbox"/> ทำให้ระบบเครื่องแม่ข่ายหรือถูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย<br><input type="checkbox"/> ถูกแก้ไขหรือเปลี่ยนแปลงข้อมูล หรือรูปภาพ บน Web Site ของจังหวัดมหาสารคาม<br><input type="checkbox"/> ถูกโจรกรรมข้อมูลที่เป็นความลับ | สูง<br>๓x๕=๑๕     | ๑. ติดตั้งระบบเครือข่ายเพื่อป้องกันและเตือนภัย<br>๒. จัดทำแผนหรือขั้นตอนการปฏิบัติที่จำเป็นเพื่อป้องกันการถูกบุกรุกตามลำดับ<br>๓. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย | การลดความเสี่ยง (Reduction) | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |
| <b>ความเสี่ยงปานกลาง</b>                                                             |                                       |                                                                                                         |                                                                                                                                                                                                                                                                                    |                   |                                                                                                                                                                                               |                             |                                                 |
| ด้านอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร<br>(Hardware and Data Communication Risk) | จากการติดไวรัสคอมพิวเตอร์หรือ Malware | ๑. โปรแกรมหรือข้อมูลถูกทำลาย<br>๒. ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ<br>๓. การถูกขโมยข้อมูล | <input type="checkbox"/> ใช้คอมพิวเตอร์ไม่ได้<br><input type="checkbox"/> ใช้ระบบงานไม่ได้<br><input type="checkbox"/> ข้อมูลที่สำคัญสูญหาย                                                                                                                                        | ปานกลาง<br>๓x๔=๑๒ | ๑. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย<br>๒. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ                                                                                                              | การลดความเสี่ยง (Reduction) | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |

| ประเภท<br>ความเสี่ยง                                                                            | ความเสี่ยง                                                                                                              | ปัจจัยความเสี่ยง                                                                                                     | ผลกระทบ                                                                            | ระดับ<br>ความเสี่ยง | กิจกรรมควบคุม                                                                                           | วิธีการจัดการ<br>ความเสี่ยง        | ผู้รับผิดชอบ                                                    |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------|
| ด้านอุปกรณ์เทคโนโลยี<br>สารสนเทศ และการ<br>สื่อสาร<br>(Hardware and Data<br>Communication Risk) | จากการถูกโจรกรรม<br>ฐานข้อมูล                                                                                           | เสี่ยงต่อการสูญหาย<br>ของข้อมูล                                                                                      | <input type="checkbox"/> ข้อมูลสูญหาย<br><input type="checkbox"/> สูญเสียรายได้    | ปานกลาง<br>๒x๕=๑๐   | ๑. ติดตั้งระบบป้องกันไวรัส<br>กับเครื่องแม่ข่าย<br>๒. อัปเดตข้อมูลไวรัส<br>อย่างสม่ำเสมอ                | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูล<br>เพื่อการ<br>พัฒนาจังหวัด |
| ด้านอุปกรณ์เทคโนโลยี<br>สารสนเทศ และการ<br>สื่อสาร<br>(Hardware and Data<br>Communication Risk) | จากการโจมตี<br>เครื่องแม่ข่ายของ<br>จังหวัดฯ ทำให้ไม่<br>สามารถให้บริการได้<br>(Denial of<br>Service-DoS)               | ๑. โปรแกรมหรือข้อมูล<br>ถูกทำ-ลาย<br>๒. ไม่สามารถเรียกใช้<br>โปรแกรมหรือ<br>ระบบงานได้ตามปกติ<br>๓. การถูกขโมยข้อมูล | <input type="checkbox"/> ข้อมูลสูญหาย<br><input type="checkbox"/> สูญเสียรายได้    | ปานกลาง<br>๒x๕=๑๐   | ๑. ติดตั้งระบบป้องกันไวรัส<br>กับเครื่องแม่ข่าย<br>๒. อัปเดตข้อมูลไวรัส<br>อย่างสม่ำเสมอ                | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูล<br>เพื่อการ<br>พัฒนาจังหวัด |
| ด้านบุคลากร<br>(Human Risk)                                                                     | การถูกฟ้องร้อง<br>จากการละเมิด<br>ข้อมูลส่วนบุคคล<br>ตามพระราชบัญญัติ<br>คุ้มครองข้อมูล<br>ส่วนบุคคล<br>พ.ศ.๒๕๖๒ (PDPA) | การดำเนินการที่ไม่<br>สอดคล้องกับ<br>พระราชบัญญัติคุ้มครอง<br>ข้อมูลส่วนบุคคล<br>พ.ศ. ๒๕๖๒                           | ข้อมูลส่วนบุคคลถูกละเมิด<br>อาจก่อให้เกิดอันตรายทั้งต่อ<br>ร่างกายหรือต่อทรัพย์สิน | ปานกลาง<br>๒x๔=๘    | ๑. แต่งตั้งคณะกรรมการ<br>อำนวยการและ<br>คณะกรรมการดำเนินการ<br>ที่เกี่ยวข้องกับ พรบ.<br>ข้อมูลส่วนบุคคล | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูล<br>เพื่อการ<br>พัฒนาจังหวัด |

| ประเภท<br>ความเสี่ยง | ความเสี่ยง | ปัจจัยความเสี่ยง | ผลกระทบ | ระดับ<br>ความเสี่ยง | กิจกรรมควบคุม                                                                                                                                                                                                                                                                                                                                                                                                                                                        | วิธีการจัดการ<br>ความเสี่ยง | ผู้รับผิดชอบ |
|----------------------|------------|------------------|---------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------|
|                      |            |                  |         |                     | <p>๒. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบายระเบียบและแนวปฏิบัติแก่บุคลากรตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล</p> <p>๓. จัดทำนโยบาย ระเบียบ และแนวปฏิบัติ ในการจัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการ และแนวปฏิบัติปีละ ๑ ครั้ง</p> <p>๔. พัฒนาสถาปัตยกรรมขององค์กร (Enterprise Architecture: EA) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถพิจารณาความเชื่อมโยงของระบบ และข้อมูลได้ และสามารถตอบสนองได้ หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น</p> |                             |              |

| ประเภท<br>ความเสี่ยง                          | ความเสี่ยง                                                                                                         | ปัจจัยความเสี่ยง                            | ผลกระทบ                                                                             | ระดับ<br>ความเสี่ยง | กิจกรรมควบคุม                                                                                                                                                                                                                                                                                      | วิธีการจัดการ<br>ความเสี่ยง        | ผู้รับผิดชอบ                                                    |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------|
|                                               |                                                                                                                    |                                             |                                                                                     |                     | ๕. พัฒนาความรู้ของบุคลากร<br>ทั้งผู้ใช้ข้อมูล ผู้ควบคุม<br>ข้อมูล และผู้ประมวลผล<br>ข้อมูลส่วนบุคคล ให้เกิด<br>การ ตระหนัก มีความรู้<br>และทักษะในการจัดการ<br>ข้อมูลส่วนบุคคล<br>๖. จัดให้มีการซ้อมกระบวนการ<br>ตอบสนอง ในกรณีเกิด<br>การละเมิด ข้อมูลส่วน<br>บุคคลขึ้น อย่างน้อย<br>๑ ครั้งต่อปี |                                    |                                                                 |
| ด้านโปรแกรม<br>คอมพิวเตอร์<br>(Software Risk) | จากการไม่สามารถ<br>ใช้งานโปรแกรม<br>(Software) ข้อมูล<br>หลักของระบบ<br>สารสนเทศใน<br>สำนักงานจังหวัด<br>มหาสารคาม | เสี่ยงต่อการให้บริการ<br>ระบบสำคัญหยุดชะงัก | <input type="checkbox"/> เจ้าหน้าที่รอนาน<br><input type="checkbox"/> ผู้ไม่พึงพอใจ | ปานกลาง<br>๒x๓=๖    | ดำเนินการตามแผน<br>Manual System                                                                                                                                                                                                                                                                   | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด |

| ประเภทความเสี่ยง                                            | ความเสี่ยง                                                | ปัจจัยความเสี่ยง                                                                                                                                                                                   | ผลกระทบ                                                                                                                                                                     | ระดับความเสี่ยง  | กิจกรรมควบคุม                                                                                                                                                                                                                                                                                                                                                                                       | วิธีการจัดการความเสี่ยง        | ผู้รับผิดชอบ                                    |
|-------------------------------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------------------|
| ด้านบุคลากร<br>(Human Risk)                                 | เจ้าหน้าที่ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์        | ๑. เสี่ยงต่อการใช้งานในทางที่ผิดหรือเปล่าประโยชน์ เช่น การฟิชชิ่งหรือดูโทรทศน์ออนไลน์ เป็นต้น<br>๒. การใช้ Resource ทำผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรม ภาพยนตร์หรือเพลงที่ไม่มีลิขสิทธิ์ เป็นต้น | <input type="checkbox"/> สูญเสีย Bandwidth ในเครือข่าย ทำให้ต้องจัดเพิ่ม Bandwidth ให้มากขึ้นทุกๆ ปี<br><input type="checkbox"/> อาจถูกร้องเรียนหรือฟ้องร้อง จากบุคคลภายนอก | ปานกลาง<br>๒x๓=๖ | ๑. บริหารจัดการด้วยข้อเสนอแนะ Ten Ways to Protect Your Network From Insider Threats เพื่อลดความเสี่ยง<br>๒. กำหนด Policy ของ Firewall ให้เหมาะสมอย่างสม่ำเสมอ<br>เปิด port เท่าที่จำเป็น<br>๓. การมีข้อตกลงที่ผู้ใช้งานต้องเป็น ผู้รับผิดชอบในการนำอุปกรณ์เครื่อง คอมพิวเตอร์ หรือ Resources ต่างๆ ไปใช้ ในทางที่ผิด รวมถึงการบันทึกการใช้งาน และรายงานการใช้งานของผู้ใช้ที่ฝ่าฝืนต่อผู้บังคับบัญชา | การลดความเสี่ยง<br>(Reduction) | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |
| ด้านกายภาพและสิ่งแวดล้อม<br>(Physical and Environment Risk) | จากการโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์ | เสี่ยงต่อการสูญหายของอุปกรณ์คอมพิวเตอร์ และข้อมูลที่มีความสำคัญ                                                                                                                                    | <input type="checkbox"/> เสี่ยงงบประมาณในการจัดหาอุปกรณ์ ทดแทน<br><input type="checkbox"/> เสียภาพลักษณ์ของจังหวัดฯ                                                         | ปานกลาง<br>๓x๒=๖ | ๑. ควบคุมการเข้าออกอาคาร<br>๒. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์เข้า-ออกอาคารตลอดเวลา                                                                                                                                                                                                                                                                                                               | การลดความเสี่ยง<br>(Reduction) | กลุ่มงานอำนวยการ                                |

| ประเภทความเสี่ยง                                         | ความเสี่ยง                          | ปัจจัยความเสี่ยง                                                                                                                                                                                  | ผลกระทบ                                                                                                                                                                                  | ระดับความเสี่ยง  | กิจกรรมควบคุม                                                                                                                                       | วิธีการจัดการความเสี่ยง        | ผู้รับผิดชอบ                                                       |
|----------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------------------------------------------------|
|                                                          |                                     |                                                                                                                                                                                                   |                                                                                                                                                                                          |                  | ๓. ติดตั้งกล่องวงจรปิดให้ครอบคลุมทุกพื้นที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่                                                                |                                |                                                                    |
| ด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) | จากระบบกระแสไฟฟ้าขัดข้อง            | ๑. ไม่สามารถใช้งานเครื่องแม่ข่าย และระบบเครือข่ายได้<br>๒. ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่ายทั้งส่วนระบบปฏิบัติการ (Operating System) เนื่องจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม | <input type="checkbox"/> ข้อมูลเสียหาย<br><input type="checkbox"/> ระบบปฏิบัติการ โปรแกรมหรือฐานข้อมูล เสียหาย<br>ต้องมีการติดตั้งใหม่                                                   | ปานกลาง<br>๓x๒=๖ | ๑. ตรวจสอบระบบสำรองไฟฟ้า (UPS)<br>๒. ตรวจสอบการทำงานของเครื่องกำเนิดไฟฟ้า (Electrical Generator)                                                    | การถ่ายโอนความเสี่ยง (Sharing) | กลุ่มงานอำนวยการและกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |
| ด้านระบบข้อมูล (Database Risk)                           | ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้ | ข้อมูลที่สำคัญมีการรั่วไหล จากการ ซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรือ แผ่น DVD/ CD                                                                                                          | <input type="checkbox"/> ข้อมูลที่อยู่ในชั้น ความลับรั่วไหล ทำให้เสียหายต่อความเชื่อถือของจังหวัดฯ<br><input type="checkbox"/> ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้ | ปานกลาง<br>๑x๕=๕ | มีการบริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk แผ่น DVD/ CD ให้แน่ใจว่าข้อมูลได้ ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆ ทิ้งแล้วหากทำได้ | การลดความเสี่ยง (Reduction)    | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด                    |

| ประเภทความเสี่ยง                                                | ความเสี่ยง               | ปัจจัยความเสี่ยง                                                                                                                     | ผลกระทบ                                                                                                                                                     | ระดับความเสี่ยง  | กิจกรรมควบคุม                                                                                                                                                                                  | วิธีการจัดการความเสี่ยง            | ผู้รับผิดชอบ                                                                               |
|-----------------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------|
| ด้านกายภาพ<br>และสิ่งแวดล้อม<br>(Physical and Environment Risk) | จากการเกิดอัคคีภัย       | ๑. คอมพิวเตอร์และ<br>เครือข่ายถูกทำลาย<br>๒. ข้อมูลถูกทำลาย<br>๓. การบาดเจ็บหรือ<br>เสียชีวิตของเจ้าหน้าที่<br>หรือลูกจ้างภายในอาคาร | <input type="checkbox"/> เสี่ยงประมาณใน การจัดหา<br>ระบบทดแทน<br><br><input type="checkbox"/> การไม่สามารถใช้งาน ระบบ<br>ระหว่างที่มีการ จัดหาระบบ<br>ทดแทน | ปานกลาง<br>๑x๕=๕ | ๑. ตรวจสอบความพร้อมของ<br>การใช้งานอุปกรณ์ดับเพลิง<br>๒. วางแผนจัดหาและติดตั้ง<br>ระบบตรวจจับควันแจ้ง<br>เตือนไฟไหม้ระบบดับเพลิง<br>๓. มีแผนในการเคลื่อนย้าย<br>อุปกรณ์ ตามลำดับ<br>ความสำคัญ  | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>อำนวยการ<br>และกลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด |
| ด้านกายภาพ<br>และสิ่งแวดล้อม<br>(Physical and Environment Risk) | จากการเกิด<br>แผ่นดินไหว | ความเสียหายด้าน<br>โครงสร้างอาจทำลาย<br>ระบบเครื่องและข้อมูล                                                                         | <input type="checkbox"/> ไม่สามารถใช้ระบบงาน<br>หรือข้อมูลได้เป็นปกติ                                                                                       | ปานกลาง<br>๑x๕=๕ | ๑. ทำการสำรองข้อมูล<br>ไว้ต่างสถานที่กัน<br>๒. จัดทำแผนสำรองฉุกเฉิน<br>เพื่อรับมือว่ามีขั้นตอน<br>ปฏิบัติอย่างไร และจะใช้<br>เครื่องทดแทนจากที่ใด<br>เพื่อ สามารถจะใช้งานได้<br>อย่างต่อเนื่อง | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด                            |
| ด้านกายภาพ<br>และสิ่งแวดล้อม<br>(Physical and Environment Risk) | จากการเกิด<br>อุทกภัย    | ความเสียหายของ<br>เครื่องคอมพิวเตอร์<br>และอุปกรณ์                                                                                   | <input type="checkbox"/> การให้บริการระบบ<br>ขาดความต่อเนื่อง                                                                                               | ปานกลาง<br>๑x๕=๕ | มีแผนในการเคลื่อนย้าย<br>อุปกรณ์ ตามลำดับ<br>ความสำคัญ                                                                                                                                         | การลด<br>ความเสี่ยง<br>(Reduction) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด                            |

| ประเภท<br>ความเสี่ยง                                               | ความเสี่ยง                                                                        | ปัจจัยความเสี่ยง                                                                                                                                                 | ผลกระทบ                                                                                                                                                                                             | ระดับ<br>ความเสี่ยง  | กิจกรรมควบคุม                                                                                                                                                        | วิธีการจัดการ<br>ความเสี่ยง             | ผู้รับผิดชอบ                                                    |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------------------------------------|
| ด้านกายภาพ<br>และสิ่งแวดล้อม<br>(Physical and<br>Environment Risk) | จากแมลง<br>หรือ สัตว์กัดแทะ<br>อุปกรณ์ คอมพิวเตอร์<br>หรือ สายไฟฟ้า/<br>สายสัญญาณ | เสี่ยงต่อการไม่สามารถ<br>ใช้งานได้ปกติ                                                                                                                           | <input type="checkbox"/> เสี่ยงประมาณในการ<br>ซ่อมแซมหรือจัดหาทดแทน<br><br><input type="checkbox"/> ไม่สามารถให้บริการระบบได้<br>อย่างต่อเนื่อง                                                     | ปานกลาง<br><br>๑x๕=๕ | ๑. ไม่ปล่อยให้มียสายไฟฟ้าหรือ<br>สายสัญญาณไม่มีท่อห่อหุ้ม<br>จนถึงจุดทางเข้าตู้ Rack<br>๒. ไม่นำอาหารหรือเครื่องดื่ม<br>มาทาน หรือเก็บไว้ใน<br>บริเวณที่มีความเสี่ยง | การลด<br>ความเสี่ยง<br>(Reduction)      | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด |
| ความเสี่ยงต่ำ                                                      |                                                                                   |                                                                                                                                                                  |                                                                                                                                                                                                     |                      |                                                                                                                                                                      |                                         |                                                                 |
| ด้านระบบข้อมูล<br>(Database Risk)                                  | จากการไม่สำรอง<br>ข้อมูล/การสำรอง<br>ข้อมูลขาด<br>การอัปเดต                       | ๑. เสี่ยงต่อการสูญหายของ<br>ข้อมูลในชั้นเล็กน้อย<br>หรือมากจนไม่สามารถ<br>ดำเนินงานได้ตามปกติ<br><br>๒. เสี่ยงต่อการมีข้อมูล<br>ที่ไม่ถูกต้องกับความ<br>เป็นจริง | <input type="checkbox"/> เสียค่าใช้จ่ายในการกู้คืน<br>ข้อมูลหรือการจัดทำขึ้นมา<br>ใหม่<br><br><input type="checkbox"/> ไม่สามารถนำข้อมูลที่มีอยู่<br>ไปใช้งานได้ เนื่องจาก<br>ขาดความมั่นใจในข้อมูล | ต่ำ<br><br>๒x๒=๔     | ๑. มีการบริหารจัดการใน<br>การทำการสำรองข้อมูล<br>(Backup) เป็นประจำ<br>อย่างสม่ำเสมอ<br>๒. มีการทดสอบการนำข้อมูล<br>กลับคืนสู่ระบบ (Restore)                         | การยอมรับ<br>ความเสี่ยง<br>(Acceptance) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด |
| ด้านโปรแกรม<br>คอมพิวเตอร์<br>(Software Risk)                      | จากการใช้ซอฟต์แวร์<br>ที่ไม่มีลิขสิทธิ์                                           | ๑. การสูญหายของข้อมูล<br>๒. การถูกฟ้องร้องเสีย<br>ชื่อเสียงและความ<br>น่าเชื่อถือของ<br>สำนักงานจังหวัด<br>มหาสารคาม                                             | <input type="checkbox"/> การใช้งานอาจไม่ได้<br>ประสิทธิภาพตาม<br>ความสามารถของซอฟต์แวร์<br>นั้น ๆ                                                                                                   | ต่ำ<br><br>๒x๒=๔     | ๑. การจัดหาซอฟต์แวร์<br>ที่ถูกกฎหมายมาใช้<br>งานตามความจำเป็น<br>๒. การรณรงค์ขอความ<br>ร่วมมือบุคลากรการ<br>ใช้งานซอฟต์แวร์ที่<br>ถูกกฎหมาย                          | การยอมรับ<br>ความเสี่ยง<br>(Acceptance) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด |

| ประเภทความเสี่ยง                                                                 | ความเสี่ยง                                   | ปัจจัยความเสี่ยง                                                                                                        | ผลกระทบ                                                                                                                                                                                                                                                                                                              | ระดับความเสี่ยง                 | กิจกรรมควบคุม                                                                                                                     | วิธีการจัดการความเสี่ยง          | ผู้รับผิดชอบ                                                                                               |
|----------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------|
|                                                                                  |                                              |                                                                                                                         | <div> <div></div> <div>สำนักงานจังหวัดมหาสารคาม</div> <div>อาจถูกฟ้องร้องเรียก</div> <div>ค่าเสียหายจากผู้เป็นเจ้าของ</div> <div>ลิขสิทธิ์ นั้นๆ</div> </div> <div> <div></div> <div>ความไม่สะดวกหากไม่ใช้งาน</div> <div>ด้วยซอฟต์แวร์ที่ไม่</div> <div>จำเป็นต้อง มีลิขสิทธิ์</div> <div>(Open Source)</div> </div> |                                 |                                                                                                                                   |                                  |                                                                                                            |
| ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) | จากระบบคอมพิวเตอร์แม่ข่ายหลักเสียหาย         | <div>๑. โพรไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ</div> <div>๒. ไม่เสี่ยงต่อความเสียหายของข้อมูลและการกู้คืนข้อมูล</div> | <div> <div></div> <div>การใช้งานระบบงาน</div> <div>ไม่สามารถใช้ได้ตามปกติ</div> </div>                                                                                                                                                                                                                               | <div>ต่ำ</div> <div>๑X๓=๓</div> | <div>๑. ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและสำรองฐานข้อมูล</div> <div>๒. จัดตั้งศูนย์สำรองข้อมูล (Backup Site)</div>                  | การยอมรับความเสี่ยง (Acceptance) | <div>กลุ่มงาน</div> <div>ยุทธศาสตร์</div> <div>และข้อมูลเพื่อ</div> <div>การพัฒนา</div> <div>จังหวัด</div> |
| ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) | จากการใช้ Wireless เข้าเครือข่ายอินเทอร์เน็ต | เสี่ยงต่อผู้ที่ไม่มิลิทธิเข้าถึงข้อมูลเข้าใช้เครือข่ายอินเทอร์เน็ตผ่านทาง WiFi                                          | <div> <div></div> <div>ข้อมูลที่เป็นความลับถูก</div> <div>เผยแพร่หรือนำไปใช้</div> <div>ประโยชน์ อันจะนำมาซึ่งการ</div> <div>ขาดความเชื่อถือของ</div> <div>สำนักงานจังหวัดมหาสารคาม</div> </div>                                                                                                                     | <div>ต่ำ</div> <div>๑X๒=๒</div> | <div>๑. ควบคุมการเข้าใช้เครือข่าย</div> <div>๒. เพิ่มความปลอดภัยในการใช้งานเพิ่มขึ้นโดยติดตั้งระบบยืนยันตน (Authentication)</div> | การยอมรับความเสี่ยง (Acceptance) | <div>กลุ่มงาน</div> <div>ยุทธศาสตร์</div> <div>และข้อมูลเพื่อ</div> <div>การพัฒนา</div> <div>จังหวัด</div> |

| ประเภทความเสี่ยง                                                                 | ความเสี่ยง                                                   | ปัจจัยความเสี่ยง                                                                                                                                                    | ผลกระทบ                                                                                                                                                                                                                                | ระดับความเสี่ยง | กิจกรรมควบคุม                                                                                                                                                                           | วิธีการจัดการความเสี่ยง          | ผู้รับผิดชอบ                                    |
|----------------------------------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------------------|
| ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) | จากการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขัดข้อง | ๑. ไม่สามารถใช้งานระบบงานของสำนักงานจังหวัดมหาสารคามผ่านเครือข่ายอินเทอร์เน็ตได้<br>๒. ไม่สามารถเชื่อมต่อภายนอกสำนักงานจังหวัดมหาสารคามผ่านเครือข่ายอินเทอร์เน็ตได้ | <input type="checkbox"/> ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้ประโยชน์ อันจะนำมาซึ่งการขาดความเชื่อถือของสำนักงานจังหวัดมหาสารคาม<br><input type="checkbox"/> บุคคลภายนอกไม่สามารถเข้าใช้ Web Server หรือ ค้นหาข้อมูลที่ต้องการได้ | ต่ำ<br>๑x๒=๒    | ตรวจสอบระบบเครือข่ายสื่อสารหลัก                                                                                                                                                         | การยอมรับความเสี่ยง (Acceptance) | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |
| ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)                                           | มีช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ภายในองค์กร              | ๑. การถูกขโมยข้อมูล<br>๒. โปรแกรมเสียหาย<br>๓. การใช้ช่องโหว่ของโปรแกรมหรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง                                                   | <input type="checkbox"/> ลดความน่าเชื่อถือต่อสำนักงานจังหวัดมหาสารคาม หากข้อมูลถูก ขโมยไปและนำไปเผยแพร่<br><input type="checkbox"/> กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานจังหวัดมหาสารคามเป็นอย่างยิ่ง                    | ต่ำ<br>๑x๒=๒    | ๑. ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง<br>๒. มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ | การยอมรับความเสี่ยง (Acceptance) | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |

| ประเภทความเสี่ยง                       | ความเสี่ยง                                                   | ปัจจัยความเสี่ยง                                                                                                                                                                              | ผลกระทบ                                                                                                                                                                                                                                                                                                                                                                                                           | ระดับความเสี่ยง | กิจกรรมควบคุม                                                                                                                                                                                                                                                                                                                        | วิธีการจัดการความเสี่ยง          | ผู้รับผิดชอบ                                    |
|----------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------------------|
|                                        |                                                              |                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                   |                 | ๓. ตรวจสอบช่องโหว่และดำเนินการปิดช่องโหว่                                                                                                                                                                                                                                                                                            |                                  |                                                 |
| ด้านโปรแกรมคอมพิวเตอร์ (Software Risk) | การใช้โปรแกรมที่พัฒนาโดย Outsource ขาดแผนบริหารความต่อเนื่อง | ๑. เสี่ยงต่อการถูกขโมยข้อมูล<br>๒. เสี่ยงต่อการทำความเสียหายแก่ โปรแกรม<br>๓. ไม่สามารถแก้ไขข้อบกพร่องได้เอง<br>๔. โปรแกรม และข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว<br>๕. เสียค่าใช้จ่ายสูง | <div><input type="checkbox"/>ลดความน่าเชื่อถือต่อสำนักงานจังหวัดมหาสารคาม หากข้อมูลถูกขโมยไปและนำไปเผยแพร่</div> <div><input type="checkbox"/>กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานจังหวัดมหาสารคามเป็นอย่างยิ่ง</div> <div><input type="checkbox"/>จัดทำงบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการบำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัปเดตอยู่เสมอ</div> | ต่ำ<br>๑x๒=๒    | ๑. การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level<br>๒. การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล ER Diagram<br>๓. ให้มีการส่งมอบ Source Code ในรูปแบบอิเล็กทรอนิกส์ไฟล์โนฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้<br>๔. หากมีการพัฒนา Library ด้วยตนเองต้องส่ง Source Code Library ที่สามารถแก้ไขได้ | การยอมรับความเสี่ยง (Acceptance) | กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด |

| ประเภท<br>ความเสี่ยง | ความเสี่ยง | ปัจจัยความเสี่ยง | ผลกระทบ | ระดับ<br>ความเสี่ยง | กิจกรรมควบคุม                                                                                                                                                                                                                                                                                                                                                                                                                                                           | วิธีการจัดการ<br>ความเสี่ยง | ผู้รับผิดชอบ |
|----------------------|------------|------------------|---------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------|
|                      |            |                  |         |                     | <p>๕. มีการถ่ายทอดความรู้เทคโนโลยี ในการพัฒนาระบบให้กับเจ้าหน้าที่</p> <p>๖. มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม</p> <p>๗. จัดทำข้อตกลงการรักษาข้อมูลความลับของหน่วยงานระหว่างผู้รับจ้างกับผู้ว่าจ้าง</p> <p>๘. มีแผนการบำรุงรักษาระบบงานที่ครอบคลุมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) การอัปเดตเมื่อมี Version ใหม่การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหายเป็นต้น</p> |                             |              |

| ประเภท<br>ความเสี่ยง                                                                                                          | ความเสี่ยง                                              | ปัจจัยความเสี่ยง                                                                                                                                                | ผลกระทบ                                                                                                                                                                                 | ระดับ<br>ความเสี่ยง | กิจกรรมควบคุม                                                                                                                                                                                                                                                                                                                                                                                                  | วิธีการจัดการ<br>ความเสี่ยง             | ผู้รับผิดชอบ                                                    |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------------------------------------------------|
| ด้านบุคลากร<br>(Human Risk)<br><br>ด้านอุปกรณ์เทคโนโลยี<br>สารสนเทศและการสื่อสาร<br>(Hardware and Data<br>Communication Risk) | ความเสี่ยงจากการ<br>ถูก Black List<br>โดย Search Engine | ๑. ผู้ใช้งานที่ต้องการ<br>ข้อมูลของจังหวัด<br>มหาสารคาม<br>หรือประชาชนทั่วไป<br>ไม่สามารถเข้าใช้งาน<br>Web Server ได้<br><br>๒. ไม่สามารถใช้งาน<br>เครือข่ายได้ | <input type="checkbox"/> ลดความน่าเชื่อถือ หรือ<br>ข้อมูลของจังหวัด<br>มหาสารคาม<br><br><input type="checkbox"/> สำนักงานจังหวัดมหาสารคาม<br>อาจถูก ฟ้องร้องโดยผู้<br>มีส่วนได้ส่วนเสีย | ต่ำ<br><br>๑x๒=๒    | ๑. ติดตั้งโปรแกรมเพื่อ<br>ตรวจสอบให้แน่ใจว่าไม่มี<br>อุปกรณ์ใดในเครือข่าย<br>จังหวัดฯ ได้ส่ง Spam<br>ออกไปยังเครือข่าย<br>อินเทอร์เน็ต<br><br>๒. ติดตั้งระบบการตรวจสอบ<br>แฟ้มข้อมูลก่อนการ<br>อัปโหลดข้อมูลขึ้น<br>Web Server หรือ<br>FTP Server<br><br>๓. มีการอัปเดตโปรแกรม<br>และ Signature อย่าง<br>สม่ำเสมอ และการทำ<br>การบำรุงรักษา<br>(Maintenance) ทั้ง<br>ฮาร์ดแวร์และซอฟต์แวร์<br>พร้อมทั้ง Update | การยอมรับ<br>ความเสี่ยง<br>(Acceptance) | กลุ่มงาน<br>ยุทธศาสตร์<br>และข้อมูลเพื่อ<br>การพัฒนา<br>จังหวัด |

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สำนักงานจังหวัดมหาสารคาม  
ระดับความเสี่ยงที่จัดทำแผนการบริหารความเสี่ยง: ปานกลาง - สูง วัตถุประสงค์: เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ  
ของสำนักงานจังหวัดมหาสารคาม บรรลุเป้าประสงค์ของการบริหารความเสี่ยง ผู้รับผิดชอบ: กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

| ประเภทความเสี่ยง/<br>กิจกรรม                           | แผนปฏิบัติ                                                                              | ระยะเวลา       | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                                         |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------|------|-----|------|------|-----|------|------|-----|------|----------|-----------------------------------------------------------------|
|                                                        |                                                                                         |                | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                                                 |
| ๑. ความเสี่ยงจากการบุกรุกโจมตีจากภายนอก<br>(ระดับ สูง) | ๑. ติดตั้งระบบตรวจจับ<br>ป้องกันและเตือนภัย<br>การถูกบุกรุก(NGFW,<br>LogYou VisibleOne) |                | ↔    | →   |      |      |     |      |      |     |      |          | ระดับความ<br>เสี่ยงลดลง<br>จาก ๒๐<br>(สูงมาก)<br>เหลือ ๑๕ (สูง) |
|                                                        | ๒. จัดทำแผนหรือ<br>ขั้นตอนการปฏิบัติ<br>ที่จำเป็นเพื่อป้องกัน<br>การถูกบุกรุกตามลำดับ   | ทุก<br>๓ เดือน |      | ↔   |      |      | ↔   |      |      | ↔   |      |          |                                                                 |
|                                                        | ๓. ตรวจสอบ Policy<br>และ Log ของระบบ<br>ป้องกันการบุกรุกระบบ<br>เครือข่าย               | ทุกวัน         | ←    |     |      |      |     |      |      |     | →    |          |                                                                 |

| ประเภทความเสี่ยง/<br>กิจกรรม                                                                                         | แผนปฏิบัติ                                                                                    | ระยะเวลา                              | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                                          |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------|------|-----|------|------|-----|------|------|-----|------|----------|------------------------------------------------------------------|
|                                                                                                                      |                                                                                               |                                       | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                                                  |
| ๒. ความเสี่ยงจาก<br>การติดไวรัส<br>คอมพิวเตอร์<br>หรือ Malware<br>(ปานกลาง)                                          | ๑. ติดตั้งระบบป้องกัน<br>ไวรัสคอมพิวเตอร์กับ<br>เครื่องแม่ข่ายและ<br>เครื่องลูกข่ายทุกเครื่อง | ทุกครั้งที่<br>ติดตั้ง<br>เครื่องใหม่ |      |     |      |      |     |      |      |     |      |          | ระดับความ<br>เสี่ยงลดลง<br>จาก ๑๖ (สูง)<br>เหลือ ๑๒<br>(ปานกลาง) |
|                                                                                                                      | ๒. อัปเดตข้อมูลไวรัส<br>อย่างสม่ำเสมอ                                                         | ทุกวัน                                | ←    |     |      |      |     |      |      |     | →    |          |                                                                  |
| ๓. ความเสี่ยงจาก<br>การถูกโจรกรรม<br>ฐานข้อมูล<br>(ปานกลาง)                                                          | ๑. ติดตั้งระบบป้องกัน<br>ไวรัสกับเครื่องแม่ข่าย<br>ทุกเครื่อง                                 | ทุกครั้งที่<br>ติดตั้ง<br>เครื่องใหม่ | ←    |     |      |      |     |      |      |     | →    |          | ระดับความ<br>เสี่ยงลดลงจาก<br>๑๕ (สูง)<br>เหลือ ๑๐<br>(ปานกลาง)  |
|                                                                                                                      | ๒. อัปเดตข้อมูลไวรัส<br>อย่างสม่ำเสมอ                                                         | ทุกวัน                                | ←    |     |      |      |     |      |      |     | →    |          |                                                                  |
| ๔. ความเสี่ยงจาก<br>การโจมตีเครื่องแม่<br>ข่ายของจังหวัดฯ<br>ไม่ให้บริการได้ (denial<br>of service-dos)<br>(ปานกลาง) | ๑. ติดตั้งระบบป้องกัน<br>ไวรัสกับเครื่องแม่ข่าย                                               | ทุกครั้งที่<br>ติดตั้ง<br>เครื่องใหม่ | ←    |     |      |      |     |      |      |     | →    |          | ระดับความ<br>เสี่ยงลดลงจาก<br>๑๕ (สูง)<br>เหลือ ๑๐<br>(ปานกลาง)  |
|                                                                                                                      | ๒. อัปเดตข้อมูลไวรัส<br>อย่างสม่ำเสมอ                                                         | ทุกวัน                                | ←    |     |      |      |     |      |      |     | →    |          |                                                                  |

| ประเภทความเสี่ยง/<br>กิจกรรม                                                                                                    | แผนปฏิบัติ                                                                                                                  | ระยะเวลา        | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                                     |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------|------|-----|------|------|-----|------|------|-----|------|----------|-------------------------------------------------------------|
|                                                                                                                                 |                                                                                                                             |                 | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                                             |
| ๕. การถูกฟ้องร้อง<br>จากการละเมิดข้อมูล<br>ส่วนบุคคลตาม<br>พระราชบัญญัติ<br>คุ้มครองข้อมูลส่วน<br>บุคคล (PDPA)<br><br>(ปานกลาง) | ๑. แต่งตั้ง<br>คณะกรรมการ<br>อำนาจการและ<br>คณะกรรมการ<br>ดำเนินการที่เกี่ยวข้อง<br>กับพรบ.ข้อมูลส่วนบุคคล                  | ทบทวน<br>ทุกปี  | ↔    |     |      |      |     |      |      |     |      |          | ระดับความ<br>เสี่ยงยังคงอยู่<br>อยู่ที่ระดับ ๘<br>(ปานกลาง) |
|                                                                                                                                 | ๒. อบรมให้ความรู้<br>ความเข้าใจเกี่ยวกับ<br>นโยบายระเบียบและ<br>แนวปฏิบัติแก่บุคลากร<br>ตามพรบ. คุ้มครอง<br>ข้อมูลส่วนบุคคล | ปีละ<br>๑ ครั้ง |      | ↔   |      |      | ↔   |      |      | ↔   |      |          |                                                             |
|                                                                                                                                 | ๓. จัดทำนโยบาย<br>ระเบียบและแนว<br>ปฏิบัติในการจัดการ<br>ข้อมูลส่วนบุคคลรวมถึง<br>ทบทวนมาตรการและ<br>แนวปฏิบัติปีละ ๑ ครั้ง | ทบทวน<br>ทุกปี  | ↔    |     |      | ↔    |     |      | ↔    |     |      |          |                                                             |

| ประเภทความเสี่ยง/<br>กิจกรรม | แผนปฏิบัติ                                                                                                                                                                                               | ระยะเวลา                  | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|------|-----|------|------|-----|------|------|-----|------|----------|-------------------------|
|                              |                                                                                                                                                                                                          |                           | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                         |
|                              | ๔. พัฒนาสถาปัตยกรรมขององค์กร (Enterprise Architecture EA) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถเชื่อมโยงระบบและข้อมูลได้ และสามารถตอบสนองได้ หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น | ทุกครั้งที่มีการพัฒนาระบบ | ←    |     |      |      |     |      |      |     | →    |          |                         |
|                              | ๕. พัฒนาความรู้ของบุคลากรทั้งผู้ใช้ข้อมูลผู้ควบคุมข้อมูลและผู้ประมวลข้อมูลส่วนบุคคลให้เกิด การตระหนักมีความรู้และทักษะในการจัดการข้อมูลส่วนบุคคล                                                         | พัฒนาอย่างต่อเนื่อง       | ←    |     |      |      |     |      |      |     | →    |          |                         |

| ประเภทความเสี่ยง/<br>กิจกรรม                                                                                | แผนปฏิบัติ                                                                                                       | ระยะเวลา        | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                                               |
|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-----------------|------|-----|------|------|-----|------|------|-----|------|----------|-----------------------------------------------------------------------|
|                                                                                                             |                                                                                                                  |                 | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                                                       |
|                                                                                                             | ๖. จัดให้มีการซ้อม<br>กระบวนการตอบสนอง<br>ในกรณีเกิดการละเมิด<br>ข้อมูลส่วนบุคคลขึ้น<br>อย่างน้อยหนึ่งครั้งต่อปี | ปีละ<br>๑ ครั้ง |      |     | ↔    |      |     | ↔    |      |     | ↔    |          |                                                                       |
| ๖. การไม่สามารถใช้<br>งานโปรแกรม software<br>ข้อมูลหลักของระบบ<br>สารสนเทศจังหวัด<br>มหาสารคาม<br>(ปานกลาง) | ๑. ดำเนินการตามแผน<br>manual system โดย<br>ซ้อมแผนปีละ ๑ ครั้ง                                                   | ปีละ<br>๑ ครั้ง |      |     | ↔    |      |     | ↔    |      |     | ↔    |          | ระดับความ<br>เสี่ยงอยู่ที่ ๖<br>(ปานกลาง)                             |
| ๗. เจ้าหน้าที่ใช้<br>คอมพิวเตอร์/<br>เครือข่ายผิด<br>วัตถุประสงค์<br>(ปานกลาง)                              | ๑. ให้ความรู้การใช้งาน<br>ระบบคอมพิวเตอร์<br>อย่างปลอดภัย                                                        | ปีละ<br>๑ ครั้ง |      |     | ↔    |      |     | ↔    |      |     | ↔    |          | ระดับความ<br>เสี่ยงลดลง<br>จาก ๙<br>(ปานกลาง)<br>เหลือ ๖<br>(ปานกลาง) |
|                                                                                                             | ๒. การมีข้อตกลงที่<br>ผู้ใช้งานต้องเป็น<br>ผู้รับผิดชอบในการนำ<br>อุปกรณ์เครื่อง                                 | ตลอดเวลา        | ←    |     |      |      |     |      |      |     | →    |          |                                                                       |

| ประเภทความเสี่ยง/<br>กิจกรรม                                            | แผนปฏิบัติ                                                                                                                    | ระยะเวลา | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|----------|------|-----|------|------|-----|------|------|-----|------|----------|----------------------------------------|
|                                                                         |                                                                                                                               |          | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                        |
|                                                                         | คอมพิวเตอร์หรือ resource ต่างๆ ใช้ ในทางที่ผิดรวมถึงการ บันทึกรการใช้งานและ รายงานการใช้งานของ ใช้ที่ฝ่าฝืนต่อ ผู้บังคับบัญชา |          |      |     |      |      |     |      |      |     |      |          |                                        |
| ๘. การโจรกรรม อุปกรณ์ คอมพิวเตอร์/ อุปกรณ์ต่อพ่วง คอมพิวเตอร์ (ปานกลาง) | ๑. ควบคุมการเข้าออก อาคาร                                                                                                     | ตลอดเวลา |      |     |      |      |     |      |      |     |      |          | ระดับความ เสี่ยงอยู่ ระดับ ๖ (ปานกลาง) |
|                                                                         | ๒. ควบคุมการขนย้าย เครื่องคอมพิวเตอร์                                                                                         | ตลอดเวลา |      |     |      |      |     |      |      |     |      |          |                                        |
|                                                                         | ๓. ติดตั้งกล้องวงจรปิด ให้ครอบคลุมทุกพื้นที่มี เครื่องเฟอร์นิเจอร์และ อุปกรณ์ติดตั้งอยู่                                      | ตลอดเวลา |      |     |      |      |     |      |      |     |      |          |                                        |

| ประเภทความเสี่ยง/<br>กิจกรรม                              | แผนปฏิบัติ                                                                                                                                                         | ระยะเวลา | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า |                                                                       |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|-----|------|------|-----|------|------|-----|------|----------|-------------------------|-----------------------------------------------------------------------|
|                                                           |                                                                                                                                                                    |          | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                         |                                                                       |
| ๙. ระบบ<br>กระแสไฟฟ้าขัดข้อง<br>(ปานกลาง)                 | ๑. ตรวจสอบระบบ<br>สำรองไฟฟ้า (UPS)                                                                                                                                 | ทุกวัน   |      |     |      |      |     |      |      |     |      |          |                         | ระดับความ<br>เสี่ยงลดลง<br>จาก ๘ (ปาน<br>กลาง) เหลือ<br>(ปานกลาง)     |
|                                                           | ๒. ตรวจสอบการ<br>ทำงานของเครื่อง<br>กำเนิดไฟฟ้า<br>(Electrical<br>Generator)                                                                                       | ทุกวัน   |      |     |      |      |     |      |      |     |      |          |                         |                                                                       |
| ๑๐. ข้อมูลรั่วไหล<br>จากการเปลี่ยนมือ<br>ผู้ใช้ (ปานกลาง) | มีการบริหารจัดการต่อ<br>อุปกรณ์เก็บข้อมูลเช่น<br>Hard disk แผ่น DVD<br>/CD USB ให้แน่ใจว่า<br>ข้อมูลได้ถูกลบทิ้งอย่าง<br>ถาวรหรือได้ทำลาย<br>อุปกรณ์นั้นๆ ทิ้งแล้ว | ตลอดเวลา |      |     |      |      |     |      |      |     |      |          |                         | ระดับความ<br>เสี่ยงลดลง<br>จาก ๑๐<br>(ปานกลาง)<br>เหลือ (ปาน<br>กลาง) |

| ประเภทความเสี่ยง/<br>กิจกรรม | แผนปฏิบัติ                                                     | ระยะเวลา     | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                                          |
|------------------------------|----------------------------------------------------------------|--------------|------|-----|------|------|-----|------|------|-----|------|----------|------------------------------------------------------------------|
|                              |                                                                |              | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                                                  |
| ๑๑. อัคคีภัย<br>(ปานกลาง)    | ๑. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง                 | ทุกวัน       | ←    |     |      |      |     |      |      |     | →    |          | ระดับความเสี่ยงลดลง<br>จาก ๑๐<br>(ปานกลาง)<br>เหลือ<br>(ปานกลาง) |
|                              | ๒. ติดตั้งระบบตรวจจับไฟระบบดับเพลิงและแจ้งเตือนการเกิดอัคคีภัย | ตลอดเวลา     | ←    |     |      |      |     |      |      |     | →    |          |                                                                  |
|                              | ๓. จัดทำและซ้อมแผนสำรองฉุกเฉิน                                 | ปีละ ๑ ครั้ง |      | ↔   |      |      | ↔   |      |      | ↔   |      |          |                                                                  |
| ๑๒. แผ่นดินไหว<br>(ปานกลาง)  | ๑. ทำการสำรองข้อมูลไว้ต่างสถานที่กัน                           | ตลอดเวลา     | ←    |     |      |      |     |      |      |     | →    |          | ระดับความเสี่ยงอยู่ที่ ๕<br>(ปานกลาง)                            |
|                              | ๒. จัดทำและซ้อมแผนสำรองฉุกเฉิน                                 | ปีละ ๑ ครั้ง |      | ↔   |      |      | ↔   |      |      | ↔   |      |          |                                                                  |
| ๑๓. อุทกภัย<br>(ปานกลาง)     | ๑. จัดทำและซ้อมแผนสำรองฉุกเฉิน                                 | ปีละ ๑ ครั้ง |      | ↔   |      |      | ↔   |      |      |     | ↔    |          | ระดับความเสี่ยงอยู่ที่ ๕<br>(ปานกลาง)                            |

| ประเภทความเสี่ยง/<br>กิจกรรม                                             | แผนปฏิบัติ                                                                                   | ระยะเวลา | ๒๕๖๗ |     |      | ๒๕๖๘ |     |      | ๒๕๖๙ |     |      | งบประมาณ | ผลลัพธ์<br>ความก้าวหน้า                                               |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------|------|-----|------|------|-----|------|------|-----|------|----------|-----------------------------------------------------------------------|
|                                                                          |                                                                                              |          | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ | ๑-๔  | ๕-๘ | ๙-๑๒ |          |                                                                       |
| ๑๔. แผลงหรือสัตว์<br>กัดแทะอุปกรณ์<br>คอมพิวเตอร์หรือ<br>สายไฟ/สายสัญญาณ | ๑. ไม่ปล่อยให้หมี<br>สายไฟฟ้าหรือ<br>สายสัญญาณไม่มีท่อ<br>ห่อหุ้มจนถึงจุดทางเข้า<br>ตู้ Rack | ตลอดเวลา | ←    |     |      |      |     |      |      |     | →    |          | ระดับความ<br>เสี่ยงลดลงจาก<br>๑๐<br>(ปานกลาง)<br>เหลือ ๕<br>(ปานกลาง) |
|                                                                          | ๒. ไม่นำอาหารหรือ<br>เครื่องดื่มมาทานหรือ<br>เก็บไว้ในบริเวณที่มี<br>ความเสี่ยง              | ตลอดเวลา | ←    |     |      |      |     |      |      |     | →    |          |                                                                       |

บทที่ ๔  
สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งเมื่อเทคโนโลยี สารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อนการดำเนินงานขององค์กรทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้นในแต่ละวันข้อมูล มหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงาน ภายในสำนักงานจังหวัด ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสถานะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือสูญหาย และถูกนำไปใช้ในทางที่ผิดทั้งจากบุคคลภายใน และภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหาจึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการความเสี่ยงในองค์กร

๑. การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่าง ๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงในระดับสูงและปานกลาง ดังต่อไปนี้

| ความเสี่ยง                                                                                 | แนวทางปฏิบัติ                                                                                                 |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| ๑. การบุกรุกโจมตีจากภายนอก                                                                 | ๑. ติดตั้งระบบเครือข่ายเพื่อป้องกัน และเตือนภัย (NGFW, LogYou VisibleOne)                                     |
|                                                                                            | ๒. จัดทำแผนทบทวน ขั้นตอนปฏิบัติที่จำเป็นตามลำดับ                                                              |
|                                                                                            | ๓. ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย                                                |
| ๒. การติดไวรัสคอมพิวเตอร์หรือ Malware                                                      | ๑. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ                                                                             |
| ๓. การถูกโจรกรรมฐานข้อมูล                                                                  | ๑. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย                                                                   |
|                                                                                            | ๒. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ                                                                             |
| ๔. การโจมตี เครื่องแม่ข่ายของจังหวัดฯ ไม่ให้สามารถให้บริการได้ (Denial of Service-DoS)     | ๑. ติดตั้งระบบป้องกันไวรัสกับเครื่องแม่ข่าย                                                                   |
|                                                                                            | ๒. อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ                                                                             |
| ๕. การถูกฟ้องร้องจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) | ๑. แต่งตั้งคณะกรรมการอำนวยการ และคณะกรรมการดำเนินการที่เกี่ยวข้องกับ พรบ. ข้อมูลส่วนบุคคล                     |
|                                                                                            | ๒. อบรมให้ความรู้ ความเข้าใจ เกี่ยวกับนโยบายระเบียบ และแนวปฏิบัติ แก่บุคลากร ตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล |

| ความเสี่ยง                                                                    | แนวทางปฏิบัติ                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                               | ๓. จัดทำนโยบาย ระเบียบ และแนวปฏิบัติ ในการจัดการข้อมูลส่วนบุคคล รวมถึงทบทวนมาตรการและแนวปฏิบัติ ปีละ ๑ ครั้ง                                                                                                            |
|                                                                               | ๔. พัฒนาสถาปัตยกรรมขององค์กร (Enterprise Architecture: EA) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถพิจารณาความเชื่อมโยงของระบบและข้อมูลได้ และสามารถตอบสนองได้ หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น |
|                                                                               | ๕. พัฒนาความรู้ของบุคลากร ทั้งผู้ใช้ข้อมูล ผู้ควบคุม ข้อมูล และผู้ประมวลผลข้อมูลส่วนบุคคล ให้เกิด การตระหนัก มีความรู้ และทักษะในการจัดการ ข้อมูลส่วนบุคคล                                                              |
|                                                                               | ๖. จัดให้มีการซ้อมกระบวนการตอบสนองในกรณีเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น อย่างน้อย ๑ ครั้งต่อปี                                                                                                                         |
| ๖. การไม่สามารถใช้งานโปรแกรม (Software) ข้อมูลหลักของสำนักงานจังหวัดมหาสารคาม | ๑. ดำเนินการตามแผน Manual System โดยซ้อมแผน ปีละ ๑ ครั้ง                                                                                                                                                                |
| ๗. เจ้าหน้าที่ใช้คอมพิวเตอร์/ เครือข่ายผิดวัตถุประสงค์                        | ๑. ให้ความรู้การใช้งานระบบคอมพิวเตอร์อย่างปลอดภัย                                                                                                                                                                       |
| ๘. การโจรกรรมอุปกรณ์คอมพิวเตอร์/อุปกรณ์ต่อพ่วงคอมพิวเตอร์                     | ๑. ควบคุมการเข้าออกอาคาร                                                                                                                                                                                                |
|                                                                               | ๒. ควบคุมการขนย้ายเครื่องคอมพิวเตอร์                                                                                                                                                                                    |
|                                                                               | ๓. ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกพื้นที่มีเครื่องคอมพิวเตอร์และ อุปกรณ์ติดตั้งอยู่                                                                                                                                   |
| ๙. ระบบกระแสไฟฟ้าขัดข้อง                                                      | ๑. ตรวจสอบระบบสำรอง ไฟฟ้า (UPS)                                                                                                                                                                                         |
|                                                                               | ๒. ตรวจสอบการทำงานของเครื่องกำเนิดไฟฟ้า (Electrical Generator)                                                                                                                                                          |
| ๑๐. ข้อมูลรั่วไหลจากการเปลี่ยนมือผู้ใช้                                       | ๑. บริหารจัดการต่ออุปกรณ์เก็บข้อมูล เช่น Hard Disk หรือ Cloud ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้น ๆ ทิ้งแล้วหากทำได้                                                                         |
| ๑๑. การเกิดอัคคีภัย                                                           | ๑. ติดตั้งและตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง                                                                                                                                                                |
|                                                                               | ๒. ติดตั้งระบบตรวจจับควันระบบดับเพลิง และการแจ้งเตือนการเกิดอัคคีภัย                                                                                                                                                    |



กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด  
สำนักงานจังหวัดมหาสารคาม