แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ
โรงพยาบาลแม่จริมระยะ 4 ปี
(พ.ศ. 2565-2568)

แผนแม่บทเทคโนโลยีสารสนเทศปี 2565-2568
คณะกรรมการสารสนเทศโรงพยาบาลแม่จริม จังหวัดน่าน

วิสัยทัศน์(Vision)

“โรงพยาบาลคุณภาพ บริการประทับใจ เทคโนโลยีทันสมัย เพื่อประชาชนสุขภาพดี”

ความหมายของวิสัยทัศน์

1. โรงพยาบาลคุณภาพ หมายถึง โรงพยาบาลให้บริการด้านสุขภาพที่ได้มาตรฐาน ปลอดภัย และมีการบริหารจัดการที่มีประสิทธิภาพ
2. บริการประทับใจ หมายถึง ผู้รับบริการได้รับการจัดการด้านสุขภาพอย่างเหมาะสม ปลอดภัยและมีความประทับใจ
3. เทคโนโลยีทันสมัย หมายถึง การพัฒนาและประยุกต์ใช้ระบบเทคโนโลยีและสารสนเทศ ในระบบบริการและระบบสนับสนุนได้อย่างมีประสิทธิภาพและตอบสนองความต้องการขององค์กร
4. ประชาชนสุขภาพดี หมายถึง ประชาชนในเครือข่ายสุขภาพ มีสุขภาพกายและจิตที่สมบูรณ์แข็งแรง ปัญหาสุขภาพสำคัญในพื้นที่ได้รับการจัดการโดยกระบวนการมีส่วนร่วมของภาคีเครือข่าย

พันธกิจ (Mission)

1) พัฒนาระบบบริการตามมาตรฐานโดยยึดผู้ป่วยเป็นศูนย์กลาง	Service
2) พัฒนาศักยภาพบุคลากรเพื่อให้บริการอย่างมีประสิทธิภาพ	people
3) ดูแลสุขภาพประชาชนในพื้นที่โดยภาคีเครือข่ายมีส่วนร่วม	PP&P
4) พัฒนาระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ	Governance

ค่านิยมองค์กร (Core Value)

“บริการด้วยใจ ใฝ่เรียนรู้ คู่คุณธรรม”

สมรรถนะหลักขององค์กร (Core Competencies)

“ให้บริการดุจญาติมิตร”

ประเด็นยุทธศาสตร์(Strategic Issues)

พันธกิจ (Mission)

1) พัฒนาระบบบริการตามมาตรฐานโดยยึดผู้ป่วยเป็นศูนย์กลาง Service

2) พัฒนาศักยภาพบุคลากรเพื่อให้บริการอย่างมีประสิทธิภาพ people

3) ดูแลสุขภาพประชาชนในพื้นที่โดยภาคีเครือข่ายมีส่วนร่วม PP&P

4) พัฒนาระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ Governance

เป้าประสงค์(Goals)

1) **พัฒนาระบบบริการตามมาตรฐานโดยยึดผู้ป่วยเป็นศูนย์กลาง**
   - ผู้รับบริการได้รับการจัดการด้านสุขภาพอย่างเหมาะสม ปลอดภัยและมีความประทับใจ

2) **พัฒนาศักยภาพบุคลากรเพื่อให้บริการอย่างมีประสิทธิภาพ**
   - บุคลากรมีองค์ความรู้และพฤติกรรมบริการตามความคาดหวังขององค์กร

3) **ดูแลสุขภาพประชาชนในพื้นที่โดยภาคีเครือข่ายมีส่วนร่วม**
   - ปัญหาสุขภาพสำคัญในพื้นที่ได้รับการจัดการโดยกระบวนการมีส่วนร่วมของภาคีเครือข่าย

4) **พัฒนาระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ**
   - โรงพยาบาลมีระบบเทคโนโลยีสารสนเทศที่ตอบสนองความต้องการขององค์กร

สร้างเสริมสุขภาพเป็นเลิศ (Promotion Prevention and Protection Excellence)

“ดูแลสุขภาพประชาชนในพื้นที่โดยภาคีเครือข่ายมีส่วนร่วม “

(1) ประชาชนทุกกลุ่มวัยได้รับการส่งเสริมสุขภาพ

(2) โรคและปัจจัยเสี่ยงด้านสุขภาพได้รับการจัดการอย่างมีประสิทธิภาพ

(3) ประชาชนฉลาดใช้ผลิตภัณฑ์สุขภาพและอาหารที่ปลอดภัย

(4) สนับสนุนระบบการจัดการขยะและสิ่งแวดล้อมที่ได้มาตรฐาน

(5) ทุกภาคส่วนร่วมพัฒนาคุณภาพชีวิตประชาชน

บริการเป็นเลิศ (Services Excellence)

พัฒนาระบบบริการตามมาตรฐานโดยยึดผู้ป่วยเป็นศูนย์กลาง

(1) ผู้ป่วยระยะยาวได้รับการดูแลตามมาตรฐานการดำเนินงานศูนย์ดูแลสุขภาพอย่างต่อเนื่อง

(2) ผู้ป่วยโรคไม่ติดต่อเรื้อรังและ Palliativeได้รับการดูแลตามมาตรฐาน

(3) ผู้รับบริการได้รับยาอย่างถูกต้องและเหมาะสม

(4) ประชาชนเข้าถึงบริการแพทย์แผนไทยและมีการใช้สมุนไพรอย่างเหมาะสม

(5) ผู้ป่วยโรคซึมเศร้าเข้าถึงบริการ และลดการฆ่าตัวตายสำเร็จ

(6) ผู้ป่วย Stroke STEMI เข้าถึงบริการและได้รับการดูแลตามมาตรฐาน

(7) ผู้ป่วยฉุกเฉินเข้าถึงบริการ และได้รับการดูแลส่งต่อตามมาตรฐานการแพทย์ฉุกเฉิน

(8) พัฒนาระบบบริการอนามัยมารดาและทารกตามเกณฑ์มาตรฐาน

(9) ลดอัตราตายจากการติดเชื้อในกระแสเลือด

(10) สนับสนุนการดำเนินงานโครงการตามพระราชดำริและโครงการเฉลิมพระเกียรติอย่างต่อเนื่อง

บุคลากรเป็นเลิศ (People Excellence)

พัฒนาศักยภาพบุคลากรเพื่อให้บริการอย่างมีประสิทธิภาพ

(1) พัฒนาองค์ความรู้ ทักษะ และสมรรถนะของบุคลากรอย่างต่อเนื่อง

(2) พัฒนาโรงพยาบาลให้เป็นองค์กรสร้างสุข

บริหารเป็นเลิศ (Governance Excellence)

พัฒนาระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

(1) บริหารทรัพยากรตามหลักธรรมาภิบาล และเศรษฐกิจพอเพียง

(2) พัฒนาองค์กรคุณภาพตามมาตรฐาน HA อย่างต่อเนื่อง

(3) พัฒนาระบบเทคโนโลยีสารสนเทศ

(4) สนับสนุนการพัฒนาผลงานวิชาการ งานวิจัย หรือนวัตกรรมสุขภาพในบุคลากรทุกระดับ

แผนแม่บทเทคโนโลยีสารสนเทศ

ส่วนที่ 1 บททั่วไป

โรงพยาบาลแม่จริมตระหนักถึงการพัฒนาเทคโนโลยีสารสนเทศที่เหมาะสม กับสภาวะเศรษฐกิจสังคมและความก้าวหน้าทางเทคโนโลยีด้วยความร่วมมือและการมีส่วนร่วมจากทุกภาคส่วนทั้งภายในและภายนอกองค์กรเพื่อให้การดำเนินงานของโรงพยาบาลเป็นไปอย่างมีประสิทธิภาพสามารถบรรลุวิสัยทัศน์และพันธกิจตามที่กำหนดไว้

วิสัยทัศน์

“โรงพยาบาลคุณภาพ บริการประทับใจ เทคโนโลยีทันสมัย เพื่อประชาชนสุขภาพดี”

พันธกิจ

“สารสนเทศโรงพยาบาลแม่จริมจะเพิ่มศักยภาพด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพเพื่อตอบสนองต่อภารกิจและและพันธกิจของโรงพยาบาลอย่างยั่งยืน”

เป้าหมายหลัก

1. ด้านการบริการจัดมีให้มีการจัดเก็บฐานข้อมูลประวัติการดูแลรักษาอย่างครบถ้วนและปลอดภัย โดยมี Hardware Software และ People ware ที่มีศักยภาพและพร้อมใช้

2. ด้านการพัฒนาคุณภาพจัดให้มีการรวบรวมข้อมูลผลการดำเนินงาน ข้อมูลความเสี่ยง และตัวชี้วัด ที่ถูกต้องครอบคลุมพร้อมนำไปวิเคราะห์ทบทวนเพื่อหาโอกาสพัฒนาระบบบริการที่ดีขึ้น

3. ด้านบริหาร จัดให้มีมีข้อมูลครบถ้วนเพื่อใช้ในการวิเคราะห์สถานการณ์ของโรงพยาบาลทั้งอัตรากำลัง ปริมาณงาน สถานะการเงิน ระบบคลังยา ระบบครุภัณฑ์การแพทย์และพัสดุทั่วไป

4. ด้านการศึกษาวิจัย จัดให้มีการสนับสนุนข้อมูลสารสนเทศที่ครบถ้วนและถูกต้อง รองรับการร้องขอทั้งหน่วยงานภายในและภายนอกองค์กร

5. พัฒนาศักยภาพบุคลากรให้มีประสิทธิภาพพร้อมพัฒนาและสร้างนวัตกรรมใหม่ๆให้ตอบสนองความต้องการของโรงพยาบาล

ส่วนที่ 2 สถานภาพและสภาพแวดล้อม

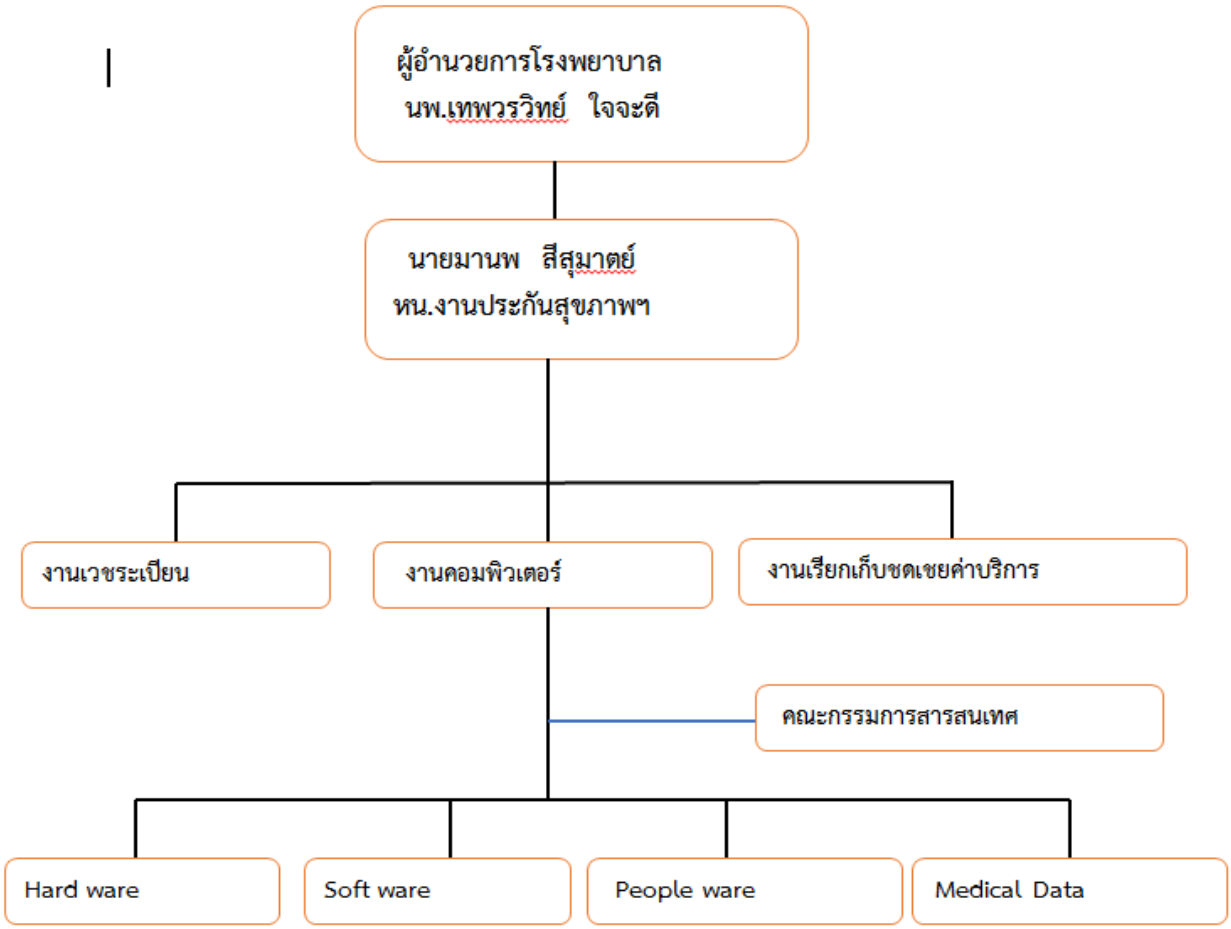
2.1 ข้อมูลทั่วไป

คณะกรรมการสารสนเทศ โรงพยาบาลแม่จริม ก่อตั้งขึ้นในปี พ.ศ.2558 เป็นหน่วยงานหนึ่งที่ทำหน้าที่พัฒนาคุณภาพการให้บริการระบบคอมพิวเตอร์ เครือข่ายสารสนเทศ และให้ข้อมูลข่าวสารขององค์กรเป็นไปด้วยความรวดเร็วและมีประสิทธิภาพ

โดยได้ดำเนินการดังนี้

- สำรวจความต้องการใช้ข้อมูลสารสนเทศแก่เจ้าหน้าที่ทุกระดับในโรงพยาบาล
- วางแผนการตอบสนองความต้องการข้อมูลสารสนเทศของหน่วยงานในโรงพยาบาล ทุกหน่วยงานมีระบบสารสนเทศของตนเอง ทั้งในรูปแบบแฟ้ม เอกสาร และฐานข้อมูลอิเลคทรอนิกส์ เพื่อการบริหารที่มีมาตรฐาน ถูกต้อง ทันเวลาเข้าถึงได้ง่าย และเชื่อมโยง กันได้ทุกหน่วยงาน ผ่านระบบ DATA center
- สนับสนุนระบบสารสนเทศโดยนำคอมพิวเตอร์ระบบเครือข่ายมาใช้ใน การบริการตรวจรักษา และบันทึกข้อมูลผู้รับบริการ เพื่อลดปริมาณการใช้กระดาษ และเพิ่มความสะดวกรวดเร็วในการเรียกใช้และประมวลผลข้อมูล
- จัดทำระบบฐานข้อมูลผู้รับบริการทั้งหมด (HosXP) เชื่อมโยงไปทุกหน่วยงานในโรงพยาบาล มี โปรแกรมประมวลผลรายงานเพื่อส่งหน่วยงานต้นสังกัดและการประมวลผลข้อมูลเชิงคุณภาพกระจายทุกฝ่ายทุกงานที่เกี่ยวข้องกับการดูแลผู้ป่วย เพื่อสะดวกในการเรียกใช้ข้อมูล
- ศูนย์ข้อมูลข่าวสารเป็นหน่วยงานกลางในการประสานงาน และตอบสนองข้อมูลข่าวสารตามที่ฝ่ายต่างๆ ร้องขอที่นอกเหนือจากการรายงานข้อมูลปกติ
- สนับสนุนระบบคอมพิวเตอร์ของโรงพยาบาล ทั้งด้าน Hardware Infrastructure และ Software

2.2 โครงสร้างองค์กรและการบริหารงาน



คณะกรรมการสารสนเทศโรงพยาบาลแม่จริมได้แบ่งความรับผิดชอบเป็น 2 ระบบคือ

1. ระบบข้อมูลสารสนเทศ(MIS) ระบบคอมพิวเตอร์และเครือข่าย (IT) มีคณะกรรมการสารสนเทศเป็นผู้รับผิดชอบ
2. ระบบเวชระเบียน (MRA) มีคณะอนุกรรมการเวชระเบียนเป็นผู้รับผิดชอบ
3. ระบบเรียกเก็บชดเชยค่าบริการทางการแพทย์ มีคณะกรรมการจัดเก็บรายได้เป็นผู้รับผิดชอบ

การบริหารอัตรากำลัง

1. งานคอมพิวเตอร์มีเจ้าหน้าที่นักวิชาการคอมพิวเตอร์ 1 คน พนักงานคอมพิวเตอร์1คน
2. งานด้านนโยบายและแผนยุทธศาสตร์ ,งานเวชระเบียนสถิติมีเจ้าพนักงานเวชสถิติ 1 คน
3. งานเรียกเก็บชดเชยค่าบริการทางการแพทย์ มีเจ้าพนักงานธุรการ 1 คน

2.4 สภาพด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลแม่จริม มีการสนับสนุนระบบสารสนเทศ ทั้งงบประมาณ ครุภัณฑ์ และสถานที่อย่างเพียงพอจากผู้บริหาร มีการเชื่อมต่อข้อมูลกับหน่วยงานภายนอกโดยใช้ Internet ความเร็วสูง ผ่าน Fiber optic และ Leased line เป็นสถานที่ศึกษาดูงานการใช้โปรแกรม HosXP มีคณะกรรมการสารสนเทศ ที่ประกอบไปด้วยสหวิชาชีพที่หลากหลายเข้ามามีส่วนร่วมตัดสินใจกำหนดโยบายสารสนเทศ โดยมีแพทย์ พยาบาล เจ้าพนักงานเวชสถิติ และนักวิชาการคอมพิวเตอร์ ที่มีความรู้ความสามารถมาเป็นผู้ดำเนินการเพื่อขับเคลื่อนแผนสารสนเทศให้บรรลุตามเป้าประสงค์ขององค์กร

2.5 สภาพแวดล้อมภายในองค์กร

จุดแข็ง (Strengths)

- ผู้บริหารระดับสูงของโรงพยาบาลเห็นความสำคัญและความจำเป็นของการนำเทคโนโลยีสารสนเทศมาใช้ในดำเนินงานตามพันธกิจและการพัฒนาองค์กร
- มีผู้บริหารระดับสูงสุดของโรงพยาบาลทำหน้าที่กำกับดูแล และร่วมพัฒนาระบบงานที่เกี่ยวข้องทางด้านเทคโนโลยีสารสนเทศ
- ผู้บริหารให้โอกาสในการทำงานอย่างอิสระ สนับสนุนการการใช้เทคโนโลยีที่ทันสมัยและเปิดกว้างสำหรับแนวคิดที่สร้างสรรค์อย่างเต็มที่
- โรงพยาบาลมีหน่วยงานที่ทำหน้าที่ดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศโดยเฉพาะ
- บุคลากรด้านเทคโนโลยีสารสนเทศมีความพร้อมและตั้งใจในการทำงานตามภารกิจอย่างเต็มที่
- เจ้าหน้าที่ทุกระดับมีความตื่นตัวและมีความพร้อมที่จะใช้เทคโนโลยีสมัยใหม่อยู่เสมอ

จุดอ่อน (Weaknesses)

- การออกแบบสารสนเทศระหว่างหน่วยงานยังขาดความต่อเนื่องเชื่อมโยง
- ขาดแผนพัฒนาบุคลากรสารสนเทศประจำหน่วยงานอย่างต่อเนื่องและเป็นระบบ
- ขาดความคล่องตัวในการจัดหาครุภัณฑ์ด้านเทคโนโลยีสารสนเทศที่ทันสมัยเนื่องจากค่าใช้จ่ายในการจัดซื้อค่อนข้างสูงและอุปกรณ์ในตลาดมีการพัฒนาที่รวดเร็วทำให้อุปกรณ์ที่มีอยู่ล้าหลังได้ง่าย
- การใช้เทคโนโลยีสารสนเทศที่ไม่เหมาะสมเช่นเพื่อความบันเทิงและการเข้าถึงเนื้อหาที่ไม่พึงประสงค์
- การเติบโตที่รวดเร็วของอุปกรณ์พกพาทำให้สามารถเข้าระบบได้ง่ายและทุกที่ ส่งผลให้ความปลอดภัยลดลงมีระบบโอกาสถูกโจมตีได้ทั้งภายในและภายนอก

2.6 สภาพแวดล้อม

ภายนอก

โอกาส (Opportunities)

- การเติบโตของ Mobile device, Big Data, Cloud Computing , IoT และการประยุกต์ใช้ AI เพื่อมาใช้กับ Healthcare Business จะมีมากขึ้นและราคาจะถูกลงในอีกไม่กี่ปีข้างหน้า
- ความก้าวหน้าและการตื่นตัวทางเทคโนโลยีสารสนเทศ ทำให้บุคคลากรสามารถเข้าถึงแหล่งข้อมูลและเรียนรู้ใช้งานอย่างง่ายดายและมีประสิทธิภาพมากยิ่งขึ้น
- ได้รับการสนับสนุนจากภาครัฐผ่านนโยบาย Thailand 4.0 และโครงการ Smart Hospital
- การสนับสนุนความรู้และความร่วมมือในการพัฒนาระบบสารสนเทศจากเครือข่าย Service Plan และ สำนักงานสาธารณสุขจังหวัดน่าน

ภัยคุกคาม (Threats)

- การพัฒนาบุคลากรบางส่วนไม่ทันกับการพัฒนาและการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี
- การบุกรุกโจมตีระบบเครือข่ายและระบบสารสนเทศทั้งจากภายในและภายนอก
- อาชญากรรมทางคอมพิวเตอร์
- การละเมิดสิทธิส่วนบุคคลผ่านการเผยแพร่ทางโซเชียลมีเดีย

ส่วนที่ 3 ยุทธศาสตร์การพัฒนาและแผนกลยุทธ์

3.1 ยุทธศาสตร์การพัฒนา

ประเด็นยุทธศาสตร์หลักโรงพยาบาลแม่จริมมี 5 ประเด็นหลักดังนี้

1. การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ บนพื้นฐานการใช้ทรัพยากรร่วมกันอย่างคุ้มค่า
2. การพัฒนานวัฒกรรมการให้บริการรูปแบบใหม่ โดยใช้ประโยชน์จากเทคโนโลยีสารสนเทศสมัยใหม่
3. การพัฒนาและเชื่อมโยงฐานข้อมูลสารสนเทศภายในและภายนอกองค์กร
4. การพัฒนาสมรรถนะบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร
5. การบริหารจัดการด้านเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัยได้มาตรฐาน

เพื่อให้บรรลุเป้าหมายหลักของโรงพยาบาลอย่างเป็นรูปธรรม คณะกรรมการสารสนเทศจึงได้กำหนดยุทธศาสตร์การพัฒนาเทคโนโลยีสารสนเทศไว้ 4 ยุทธศาสตร์ (Strategic issue) ได้แก่

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ
ยุทธศาสตร์ที่ 2 พัฒนาระบบข้อมูลสารสนเทศและเชื่อมโยงฐานข้อมูลจากสถานบริการในเครือข่าย
ยุทธศาสตร์ที่ 3 สร้างเสริมนวัตกรรมและประยุกต์ใช้เทคโนโลยีที่ทันสมัยเพื่อเพิ่มประสิทธิภาพระบบบริการ

ยุทธศาสตร์ที่ 4 พัฒนาบุคลากรให้มีความสามารถในการใช้เทคโนโลยีสารสนเทศ

ยุทธศาสตร์ที่ 1 **(Strategic issue)** พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ		
กลยุทธ์ **(Strategies)**	**แผนงาน/โครงการ/กิจกรรม** **(plans/projects)**	**ตัวชี้วัดและเป้าหมาย** **Measures(KPIs) and Target**
1.พัฒนาระบบโครงข่าย (Network) และอุปกรณ์ให้สามารถเชื่อมโยงกันได้ทุกหน่วยงานอย่างมีเสถียรภาพ ปลอดภัย และรวดเร็ว	- โครงการการปรับปรุงคุณภาพของโครงข่ายทั้งหมดเพื่อเตรียมตัวเข้าสู่โครงข่าย Next Generation (NGN) เพื่อรองรับระบบ IoT - โครงการติดตั้งระบบ Network ที่ทั้งโรงพยาบาล ปี 2566 - โครงการพัฒนาประสิทธิภาพการเชื่อมโยงระบบเครือข่ายอินเตอร์เน็ตที่รวดเร็ว ปลอดภัยและเสถียร - โครงการระบบรักษาความปลอดภัยด้วยกล้องวงจรปิด	- ผ่านมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศตามที่ TMI กำหนด -มีระบบโครงข่ายที่ครอบคลุมทุกจุดบริการทั้งระบบมีสายและไร้สาย สามารถเชื่อมต่อที่ระดับความเร็ว Gigabit -มีระบบเชื่อมโยงโครงข่ายระหว่างอาคารที่รวดเร็วและปลอดภัย (Fiber Optic) ระดับ 10 Gigabit - ระบบ Internet ความเร็วมากกว่า 50 MB และขัดข้องไม่เกิน 30 นาที
2.พัฒนาปรับปรุงห้องควบคุมระบบเครือข่ายและห้องแม่ข่าย (Server)ให้มั่นคงปลอดภัยได้มาตรฐานสากล	- โครงการย้ายห้องแม่ข่ายไปตึกอำนวยการ และปรับปรุงการงานของระบบเครือข่ายหลักระดับ Core Switch Network ปี 2566 - โครงการปรับปรุงระบบ wireless อาคารเก่าและบ้านพัก ปี 2566	-มีห้อง Server ที่ทันสมัยและได้มาตรฐาน TMI และผ่าน HAIT -เสถียรภาพของระบบโรงพยาบาลรับประกันการ Unplanned Down Time HosXP Server ไม่เกิน 2 ครั้งต่อปีและไม่เกิน 1.30 ชม./ครั้ง
3.พัฒนาระบบเครื่องคอมพิวเตอร์ให้เพียงพอและมีประสิทธิภาพเหมาะสมกับการใช้งาน	-โครงการจัดซื้อระบบคอมพิวเตอร์ทดแทนเครื่องเดิมที่ใช้งานหลายปี -โครงการพัฒนาระบบทะเบียนครุภัณฑ์คอมพิวเตอร์อุปกรณ์ต่อพ่วงที่ถูกต้อง ทันสมัย สืบค้นง่าย	- มีอุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่เพียงพอกับการปฏิบัติงานโดยสัดส่วนเครื่องคอมพิวเตอร์และอุปกรณ์ต่อบุคลากรที่จำเป็นต้องใช้ ICT - จัดลำดับความสำคัญของการให้บริการแก้ไขปัญหา Service

		Level Agreement (SLAs) ของHardware และ Software โดย PC แก้ไขภายใน 3 ชม. - ร้อยละอัตราการซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ที่บำรุงรักษาได้มากกว่า 80 %
4. พัฒนาโปรแกรมระบบงานทั้ง Front Office และ Back Office ตามความต้องการของหน่วยงานภายใน	-จัดซื้อลิขสิทธิ์ซอฟต์แวร์ที่เพียงพอกับความกับต้องการ -พัฒนาซอฟต์แวร์ทั้งครบตามความต้องการ โดยใช้ระบบ e-office เช่น ระบบ RM ระบบซ่อมบำรุง ระบบ HRD ระบบ Supply จองรถ จองห้องประชุม -Website ของโรงพยาบาลที่ทันสัยและรองรับการใช้งานที่ครบถ้วน -โครงการ Google Drive sharing	- ซอฟต์แวร์มีจำนวนที่ครบถ้วนตามที่ร้องขอ 80 % - จำนวนผู้เข้ามาใช้บริการ Website เพิ่มขึ้น -ทุกจุดบริการสามารถส่งข้อมูลผ่าน Google Drive Share ได้ครบทุกหน่วยงาน

ยุทธศาสตร์ที่ 2 (Strategic issue) พัฒนาระบบข้อมูลสารสนเทศและเชื่อมโยงข้อมูลจากสถานบริการในเครือข่าย		
กลยุทธ์ (Strategies)	**แผนงาน/โครงการ/กิจกรรม (plans/projects)**	**ตัวชี้วัดและเป้าหมาย Measures(KPIs) and Target**
1.พัฒนาคุณภาพของข้อมูล	-พัฒนามาตรฐานการวินิจฉัยโรคโดยอิง ICD 10 TM (International Classification of Disease version 10 Thai Modification) และการให้หัตถการ ICD 9 CM -โครงการการตรวจสอบเวชคุณภาพเวชระเบียน (Audit)	-อัตราความสมบูรณ์ของเวชระเบียนผู้ป่วยในและผู้ป่วยนอกมากกว่าร้อยร้อยละ 80 -อัตราความสมบูรณ์ของข้อมูล 43 แฟ้ม -ค่า CMI ได้ระดับตามเกณฑ์ของขนาดโรงพยาบาล
2.พัฒนามาตรฐานความปลอดภัยของข้อมูล	-ปรับปรุงมาตรฐานการรักษาความปลอดภัยและความเป็นส่วนตัวข้อมูลสุขภาพ (Security and privacy standards) มาตรฐานของกฎเกณฑ์ (Rule) นโยบาย (Policy) -เพิ่มมาตรฐานทางเทคนิคที่จำเป็นสำหรับการรักษาความปลอดภัย -พัฒนาระบบเครื่องแม่ข่ายสาหรับระบบงาน Active Directory, Domain, Certificate Authority	-ไม่มีอุบัติการณ์การรั่วไหลของข้อมูล -ไม่มีอุบัติการณ์การละเมิดข้อมูลส่วนบุคคลของผู้ป่วยและเจ้าหน้าที่ ผ่านการเผยแพร่ข้อมูล internet หรือ ผ่านโซเชียลมีเดีย
3.พัฒนาระบบสารสนเทศเชิงบูรณาการ วิเคราะห์และการเชื่อมโยง	- โครงการจัดทำระบบ i Data Center - โครงการจัดทำคลังข้อมูล เพื่อนำข้อมูลไปสนับสนุนการบริหารจัดการ - เชื่อมโยงส่งต่อข้อมูลด้านสุขภาพกับภาคีเครือข่าย ผ่านระบบ Data center	-ข้อมูลใน Data center มีความครบถ้วนมากกว่า 80% -ผู้บริหารและทีมนำคุณภาพมีข้อมูลไป นำไปตัดสินใจเชิงนโยบายได้ทุกโครงการ -ข้อมูลการส่งต่อสามารถเชื่อมโยงกันได้ทุกสถานบริการในเครือข่าย
4.การพัฒนาระบบเวชระเบียนอีเล็กทรอนิกส์	-โครงการ Medical record Paperless	-มีระบบ Paperless ใช้ทั้งผู้ป่วยในและผู้ป่วยนอก

ยุทธศาสตร์ที่ **3 (Strategic issue)** สร้างเสริมนวัตกรรมและประยุกต์ใช้เทคโนโลยีที่ทันสมัยเพื่อเพิ่มประสิทธิภาพระบบบริการ		
กลยุทธ์ **(Strategies)**	**แผนงาน/โครงการ/กิจกรรม** **(plans/projects)**	**ตัวชี้วัดและเป้าหมาย** **Measures(KPIs) and Target**
1.พัฒนาการให้บริการทางการแพทย์ในรูปแบบของอุปกรณ์อัจฉริยะ (Smart device)	-โครงการ Smart OPD และ Smart IPD -เพิ่มระบบ IoT ในอุปกรณ์การแพทย์ที่สำคัญ -โครงการพัฒนาระบบข้อมูลที่เชื่อมโยงระหว่างโรงพยาบาลกับสถานบริการอื่น	-มีอุปกรณ์ Smart OPD ให้บริการครอบคลุม OPD ที่สำคัญ -มีการเชื่อมโยงระบบข้อมูลและระบบ consult online ผ่านระบบ internet หรือ LAN
2.พัฒนาระบบการเฝ้าระวังและเตือนภัยสุขภาพ และการมีส่วนร่วมของชุมชน	-พัฒนาระบบการนัดหมายการตรวจทาง Internet -โครงพัฒนาแอปพลิเคชั่นแพลตฟอร์มบันทึกประวัติสุขภาพผู้ป่วยอิเล็กทรอนิกส์ (Electronic personal health record) เช่นผลการตรวจประจำปี ระดับความดัน ระดับน้ำตาล	-อัตราความพึงพอใจมากกว่าร้อยละ 80 -อัตราการผิดนัดไม่เกินร้อยละ 5 -มี Social Media ที่ผู้รับบริการสามารถเข้าถึงได้

	-ส่งเสริมการใช้เครือข่ายสังคมออนไลน์ (Social Media) เพื่อเป็นเวทีในการเข้าถึงและตอบข้อซักถาม	
3.การพัฒนาแพลตฟอร์มผ่าน mobile Application ที่ช่วยให้การสื่อสารระหว่างผู้ให้บริการและผู้รับบริการได้มากขึ้น	-โครงพัฒนาแอปพลิเคชั่นแพลตฟอร์มการนัดหมายการกำหนดระยะเวลารอคอย	-มีแอปพลิเคชั่นหรือแพลตฟอร์มการนัดหมาย การแจ้งระยะเวลารอคอย
ยุทธศาสตร์ที่ **4 (Strategic issue)** พัฒนาบุคลากรให้มีความสามารถในการใช้เทคโนโลยีสารสนเทศ		
กลยุทธ์ **(Strategies)**	**แผนงาน/โครงการ/กิจกรรม** **(plans/projects)**	**ตัวชี้วัด** **Measures(KPIs)**
1.การพัฒนาบุคลากรให้มีความรู้และทักษะในการให้บริการและบริหารจัดการด้านเทคโนโลยีสารสนเทศภายในหน่วยงาน	- สนับสนุนให้เจ้าหน้าที่เข้ารับการอบรมทักษะด้าน ICT เพื่อให้สามารถดูแล บำรุงรักษา ในการพัฒนาเครือข่ายและคอมพิวเตอร์ และพัฒนาโปรแกรมระบบงานอย่างสร้างสรรค์ทั้งระดับหน่วยงานและระดับโรงพยาบาล -หน่วยงานสามารถนำระบบเทคโนโลยีสมัยใหม่มาช่วยลดภาระงานในปัจจุบันได้มากขึ้น	- ไม่น้อยกว่าร้อยละ 80ของผู้อบรม มีความรู้ความเข้าใจอยู่ในระดับมาก-มากที่สุด - ผู้ผ่านการอบรมสามารถนำความรู้ที่ได้ไปประยุกต์ใช้กับการทำงานในระดับดีขึ้นไป
2.เพิ่มอัตรากำลังและสรรหาบุคลากรที่มีสมรรถนะด้านเทคโนโลยีสารสนเทศ	-มีจำนวนบุคลากรที่มีความรู้ระดับผู้เชี่ยวชาญเพิ่มขึ้น	-จำนวนเจ้าหน้าที่คอมพิวเตอร์มีจำนวนที่เพียงพอต่อปริมาณคอมพิวเตอร์และอุปกรณ์ต่อพ่วง -อัตราความพึงพอใจของผู้รับบริการมากกว่าร้อยละ 80

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. ความหมายและความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ ที่ไม่แน่นอน ซึ่งมีโอกาสที่จะเกิดขึ้นในอนาคต และมีผลกระทบทั้งทางบวกและทางลบ หากเป็นทางลบ จะก่อให้เกิดความผิดพลาดความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ทำให้ การดเนินงานขององค์กรไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้และจะส่งผลกระทบหรือสร้าง ความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ตามขั้นตอนการดำเนินงานที่กำหนดไว้ ทั้งปัจจัยภายในองค์กรเช่น โครงสร้างพื้นฐาน (Infrastructure) พนักงาน (Personnel) กระบวนการ(Process) เทคโนโลยี(Technology) และภายนอกองค์กร เช่น ภัยธรรมชาติ(Natural Environment) ภาวะเศรษฐกิจ(Economic) ภาวะการเมือง(Political) เทคโนโลยี(Technology) ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดล าดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และ ผลกระทบ (Impact) เมื่อท าการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับคือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหาร จัดการ ให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์รวมทั้ง การกำหนดวิธีการในการบริหารและการควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือการยอมรับ การลด/ควบคุม การยกเลิก และการ โอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อ ลดความเสี่ยง โดยทำตามแนวทางการตอบสนองต่อความเสี่ยงที่วางไว้ ประกอบด้วยกิจกรรมการควบคุมเกิดขึ้นในทุกระดับ ทุกหน้าที่งานและทั่วทั้งองค์กร และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ค้นพบ การควบคุมแบบส่งเสริม และการควบคุมแบบแก้ไข

2.ความเสี่ยงหลักด้านระบบเทคโนโลยีสารสนเทศ การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการการทำงานที่ ช่วยให้IT Managers สามารถองค์กรดำเนินธุรกิจให้บรรลุผลสำเร็จของพันธกิจ และปกป้องระบบเทคโนโลยี สารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

2.1 ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ (Access Risk) โดย บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูล และระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานมิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการ กำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและ ควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

2.2 ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบ คอมพิวเตอร์ Integrity Risk ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงาน มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มือ านาจหน้าที่เกี่ยวข้องที่ รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูก แก้ไขเปลี่ยนแปลงโดยมิชอบได้หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่ รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่ สอดคล้องกับความต้องการของผู้ใช้งานได้

2.3 ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ Availability Risk ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิด จากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวม ไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากหน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและ รัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

2.4 ความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยี สารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี Infrastructure Risk : รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจากการ แบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการ

ดำเนินงาน และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

3.แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถแบ่งออกเป็น 4 ประเภท ดังนี้

3.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบควบคุมการเข้า-ออก ห้องคอมพิวเตอร์ แม่ข่าย (Server Room)

การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม มีประเด็นหลัก ดังนี้

1.ตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารหลัก การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มี ความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่นเครื่องปรับอากาศ ตู้Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย ถังดับเพลิง เป็นต้น

2. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) ของห้องคอมพิวเตอร์แม่ข่าย (Server Room) ของสำนักงาน จำเป็นต้องมีการ ควบคุม เข้าได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ในกรณีที่มีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำอำนาจมีความจำเป็นต้องเข้าห้องคอมพิวเตอร์แม่ข่ายในบางครั้ง จำเป็นต้องมีการควบคุม อย่างรัดกุมและรอบคอบ เช่น การแจ้งให้งานเทคโนโลยีสารสนเทศทราบก่อนทุกครั้งและต้อง เซ็นชื่อในสมุดบันทึกเข้าออกห้องสื่อสารทุกครั้ง เป็นต้น

3.การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม จัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลากรณีฉุกเฉินเพื่อใช้ในการดับเพลิงเบื้องต้น

4 การป้องกันความเสี่ยงจากระบบป้องกันไฟฟ้าลัดวงจร ทำได้โดยมีระบบป้องกันไฟฟ้ากระชากไม่ให้คอมพิวเตอร์แม่ข่ายให้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า อุปกรณ์ ป้องกันไฟ จัดให้ระบบไฟฟ้าสำรองสำหรับคอมพิวเตอร์ทั้งแม่ข่ายและลูกข่าย เพื่อให้การ ดำเนินงานมีความต่อเนื่องกรณีท้องถิ่นดับหรือเกิดขัดข้องไม่สามารถใช้งานได้

5 ความเสี่ยงในเรื่องของงบประมาณที่จะดำเนินการอย่างได้ประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

6 ความเสี่ยงในเรื่องของประเด็นนโยบายผู้บริหาร ซึ่งแนวนโยบายและวิสัยทัศน์ของแต่ละยุคสมัยเปลี่ยนแปลงไป อันส่งผลมายังแนวทางในการดำเนินงาน

3.2 ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการ ดำเนินงานด้านเทคโนโลยีสารสนเทศรวมถึงการวางแผนการตรวจสอบการท างานการมอบหมายหน้าที่และ สิทธิของบุคลากร / คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากร มีความรู้ความเข้าใจในการใช้งาน

การบริหารความเสี่ยงด้านบุคคลกร มีประเด็นหลัก ดังนี้

1. กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการด้านบุคลากร การแต่งตั้งเจ้าหน้าที่ที่มีความเหมาะสม การกำหนดโครงสร้าง การแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบายและขั้นตอนการปฏิบัติงานและกำกับดูแลควบคุมการปฏิบัติงานเป็นหลัก

2. การว่าจ้าง / จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการด้านระบบ เทคโนโลยีสารสนเทศ เพราะเป็นผู้มีความรู้ ความชำนาญเฉพาะทาง มีเครื่องมือและ เทคโนโลยีที่ใช้พร้อมและทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศเฉพาะด้านมากกว่า ภาคราชการ โดยการว่าจ้างบุคลากรภายนอกนี้ก็จะมีความเสี่ยงในเรื่องของ ความรู้ความ เข้าใจในระบบราชการ และผลสัมฤทธิ์ที่เกิดจากการทำงาน อีกทั้งในแง่ของความคุ้มค่าของ การใช้จ่ายงบประมาณ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงของการว่าจ้าง บุคลากรภายนอกนี้ ทำได้โดย หน่วยงานที่เป็นเจ้าของเรื่อง หรือเป็นผู้รับผิดชอบในประเด็น ต่างๆ ต้องเป็นผู้เข้ามากำกับดูแลตั้งแต่เริ่มกระบวนการ และต่อเนื่อง โดยหลักการบริหาร จัดการที่ดี อีกทั้งรักษาผลประโยชน์ของทางราชการให้มากที่สุด

3. บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจเรื่องของระบบเทคโนโลยีสารสนเทศ โดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรม และนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะ ประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหาร ความเสี่ยงในประเด็นนี้โดยการส่งเจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศ รวมถึงการรับบุคลากรที่มีความรู้ความเข้าใจด้านระบบเทคโนโลยีสารสนเทศมาปฏิบัติงาน มากยิ่งขึ้น

4. แผนการบริหารความเสี่ยงด้านบุคลากร คือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบ ใน 3 ระดับ คือ ระดับผู้บริหาร(CIO) ระดับผู้ดูแลระบบ (Administrator) และใช้งานทั่วไป (User) ทำให้บุคลากรของหน่วยงานสามารถใช้งานวางแผนงานระบบสารสนเทศ ดูแล ปรับปรุง และพัฒนาระบบได้ เป็นการสนับสนุนบุคลากรทางคอมพิวเตอร์ รวมทั้งผู้ใช้งานให้มี ความรู้ด้านการรักษาความปลอดภัยระบบ ได้อย่างมีประสิทธิภาพ

3.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความ ผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากทำงานผิดพลาดของ อุปกรณ์ ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ ไวรัสคอมพิวเตอร์เป็นต้น

การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ มีประเด็นหลัก ดังนี้

1.ความเสี่ยงในเรื่องของจัดหาอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมกับแผนงาน /โครงการและองค์กร ซึ่งควรให้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆให้ได้ตามมาตรฐานของ อุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมตามลักษณะ ของโครงการ และงบประมาณ

2. ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) โดยมีข้อควร ปฏิบัติได้แก่

- มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแล อย่างถูกต้องและต่อเนื่อง

– ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว

- การใช้อุปกรณ์ต่อพ่วง เช่น Flash Drive ควรตรวจสอบไวรัสก่อนทุกครั้ง

– ควรปัดฝุ่นหรือทำความสะอาดเครื่องคอมพิวเตอร์อยู่เสมอ เพราะเมื่อมีฝุ่นเข้าสู่ เครื่องคอมพิวเตอร์มากๆ จะทำให้เครื่องคอมพิวเตอร์ร้อนจัดได้ง่าย เป็นสาเหตุของ อาการเครื่องค้างหรือรวนได้ - ระบบปฏิบัติการ Windows ควรทำการ Update เป็นประจำ

- การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ

- การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงานเกี่ยวกับ การใช้เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ ระบบสารสนเทศ เช่น การกำหนดรหัสผู้ใช้ และการใช้รหัสผ่าน

– การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ

- การสำรองข้อมูล (Backup) ข้อมูลระบบสารสนเทศ

- การบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ได้แก่ ระบบปฏิบัติการ คอมพิวเตอร์ ระบบเครือข่าย และการใช้งานและประสิทธิผลของเครื่องคอมพิวเตอร์ อุปกรณ์เทคโนโลยีสารสนเทศ

- กำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของ คอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

- ทำการทดสอบ Software เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้ งานอย่างสม่ำเสมอ

- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนค่า Parameter ต่างๆ ของ ระบบคอมพิวเตอร์แม่ข่ายอย่างชัดเจน

3.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงาน โปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้นสำหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์ อื่นๆ ที่ใช้ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่างเช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่ง และการถูกไม่หวังดีทำลายระบบ (Hacker) เป็นต้น

การบริหารจัดการความเสี่ยงด้านโปรแกรมคอมพิวเตอร์มีประเด็นหลัก ดังนี้ มีการพัฒนามาตรฐานและการบริการโปรแกรมคอมพิวเตอร์พัฒนาและปรับปรุงมาตรฐาน Hardware Software, Peopleware Data และNetwork ให้เป็นฐานข้อมูลกลางของงาน เทคโนโลยีสารสนเทศ และเป็นไปในทิศทางเดียวกัน พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐานและแบ่งสรรการให้ ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้

3.5 ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆ ที่เกิดขึ้นกับระบบ เครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุ มาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้ายกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้ ความเสียหายที่เกิดขึ้นจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่ายและ การจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่าย ได้มีระบบการติดตามและเฝ้าดู แลการใช้เครือข่ายภายในและการเข้าออก Internet

ทุกวัน รวมทั้งการสร้าง Firewall เพื่อ ป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูลระบบ Web Server เป็นต้น

เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายในให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณข้อมูล และการเคลื่อนไหวของฐานข้อมูล มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) มีวัตถุประสงค์ เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูล หรือการทำงานของระบบเครือข่ายที่จะมีผลถึงระบบเครือข่ายที่จะมี ผลถึงระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่าน ระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสี่ยง (availability risk) แก้ข้อมูลหรือการท างานของระบบคอมพิวเตอร์ กำหนดมาตรการรักษาความปลอดภัยข้อมูล เช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อม กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึง ผ่านระบบงาน รวมถึงการเข้าถึงข้อมูลผ่านเครือข่ายในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege)เช่น สิทธิในการใช้ โปรแกรมระบบงานคอมพิวเตอร์ (Application System) ให้แก่ ผู้ใช้งานให้เหมาะสมกับ หน้าที่และความรับผิดชอบ กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าว กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีความลับ ในการที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นให้มีสิทธิในการใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องมีการอนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึงกำหนดระยะเวลาในการใช้งาน ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากลโดยทั่วไปไม่ต่ำกว่า 6 ตัวอักษร
- ควรใช้อักขระพิเศษประกอบ เช่น @ ; < > เป็นต้น
- สำหรับผู้ใช้งานทั่วไปจะมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วนผู้ดูแลระบบ ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้งจะไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคล อื่น ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายในส่วน เครือข่ายภายนอก

ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall ระหว่างเครือข่ายในกับเครือข่ายนอกโดยการ ติดตั้งผ่านอุปกรณ์คอมพิวเตอร์ ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วย ซอฟต์แวร์และฮาร์ดแวร์ให้แก่ และมีซอฟต์แวร์ที่ดูแลระบบจะติดตั้งและกำหนดรูปแบบการ อนุญาตให้เข้าใช้เครือข่ายอินเตอร์เน็ต จัดทำแผนผังระบบเครือข่าย / แผนผังการเชื่อมโยงระบบเครือข่าย (Network Diagram) ซึ่ง มีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งในและภายนอกและอุปกรณ์ให้เป็นปัจจุบันอยู่ เสมอ ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส เป็นต้น กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของ อุปกรณ์เครือข่าย กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่อง คอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกัน ไวรัสเป็นต้น การปกป้องระบบ

เครือข่าย สิ่งที่สำคัญอย่างยิ่งคือ ผู้ใช้งานในระบบจะต้องคอย ดูแล และป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตาม และหากหาวิธีการป้องกัน และแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบ เครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นต้องมีระบบป้องกันที่ดีโดยมีวิธีการดังนี้

- ติดตั้งโปรแกรมกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
- สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ
- อัพเดทข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดท
- เปิดใช้งาน Auto Protect - ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง การป้องกันจากการเปิดไฟล์จากบันทึกข้อมูลก่อนใช้งานทุกครั้ง - แผ่น CD เทปต่างๆ
- สแกนหาไวรัสจากอื่นบันทึกก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif , .exe เป็นต้น
- ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา การป้องกันจากการเปิด E-Mail
- อย่าเปิดไฟล์E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา
- อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ
- ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทั้งทันที
- อัพเดทโปรแกรม E-Mail สม่ำเสมอ การป้องกันจาการดาวน์โหลดจาก Internet
- ไม่เปิดไฟล์ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น MSN
- ไม่ควรเข้า Website ที่มากับ E-Mail
- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลด้านความปลอดภัยเสมอ
- หลีกเลี่ยงการแชร์ไฟล์ไม่จำเป็น
- หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer

3.6 ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบ สารสนเทศอันอาจจะก่อให้เกิดความเสี่ยหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลสำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล การบริหารจัดการความเสี่ยงด้านข้อมูล มีประเด็นหลัก ดังนี้ ฐานข้อมูล มีความเสี่ยงกับการเข้าถึงข้อมูล (Access Risk) และระบบคอมพิวเตอร์ในส่วน ที่เกี่ยวข้องหรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและ ระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งทางหน่วยงานไม่มีวิธีการจัดการ และควบคุมความเสี่ยง (Access Risk) ที่รอบคอบและรัดกุมอาจทำให้บุคคลที่ไม่มีอำนาจ หน้าที่เกี่ยวข้องได้รับข้อมูลและนำข้อมูลไปใช้ก่อให้เกิดความเสียหายได้ อีกทั้งข้อมูลและการ ทำงานของระบบคอมพิวเตอร์ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ฐานข้อมูล มีความเสี่ยงเกี่ยวกับความเสี่ยงไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และ การทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มี อำนาจหน้าทีเกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบ คอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access Risk) ซึ่งส่งผลให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์อาจถูกแก้ไข

เปลี่ยนแปลงได้ หรือสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบ คอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความ เสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้สำรองข้อมูลและระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้หากไม่มีการควบคุมเกี่ยวกับการเข้าถึง ข้อมูลและระบบคอมพิวเตอร์ที่รัดกุมเพียงพอแล้ว (Access Risk) ก็อาจส่งผลให้บุคคลที่ไม่มี อำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์ เสียหายได้ ฐานข้อมูล มีความเสี่ยงกับการที่หน่วยงานไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยี สารสนเทศที่สะท้อนระบบคบคุมภายในที่ดี (Infrastructure Risk) รวมทั้งไม่ได้จัดให้มีระบบ คอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการทำงานของหน่วยงาน รวมถึงไม่มีการจัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่ง ทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอน การปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่าง เพียงพอ เพื่อให้มีความรู้ความรู้และเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุม การ ปฏิบัติงาน ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back up) ที่สำคัญของศูนย์เทคโนโลยีสารสนเทศ นั้นเพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูล (Back up) การกู้คืนข้อมูล (Recovery) ตลอดจนสถานที่จัดเก็บข้อมูลที่เหมาะสมและปลอดภัย ดังนั้นการสำรองข้อมูล และการเตรียมข้อมูลให้พร้อมกรณีฉุกเฉิน จึงมีวัตถุประสงค์เพื่อให้ข้อมูลและระบบ คอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่องมีประสิทธิภาพและในเวลาที่ต้องการ (Availability Risk) โดยที่เนื้อหาครอบคลุมเกี่ยวข้องกับแนวทางการสารองข้อมูลและระบบ คอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับ การจัดทำและการทดสอบแผนฉุกเฉิน

– การกำหนดการสำรองข้อมูล (Back up)

- การทดสอบ กำหนดทดสอบข้อมูลสารองอย่างน้อยเดือนละ 1 ครั้ง เพื่อตรวจสอบได้ ว่าข้อมูลรวมทั้งโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้ การเก็บรักษาที่เจ้าหน้าที่จัดเก็บข้อมูลโดยตรง และมีการจัดเก็บข้อมูลสำรองไว้ใน สถานที่ที่ปลอดภัย และติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง

- การกู้คืนข้อมูลสู่ระบบ มีกำหนดบุคลากรผู้ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้ โดย Login ผ่าน Username & Password ที่กำหนดไว้

3.7 กระบวนการในการบริหารความเสี่ยงของระบบสารสนเทศ

ขั้นที่1 การระบุความเสี่ยงและผลกระทบที่มีผลกระทบต่อระบบข้อมูลสารสนเทศ

ขั้นที่2 ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบซึ่งแต่ละ ความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยง ความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยง

ขั้นที่3 มีการวางแผนโดยกำหนดมาตรการกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่ อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้โดยให้มีการแต่งตั้ง เจ้าหน้าที่ผู้รับผิดชอบของ

แต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของ ระบบและป้องกัน / แก้ไข / ควบคุมความเสี่ยงไม่ให้มีผลกระทบที่วางไว้

ขั้นที่4 การติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยงในขั้นตอนนี้ เจ้าหน้าที่รับผิดชอบ จะต้องมีการรวบรวมและรายงานข้อมูลของความเสี่ยงได้ ทั้งระยะยาวและข้อมูลที่ เกี่ยวข้องเพื่อน าเสนอให้ผู้บังคับบัญชาทราบและจะได้มีบันทึกไว้เป็นหลักฐาน

ขั้นที่5 การติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง มีการตรวจสอบ การทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของ ระบบโดยมีหลักฐานประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนด

4. การประเมินความเสี่ยง (Risk assessment)

4.1 การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศสามารถแยกประเภทความเสี่ยงด้านเป็น 4 ประเภท ดังนี้

4.1.1 ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือ และอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Hacker เป็นต้น

4.1.2 ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการจัดความสำคัญใน การเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูล ต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

4.1.3 ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

4.1.4 ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหาร จัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

4.2 การประเมินความเสี่ยง (Risk Estimation) เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใดเกณฑ์การประมาณ เป็น การกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรง ของผลกระทบ และระดับความเสี่ยง ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ		
ระดับ	**โอกาส**	**คำอธิบาย**
5	สูงมาก	5 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**โอกาส**	**ตำอธิบาย**
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความ เสียหายอย่างมากต่อความ ปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผล ต่อความถูกต้องของข้อมูล บางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสีย ไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนภูมิความเสี่ยง (Risk Map)

ความเสี่ยงปานกลาง -ผลกระทบรุนแรงมาก -โอกาสเกิดน้อย	**ความเสี่ยงสูง** -ผลกระทบรุนแรงมาก -โอกาสเกิดมาก
ความเสี่ยงต่ำ -ผลกระทบน้อย -โอกาสเกิดน้อย	**ความเสี่ยงปานกลาง** -ผลกระทบน้อย -โอกาสเกิดมาก

วิธีการจัดการความเสี่ยง (Risk treatment) การกำหนดวิธีการจัดการความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์ การจัดการ ความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดังต่อไป

5.1 Take – การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับให้มีความเสี่ยง เนื่องจากค่าใช้จ่ายในการจัดการหรือสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ก็ควรมีมาตรการ ติดตามและดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับ/จัดการความ เสี่ยง เป็นต้น

5.2 Treat – การลด/ควบคุมความเสี่ยง (Risk Reduction/Control) การออกแบบระบบควบคุมการ แก้ไขปรับปรุงการทำงาน เพื่อป้องกันหรือจำกัดผลกระทบ และโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

5.3 Terminate – การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหยุดหรือเปลี่ยนแปลงกิจกรรมที่ เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

5.4 Transfer – การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) การกระจายทรัพย์สินหรือ กระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่น การประกันทรัพย์สิน เพื่อโอนความเสี่ยงไป

ยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงานบางส่วนแทน การทำสำนาเอกสารหลายๆ ชุด การกระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

6. การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting) เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถอ่าน ได้เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้ รายงานประกอบด้วยรายละเอียด อย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วนต่างๆได้รับรู้ ดังต่อไปนี้

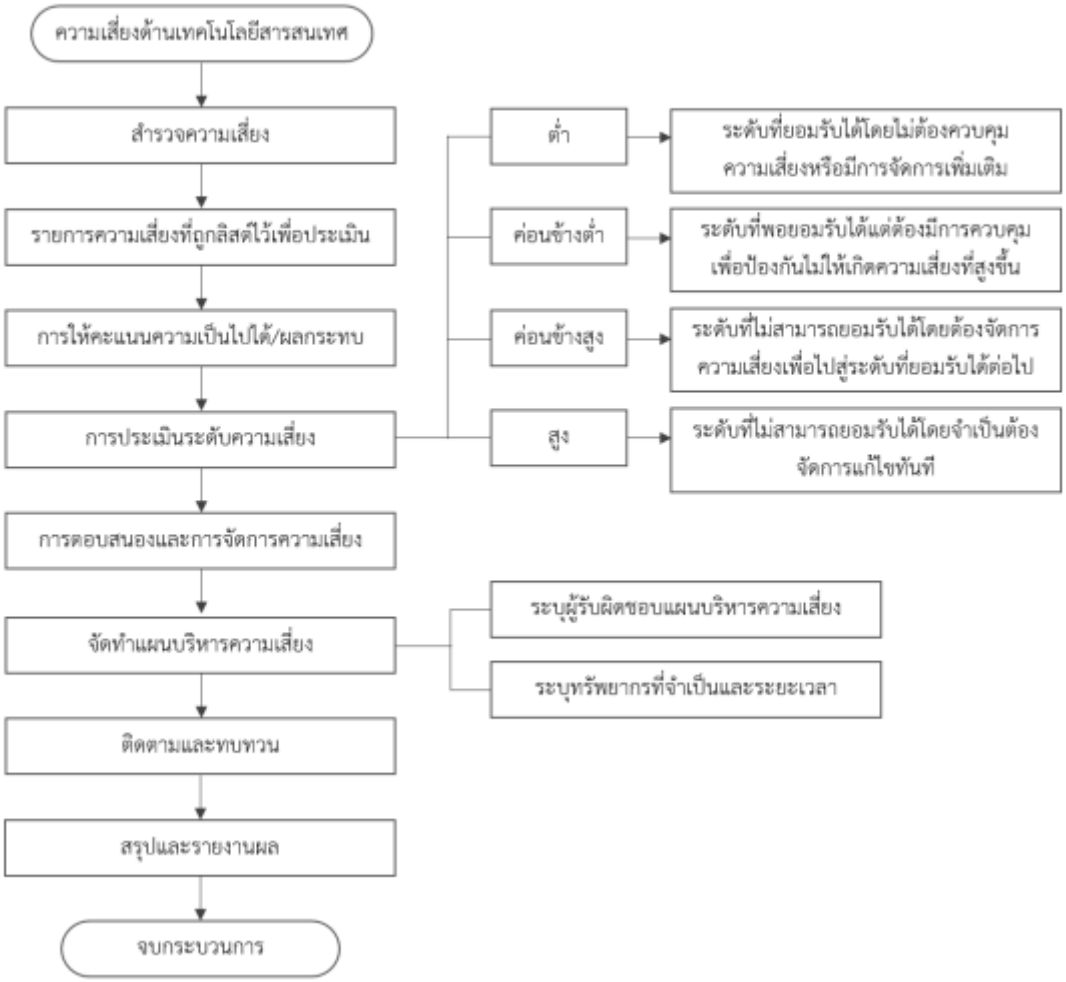
6.1 ฝ่ายบริหาร ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น รับรู้ความเสี่ยงที่องค์กรเผชิญอยู่ เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมีเหตุ หรือเหตุการณ์และเกิดผลเสียต่อภารกิจและผลประกอบการ ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ที่ได้รับผลกระทบ ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกำลังเป็นไปอย่างได้ผล ออกนโยบายบริหารความเสี่ยงและความรับผิดชอบของหน่วยงานและบุคลากรต่างๆในการ บริหารความเสี่ยง

6.2 หัวหน้างาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อหน่วยงานอื่น หรือกิจกรรมอื่นในองค์กร มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับผลกระทบ จากความเสี่ยงมากน้อยเพียงใด รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางการแก้ไข รายงานความเสี่ยงใดๆที่เกิดใหม่หรือความล้มเหลวใดๆ ในมาตรการการควบคุมหรือป้องกัน อารักขาสารสนเทศที่มีอยู่

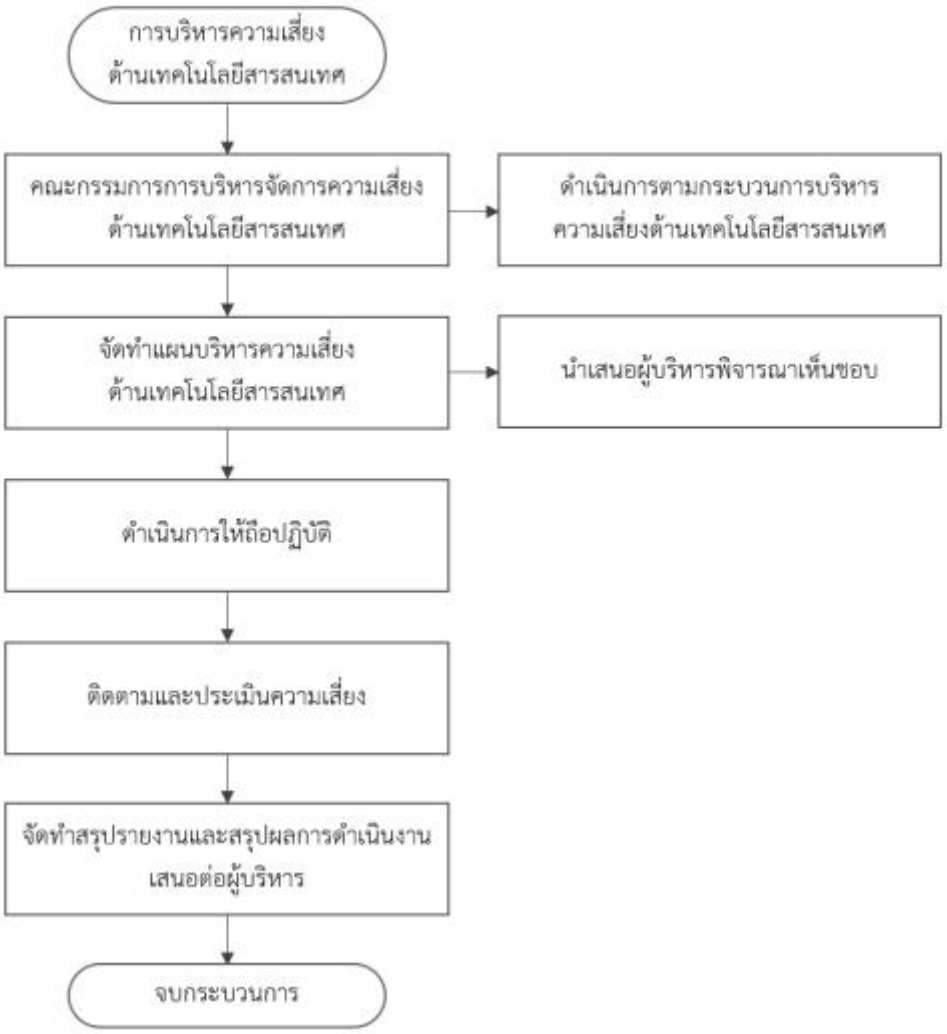
6.3 ผู้ปฏิบัติงาน ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น เข้าในบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กรที่ สำคัญอย่างหนึ่ง

7. การรายงานความเสี่ยงตกค้าง (Residual risk reporting) เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการประเมิน และการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผลหรือไม่เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือการมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบ โดยกระบวนการ IT auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบ มีการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา จึงเป็นต้องมี การบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง



กระบวนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



บทสรุป การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นการบริหารเพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีการพัฒนาและใช้งานได้อย่างต่อเนื่อง เพื่อสนับสนุนภารกิจของหน่วยงานภายในองค์กร ช่วยป้องกันหรือลดเหตุการณ์ที่จะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารให้อยู่ในระดับที่สามารถ ยอมรับ ควบคุม และตรวจสอบได้อย่างมีระบบ ซึ่งการบริหารจัดการนอกจากผู้ปฏิบัติงานโดยตรงจะต้องรับทราบแล้ว ผู้บริหารควรได้รับทราบถึงความเสี่ยงในด้านต่างๆ เพื่อนำไปจัดการและวางแผนการบริหาร ให้องค์กรดำเนินงานได้อย่างต่อเนื่องต่อไป

ประเภท ความเสี่ยง	ลักษณะ ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับ ความเสี่ยง	แนวทาง การควบคุม	วิธีจัดการ ความเสี่ยง
ความเสี่ยงด้านบุคลากร (Human Risk)	ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	1. เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อย่างปลอดภัย 2. การใช้งานโปรแกรมผิดกฎหมาย เช่น การดาวน์โหลดโปรแกรมที่ไม่มีลิขสิทธิ์	1. ระบบเสียหาย และการทำงานหยุดชะงัก 2. สูญเสีย Bandwidth ในเครือข่ายทำให้ต้องจัดสรรเพิ่มทำให้สิ้นเปลืองทรัพยากรด้านงบประมาณในการจัดสรร Bandwidth 3. อาจถูกร้องเรียนหรือฟ้องร้องจากบุคคลภายนอก	สูง 4x4 = 16	1. อบรม สร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศที่ถูกวิธี 2. กำหนด Policy ในการใช้งานอุปกรณ์ พร้อมทั้งรักษาความปลอดภัยของระบบให้มีความปลอดภัยและตรวจสอบการทำงานของระบบอย่างสม่ำเสมอ และเปิดสิทธิเข้าใช้งานเท่าที่จำเป็น 3. กำกับดูแลการปฏิบัติตามแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)
ความเสี่ยงด้านบุคลากร (Human Risk)	ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ และสิทธิการเข้าถึงข้อมูลของผู้ใช้งานไม่เป็นปัจจุบัน เนื่องจากผู้ใช้งานมีการลาออก โอน ย้าย สิ้นสุดการจ้างตลอดเวลา	1. หน่วยงาน/ผู้บริหาร/ผู้ใช้งาน อาจได้รับความเสียหายจากการถูกนำสิทธิ์การเข้าถึงระบบไปใช้ในทางผิดกฎหมาย รวมทั้งต้องรับโทษทางกฎหมาย 2. ข้อมูลที่เป็นความลับถูกเผยแพร่หรือนำไปใช้จะนำมาซึ่งการขาดความเชื่อถือของหน่วยงานฯ และอาจเกิดข้อร้องเรียนซึ่งทำให้เกิดข้อพิพาททางกฎหมาย	สูง 3x5 = 15	หน่วยงานต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้งานบุคคลแจ้งผู้ดูแลระบบให้ทราบทันที เพื่อปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	การควบคุม (Treat)

ประเภท ความเสี่ยง	ลักษณะ ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับ ความเสี่ยง	แนวทาง การควบคุม	วิธีจัดการ ความเสี่ยง
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากระบบคอมพิวเตอร์หลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	การทำงานของอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนสำคัญของระบบเกิดการขัดข้อง จากการใช้งานและอายุการใช้งาน	1. ระบบงานไม่สามารถดำเนินต่อไปได้ตามปกติ 2. ข้อมูลที่ถูกบันทึกไว้ในอุปกรณ์เกิดความเสียหาย	สูง 3x5 = 15	1. ตรวจสอบอุปกรณ์คอมพิวเตอร์ที่อยู่ในความรับผิดชอบขององค์กร/กลุ่มงาน/บุคคล อย่างสม่ำเสมอ 2. สำรองข้อมูลสำคัญไว้ที่ระบบ Cloud ขององค์กร หรือ External Hard disk ส่วนบุคคล 3. จัดจ้างผู้ดูแลระบบ (Out Source)	การถ่ายโอน (Transfer)
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware เป็นต้น	การถูกโจมตีจากภายนอกผ่านเครือข่ายอินเทอร์เน็ต	1. อาจทำให้เครื่องแม่ข่าย หรือเครื่องลูกข่ายติดไวรัส และแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย 2. ระบบ/ข้อมูลอาจจะถูกแก้ไขหรือเปลี่ยนแปลง เช่น ข้อมูลบนเว็บไซต์ของสำนักงาน 3. อาจถูกโจรกรรมข้อมูลที่เป็นความลับ	สูง 3x5 = 15	1. ติดตั้งโปรแกรมป้องกันไวรัส และทำการอัพเดทอย่างสม่ำเสมอ 2. ตรวจสอบการตั้งค่า Policy และ Log File ในระบบอย่างสม่ำเสมอ 3. อัพเดทระบบปฏิบัติการให้เป็นเวอร์ชันปัจจุบันและสม่ำเสมอ 4. จัดเจ้าหน้าที่รับผิดชอบตรวจสอบ และเฝ้าระวัง	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากความชื้นและอุณหภูมิในห้อง Server ซึ่งไม่มีระบบปรับอากาศที่ได้มาตรฐาน ทำให้ไม่สามารถควบคุมอุณหภูมิและความชื้นได้	ระบบปรับอากาศที่ไม่ได้มาตรฐานสำหรับห้อง Server	อายุของอุปกรณ์คอมพิวเตอร์สั้นลง ทำให้สิ้นเปลืองงบประมาณมากในการซ่อม/เปลี่ยนอุปกรณ์ใหม่	ค่อนข้างสูง 4x3 = 12	1. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ 2. วางแผนจัดหาระบบปรับอากาศ ชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้น เพื่อให้อุปกรณ์อยู่ในสภาวะที่เหมาะสม ลดความเสื่อม และยืดอายุการใช้งานได้	การยอมรับ (Take)

ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากการเกิดไฟฟ้าขัดข้องทำไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ อุปกรณ์คอมพิวเตอร์ถูก Shutdown อย่างเหมาะสม อาจทำให้อุปกรณ์คอมพิวเตอร์ในระบบเกิดความเสียหาย	1. ระบบไฟฟ้าขัดข้อง 2. ไม่มีระบบสำรองไฟในสำนักงาน กรณีที่เกิดไฟฟ้าดับ 3. ไม่มีระบบแจ้งเตือนไฟฟ้าขัดข้อง 4. UPS ไม่สามารถทำงานได้อย่างเต็มประสิทธิภาพเนื่องจากหมดอายุการใช้งาน	1. ระบบไม่สามารถทำงานได้ 2. ข้อมูล/อุปกรณ์เสียหาย 3. ระบบปฏิบัติการโปรแกรม ข้อมูลเสียหาย ต้องมีการ Recovery และติดตั้งใหม่	ค่อนข้างสูง 4x3 = 12	1. วางแผนการจัดหาและติดตั้ง UPS และ เครื่องกำเนิดไฟฟ้า (Electrical Generator) 2. ตรวจสอบการทำงานของเครื่องสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ	การควบคุม (Treat)
ความเสี่ยงด้านบุคลากร (Human Risk)	ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone, Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	1. ระบบเทคโนโลยีสารสนเทศไม่มีการรักษาความปลอดภัยที่ถูกต้องและเพียงพอ 2. การไม่ตระหนักต่อความเสี่ยงที่อาจเกิดขึ้นในการใช้งานระบบของผู้ใช้	อาจเกิดช่องโหว่ของระบบรักษาความปลอดภัยของหน่วยงาน และอาจมีการโจมตี ทำให้ระบบไม่สามารถทำงานได้	ค่อนข้างสูง 5x2 = 10	1. อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน 2. กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	การควบคุม (Treat)
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินการกู้คืนข้อมูลได้หากระบบเกิดเหตุขัดข้อง	ระบบสารสนเทศที่ไม่มีการสำรองข้อมูล หรือ ไม่มีการสำรองข้อมูลอย่างต่อเนื่อง	ระบบเกิดขัดข้อง/ข้อมูลเสียหาย ไม่สามารถกู้คืนข้อมูลได้	ค่อนข้างสูง 2x5=10	1. หน่วยงานต้องมีการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ 2. ผู้ใช้งานต้องมีการสำรองข้อมูล (Backup) ไว้ที่ระบบ Cloud ขององค์กร หรือ External Hard disk ส่วนบุคคลอย่างสม่ำเสมอ	การควบคุม (Treat)

ประเภท ความเสี่ยง	ลักษณะ ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับ ความเสี่ยง	แนวทาง การควบคุม	วิธีจัดการ ความเสี่ยง
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	ผู้ใช้ติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	หน่วยงานอาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ	ค่อนข้างสูง 3x4 = 12	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	ยอมรับ (Accept)
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากการเชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตขัดข้อง	ไม่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตภายนอกสำนักงานได้	ผู้ใช้ไม่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตภายนอกสำนักงานได้ ทำให้ขาดการติดต่อสื่อสาร และรับ-ส่ง ข้อมูล	ค่อนข้างสูง 2x4 = 8	1. ตรวจสอบระบบเครือข่ายสื่อสารหลักจากผู้ให้บริการเครือข่ายอินเทอร์เน็ต (ISP) เพื่อแก้ไขปัญหาที่เกิดขึ้น 2. ตรวจสอบการทำงานของอุปกรณ์เครือข่ายอย่างสม่ำเสมอ หากพบปัญหาให้ดำเนินการแก้ไขอย่างรวดเร็ว	ยอมรับ (Accept)
ความเสี่ยงด้านระบบข้อมูล (Database Risk)	ความเสี่ยงจากข้อมูลรั่วไหลเนื่องจากการเปลี่ยนผู้รับผิดชอบหรือผู้ใช้ระบบ	ข้อมูลที่สำคัญมีการรั่วไหลจากการซ่อมแซมเครื่องที่เสีย เช่น Hard Disk หรืออุปกรณ์สำรองข้อมูลประเภทต่างๆ	1. ข้อมูลที่อยู่ในชั้นความลับรั่วไหล ส่งผลต่อความน่าเชื่อถือ 2. ข้อมูลที่รั่วไหลอาจทำให้ฝ่ายใดฝ่ายหนึ่งนำไปใช้ประโยชน์ได้โดยไม่ถูกต้องตามกฎหมาย	ค่อนข้างสูง 2x4 = 8	มีการบริหารจัดการอุปกรณ์เก็บข้อมูล เช่น Hard Disk อุปกรณ์สำรองข้อมูลประเภทต่างๆ ให้แน่ใจว่าข้อมูลได้ถูกลบทิ้งอย่างถาวร หรือได้ทำลายอุปกรณ์นั้นๆทิ้งก่อนการจำหน่าย	ยอมรับ (Accept)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากการเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่มจนไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์แลอุปกรณ์ต่างๆได้ส่งผลให้ระบบไม่สามารถทำงานได้	ไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ อุบัติเหตุฉุกเฉิน	1. สูญเสียงบประมาณในการจัดหาระบบทดแทน 2. ไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทนได้	ค่อนข้างต่ำ 1x5 = 5	1. จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) 2. วางแผนจัดหาและ ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ ระบบดับเพลิง 3. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	การควบคุม (Treat)

ประเภท ความเสี่ยง	ลักษณะ ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	ระดับ ความเสี่ยง	แนวทาง การควบคุม	วิธีจัดการ ความเสี่ยง
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากสถานการณ์ความสงบเรียบร้อยในบ้านเมือง	- การชุมนุมประท้วง - การจลาจล/ก่อการร้าย - การสูญหายและถูกทำลายของอุปกรณ์ และข้อมูลที่เป็นส่วนสำคัญขององค์กร	การเกิดสถานการณ์ความรุนแรงหรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	ค่อนข้างต่ำ 1x4 = 4	1. จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) 2. สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากแมลงหรือสัตว์กัดแทะคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ สายไฟฟ้าหรือสายสัญญาณ	เสี่ยงต่อการอุปกรณ์/ระบบไม่สามารถใช้งานได้ปกติ	1. เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน 2. ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง	ค่อนข้างต่ำ 1x4 = 4	1. ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack 2. ไม่นำอาหาร/เครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง	การควบคุม (Treat)
ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)	ความเสี่ยงจากการถูกโจมตีระบบจากเครือข่ายภายใน	เสี่ยงต่อการถูกโจมตีจากโปรแกรมต่างๆโดยเฉพาะประเภทTrojan ที่มีการติดตั้งที่เครื่องลูกข่ายโดยผู้ใช้งานภายใน ทั้งที่ไม่ได้ตั้งใจและตั้งใจ	อาจส่งผลให้ระบบเครือข่ายไม่สามารถใช้ได้อย่างปกติ	ค่อนข้างต่ำ 1x5 = 5	1. กำหนดแนวปฏิบัติการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ 2. การควบคุมด้วยระบบ Desktop Management	การควบคุม (Treat)
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	ความเสี่ยงจากการถูกโจรกรรมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์ต่อพ่วง	เสี่ยงต่อการสูญหายของอุปกรณ์ และข้อมูลที่มีความสาคัญเสี่ยงต่อการสูญหาย ของอุปกรณ์ และ ข้อมูลที่มีความสาคัญ	1. เสียงบประมาณในการจัดหาอุปกรณ์ทดแทน 2. เสียเวลาในการกู้ระบบ	ค่อนข้างต่ำ 1x5 = 5	1. ติดตั้งระบบรักษาความปลอดภัยในการควบคุมการเข้า - ออกห้อง Server 2. จัดเก็บเครื่องคอมพิวเตอร์ที่สามารถเคลื่อนย้ายได้สะดวก เช่น Notebook ไว้ในที่มิดชิดเมื่อไม่ได้ใช้งาน 3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมพื้นที่ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	การควบคุม (Treat)

แผนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ระยะเวลา ปีงบประมาณ 2565 - 2568

วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2565		2566		2567		2568		ผู้รับผิดชอบ
			1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	
ความเสี่ยงจากการที่ผู้ใช้งานขาดความตระหนักในการใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย	1. อบรม สร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศที่ถูกวิธี	1 ครั้ง/ปี		◄►		◄►		◄►		◄►	
	2. กำหนด Policy ในการใช้งานอุปกรณ์ พร้อมทั้งรักษาความปลอดภัยของระบบให้มีความปลอดภัยและตรวจสอบการทำงานของระบบอย่างสม่ำเสมอ และเปิดสิทธิเข้าใช้งานเท่าที่จำเป็น	1 ครั้ง/ปี	◄►		◄►		◄►		◄►		
	3. กำกับดูแลการปฏิบัติตามแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	1 ครั้ง/เดือน	◄	—	—	—	—	—	—	►	

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2565		2566		2567		2568		ผู้รับผิดชอบ
			1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	
ความเสี่ยงจากการถูกนำสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานที่ไม่ได้รับอนุญาตไปใช้ในทางที่ผิดกฎหมาย	หน่วยงานต้องดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยฯ ในกรณีผู้ใช้งานของหน่วยงานลาออก โอน ย้าย หรือสิ้นสุดการจ้าง ให้งานบุคคลแจ้งผู้ดูแลระบบให้ทราบทันที เพื่อปรับปรุงฐานข้อมูลผู้มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน	ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งาน	←							→	
ความเสี่ยงจากระบบคอมพิวเตอร์หลักและอุปกรณ์เสียหาย ทำให้ไม่สามารถใช้ระบบงานได้เต็มประสิทธิภาพ	1. ตรวจสอบอุปกรณ์คอมพิวเตอร์ที่อยู่ในความรับผิดชอบขององค์กร/กลุ่มงาน/บุคคล อย่างสม่ำเสมอ 2. สำรองข้อมูลสำคัญไว้ที่ระบบ Cloud ขององค์กร หรือ External Hard disk ส่วนบุคคล 3. จัดจ้างผู้ดูแลระบบ (Out Source)	ทุกสัปดาห์ ทุกสัปดาห์ ปีงบประมาณ 2568	←						←	→	

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2565		2566		2567		2568		ผู้รับผิดชอบ
			1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	
ความเสี่ยงจากการบุกรุกจากผู้ไม่ประสงค์ดี/ไวรัสคอมพิวเตอร์ เช่น Hacker Virus Malware เป็นต้น	1. ติดตั้งโปรแกรมป้องกันไวรัส และทำการอัพเดทอย่างสม่ำเสมอ	1 ครั้ง/ปี	←	→	→	→	→	→	→	→	
	2. ตรวจสอบการตั้งค่า Policy และ Log File ในระบบอย่างสม่ำเสมอ	2 ครั้ง/ปี	←	→	→	→	→	→	→	→	
	3. อัพเดทระบบปฏิบัติการให้เป็นเวอร์ชันปัจจุบันและสม่ำเสมอ	1 ครั้ง/ปี	←	→	→	→	→	→	→	→	
	4. จัดเจ้าหน้าที่รับผิดชอบตรวจสอบและเฝ้าระวัง	2 ครั้ง/ปี	←	→	→	→	→	→	→	→	
ความเสี่ยงจากความชื้นและอุณหภูมิในห้อง Server ซึ่งไม่มีระบบปรับอากาศที่ได้มาตรฐานทำให้ไม่สามารถควบคุมอุณหภูมิและความชื้นได้	1. ตรวจสอบการทำงาน/อุณหภูมิเครื่องปรับอากาศที่มีอยู่เดิมอย่างสม่ำเสมอ	ทุกสัปดาห์	←	→	→	→	→	→	→	→	
	2. วางแผนจัดหาระบบปรับอากาศชนิดที่สามารถควบคุมได้ทั้งอุณหภูมิและความชื้น เพื่อให้อุปกรณ์อยู่ในสภาวะที่เหมาะสม ลดความเสื่อมและยืดอายุการใช้งานได้	ปีงบประมาณ 2568							←	→	

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2565		2566		2567		2568		ผู้รับผิดชอบ
			1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	
ความเสี่ยงจากการเกิดไฟฟ้าขัดข้องทำไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ อุปกรณ์คอมพิวเตอร์ถูก Shutdown อย่างเหมาะสม อาจทำให้อุปกรณ์คอมพิวเตอร์ในระบบเกิดความเสียหาย	1. วางแผนการจัดหาและติดตั้ง UPS และ เครื่องกำเนิดไฟฟ้า (Electrical Generator) 2. ตรวจสอบการทำงานของเครื่องสำรองไฟฟ้า (UPS) อย่างสม่ำเสมอ	ปีงบประมาณ 2567 1 ครั้ง/ปี					◄	►		►	
ความเสี่ยงจากการนำอุปกรณ์เคลื่อนที่ (Smart phone, Tablet, PC) ส่วนตัวเข้ามาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานโดยขาดความระมัดระวังในการใช้งาน	1.อบรม เผยแพร่ประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยสารเทศให้กับบุคลากรของหน่วยงาน 2.กำกับดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด	1 ครั้ง/ปี 2 ครั้ง/ปี	◄							►	

ประเภทความเสี่ยง/ กิจกรรม	แผนปฏิบัติ	ระยะเวลา	2565		2566		2567		2568		ผู้รับผิดชอบ
			1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	1 - 6	7 - 12	
ความเสี่ยงต่อการสูญหายของข้อมูล ในขั้นเล็กน้อยหรือมากจนไม่สามารถดำเนินการกู้คืนข้อมูลได้หากระบบเกิดเหตุขัดข้อง	1. หน่วยงานต้องมีการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ 2. ผู้ใช้งานต้องมีการสำรองข้อมูล (Backup) ไว้ที่ระบบ Cloud ขององค์กร หรือ External Hard disk ส่วนบุคคลอย่างสม่ำเสมอ	ทุกเดือน ทุกวัน	◄	►	◄	►	◄	►	◄	►	
การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	1. การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น 2. สร้างความตระหนักในการใช้งานซอฟต์แวร์มีลิขสิทธิ์และถูกต้องตามกฎหมาย	1 ครั้ง/ปี ทุกเดือน	◄	►	◄	►	◄	►	◄	►	