แผน/แนวทางบริหารจัดการความเสี่ยงสารสนเทศ
สำนักงานโครงการ TO BE NUMBER ONE

สำนักงานโครงการ TO BE NUMBER ONE ได้นำเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาใช้ในการปฏิบัติงานของหน่วยงานจึงมีความจำเป็นต้องมีแผนบริหารจัดการความเสี่ยงด้านสารสนเทศ ภายใต้แผนบริหารจัดการความเสี่ยงของกรมสุขภาพจิตอีกลำดับหนึ่งเพื่อป้องกันปัญหาที่อาจเกิดขึ้น อันส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานอันจะเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการ

ความหมายของความบริหารความเสี่ยง

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและส่งผลกระทบหรือสร้างความเสียหายหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายของสำนักงานโครงการ TO BE NUMBER ONE

ปัจจัยเสี่ยง หมายถึง ต้นเหตุ หรือสาเหตุ ที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดขึ้นที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การบริหารความเสี่ยง หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ซึ่งการจัดการความเสี่ยง

การควบคุม หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่างๆเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ คือการควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงของสำนักงานโครงการ TO BE NUMBER ONEเพื่อลดความเสียหายของเทคโนโลยีสารสนเทศ

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

2. การระบุความเสี่ยง (Event Identification)

3. การประเมินความเสี่ยง (Risk Assessment)

4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Respornse)

5. กิจกรรมการบริหารความเสี่ยง (Control Activitiess)

6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)

7. การติดตามประเมินผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

วัตถุประสงค์

1. เพื่อจัดการเทคโนโลยีสารสนเทศในหน่วยงาน ในการลดโอกาสที่เกิดความเสียหายกับปัญหาเทคโนโลยีสารสนเทศ

2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับข้อมูลและระบบฐานข้อมูลสารสนเทศของหน่วยงาน

3. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยความเสี่ยงในด้านต่างๆที่น่าจะมีผลกระทบกับการดำเนินงาน แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของสำนักงานโครงการ TO BE NUMBER ONE

การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของสำนักงานโครงการ TO BE NUMBER ONE แยกประเภทความเสี่ยงเป็น 4 ประเภท ดังนี้

ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ ซึ่งอาจเกิดจากการถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker เป็นต้น

ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศของหน่วยงานได้

ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถาการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าดับ ไฟไหม้ อาคารถล่ม เป็นต้น

ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ หรือเหตุการณ์ว่ามีมากน้อยเพียงไรและผลที่ตามมาว่ามีความรุนแรงหรือเสียหายมากน้องเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งหน่วยงานได้ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง

ระดับ	โอกาสที่จะเกิด	อธิบาย
5	สูงมาก	5ครั้ง/ปี
4	สูง	4ครั้ง/ปี
3	ปานกลาง	3ครั้ง/ปี
2	น้อย	2ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี

การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่าน ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุ่นแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของการควบคุมความเสี่ยงและความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ ทั้งนี้หลังจากเกิดความเสี่ยงแล้วดำเนินการตามแผนของความ

เสี่ยงภายใต้ของกรมสุขภาพจิตอีกชั้นหนึ่ง แล้วรายงานผลตามแบบรายงานความเสี่ยงการดำเนินงานของกรมสุขภาพจิต ซึ่งจัดแผนภูมิความเสี่ยงดังนี้

การจัดการความเสี่ยง

การจัดการความเสี่ยงตามแนวทางและนโยบายของกลุ่มงานพัฒนาระบบข้อมูลและสารสนเทศ สำนักยุทธศาสตร์สุขภาพจิต กรมสุขภาพจิต และรายงานผลการดำเนินการความเสี่ยงทุกๆ 6 เดือน เพราะหน่วยงานเป็นหน่วยงานส่วนกลางอยู่ภายใต้การบริหารจัดการของกลุ่มงานพัฒนาระบบข้อมูลและสารสนเทศ กรมสุขภาพจิต
