



กรมสุขภาพจิต
DEPARTMENT OF MENTAL HEALTH

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ
สำนักงานโครงการ TO BE NUMBER ONE
กรมสุขภาพจิต

 กรมสุขภาพจิต <small>DEPARTMENT OF MENTAL HEALTH</small>	ระเบียบปฏิบัติ	หน้า: 1/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ
สำนักงานโครงการ TO BE NUMBER ONE

สำนักงานโครงการ TO BE NUMBER ONE ได้นำเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาใช้ในการปฏิบัติงานของหน่วยงานจึงมีความจำเป็นต้องมีแผนบริหารจัดการความเสี่ยงด้านสารสนเทศ ภายใต้แผนบริหารจัดการความเสี่ยงของกรมสุขภาพจิตอีกลำดับหนึ่งเพื่อป้องกันปัญหาที่อาจเกิดขึ้น อันส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานอันจะเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น ด้วยการคาดการณ์ล่วงหน้าในกรณีที่มีความเสี่ยงเกิดขึ้นจริงและนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการ

ความหมายของความบริหารความเสี่ยง

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและส่งผลกระทบต่อหรือสร้างความเสียหายหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายของสำนักงานโครงการ TO BE NUMBER ONE

ปัจจัยเสี่ยง หมายถึง ต้นเหตุ หรือสาเหตุ ที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดขึ้นที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การบริหารความเสี่ยง หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ซึ่งการจัดการความเสี่ยง

การควบคุม หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่างๆเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ คือการควบคุมเพื่อป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 2/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงของสำนักงานโครงการ TO BE NUMBER ONE เพื่อลดความเสียหายของเทคโนโลยีสารสนเทศ


1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุความเสี่ยง (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
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 ภายใต้วงรับผิดชอบของสำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 3/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ 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 การจัดการสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศของหน่วยงานได้

ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าดับ ไฟไหม้ อาคารถล่ม เป็นต้น

ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ หรือเหตุการณ์ว่ามีมากน้อยเพียงไรและผลที่ตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งหน่วยงานได้ใช้เกณฑ์ดังนี้

การประมาณความเสี่ยง (Risk estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ หรือเหตุการณ์ว่ามีมากน้อยเพียงไรและผลที่ตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

 กรมสุขภาพจิต <small>DEPARTMENT OF MENTAL HEALTH</small>	ระเบียบปฏิบัติ	หน้า: 4/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

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 ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของการควบคุมความเสี่ยงและความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ ทั้งนี้หลังจากเกิดความเสี่ยงแล้วดำเนินการตามแผนของความเสี่ยงภายใต้ของกรมสุขภาพจิตอีกชั้นหนึ่ง แล้วรายงานผลตามแบบรายงานความเสี่ยงการดำเนินงานของกรมสุขภาพจิต ซึ่งจัดแผนภูมิความเสี่ยงดังนี้

 กรมสุขภาพจิต <small>DEPARTMENT OF MENTAL HEALTH</small>	ระเบียบปฏิบัติ	หน้า: 5/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		



การจัดการความเสี่ยง

การจัดการความเสี่ยงตามแนวทางและนโยบายของสำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต ซึ่งหน่วยงานเป็นหน่วยงานส่วนกลางอยู่ภายใต้การบริหารจัดการของสำนักงานเทคโนโลยีสารสนเทศ กรมสุขภาพจิต

 กรมสุขภาพจิต <small>DEPARTMENT OF MENTAL HEALTH</small>	ระเบียบปฏิบัติ	หน้า: 6/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานโครงการ TO BE NUMBER ONE

เนื่องด้วยสำนักงานโครงการ TO BE NUMBER ONE ได้มีการนำระบบคอมพิวเตอร์และสารสนเทศมาประยุกต์ใช้ในหน่วยงาน เพื่อสนับสนุนการทำงานของเจ้าหน้าที่ภายในหน่วยงานให้เป็นที่ไปด้วยความเรียบร้อย ซึ่งส่งผลให้ต้องมีการจัดทำแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศภายในหน่วยงาน เพื่อใช้เป็นแนวทางปฏิบัติและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นภายในหน่วยงานจากการใช้ระบบสารสนเทศของเจ้าหน้าที่ในหน่วยงาน

วัตถุประสงค์

1. เพื่อเป็นแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศภายในหน่วยงาน
2. เพื่อเป็นแนวทางในการลดความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศภายในหน่วยงาน
3. เพื่อเป็นแนวทางปฏิบัติเมื่อมีความเสี่ยงเกิดขึ้นกับระบบสารสนเทศในหน่วยงาน

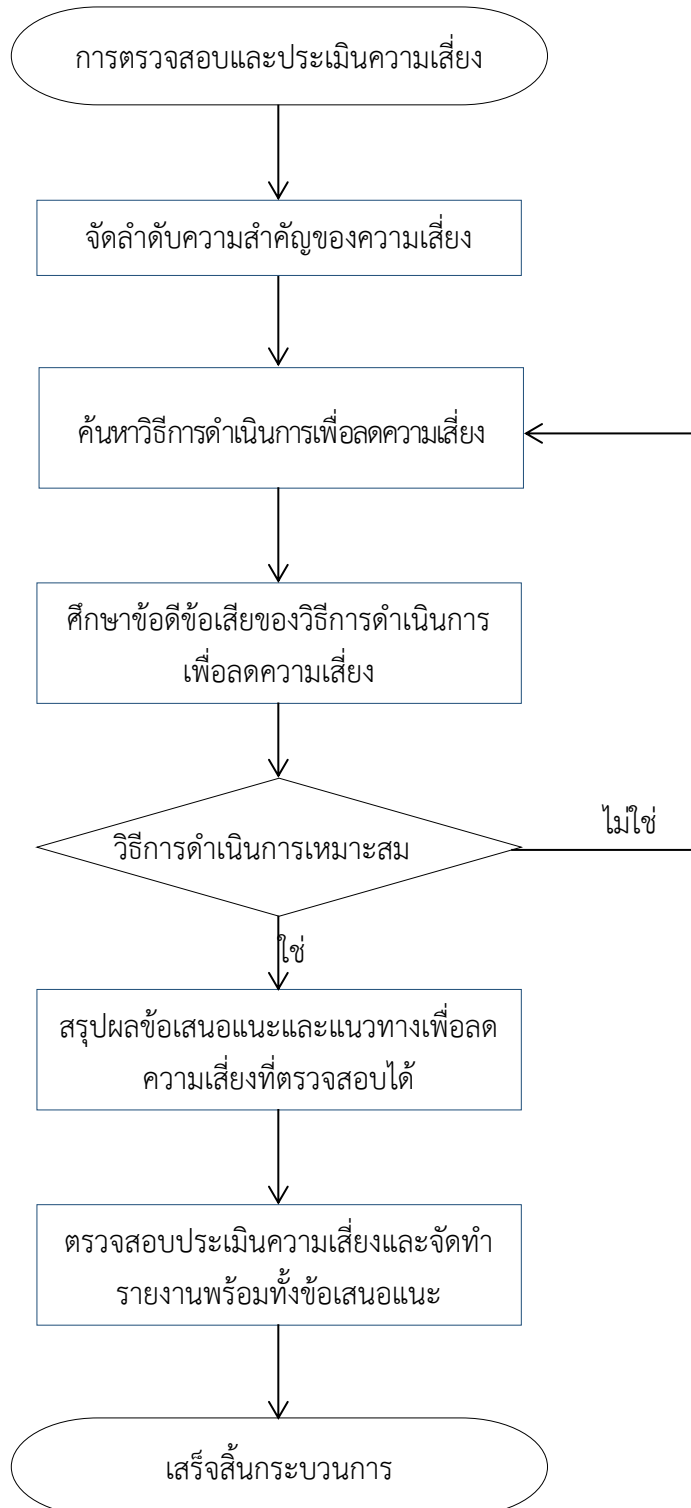
การตรวจสอบและประเมินความเสี่ยง


ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในสำนักงานโครงการ TO BE NUMBER ONEจากผู้รับผิดชอบการตรวจสอบภายในหน่วยงาน(Internal Auditor) โดยมีแนวทางในการตรวจและประเมินความเสี่ยงดังนี้

1. จัดลำดับความสำคัญของความเสี่ยง
2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
4. สรุปผลข้อเสนอแนะและแนวทางเพื่อลดความเสี่ยงที่ตรวจสอบได้
5. มีการตรวจสอบประเมินความเสี่ยงและจัดทำรายงานพร้อมข้อเสนอแนะ

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 7/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
หน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

ผังงานการตรวจสอบและประเมินความเสี่ยง



 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 8/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

การประเมินความเสี่ยง

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
1	ความเสี่ยงด้านอุปกรณ์		
	1.1 อุปกรณ์คอมพิวเตอร์เสียหาย	-อายุการใช้งานของเครื่องคอมพิวเตอร์ -การใช้งานหนัก -ขาดการดูแล บำรุงรักษา -ขาดแผนการจัดซื้อทดแทน	-เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ -อุปกรณ์ภายในคอมพิวเตอร์เสียหาย
	1.2 อุปกรณ์เครือข่ายเสียหาย	-สภาพแวดล้อมที่ใช้งาน -อุปกรณ์ชำรุด ขาดการตรวจสอบ ซ่อมบำรุง -ปัญหาที่เกิดจากภายนอก ซึ่งไม่สามารถควบคุมได้	-เครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้ -เครือข่ายอินทราเน็ตไม่สามารถใช้งานได้
	1.3 อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย	-ขาดการดูแล บำรุงรักษา -อายุการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายมีการใช้งานหนักและหลายปี -การจัดซื้อทดแทนไม่เป็นไปตามแผน	-อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย -เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถใช้งานได้
	1.4 อุปกรณ์จัดเก็บข้อมูลกลางเสียหาย	-ขาดการดูแล บำรุงรักษา -อายุการใช้งานของอุปกรณ์ -การจัดซื้อทดแทนไม่เป็นไปตามแผน	-อุปกรณ์จัดเก็บข้อมูลกลางเสียหายไม่สามารถใช้งานได้ -ข้อมูลที่ถูกรักษาไว้สูญหาย
2	ความเสียหายด้านซอฟต์แวร์		
	2.1 ระบบปฏิบัติการเสียหาย	-อายุการใช้งานของเครื่องคอมพิวเตอร์ -อายุการใช้งานของระบบปฏิบัติการ -ไวรัส มัลแวร์ -การลงซอฟต์แวร์ การติดตั้ง Driver ต่างๆ -ขาดการ Update ระบบปฏิบัติการ -ระบบปฏิบัติการที่สิ้นสุดการ support -การใช้ระบบปฏิบัติการ ที่ละเมิดลิขสิทธิ์	-เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ -ระบบปฏิบัติการไม่สามารถใช้งานได้ -ข้อมูลที่อยู่ภายในเครื่องสูญหาย



ระเบียบปฏิบัติ

หน้า: 9/18


เรื่อง : การบริหารความเสี่ยง

ฉบับที่ : 01 แก้ไขครั้งที่ 00

ประกาศใช้ : 1 กันยายน 2566

ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
	2.2 ซอฟต์แวร์ด้านการใช้ประโยชน์อื่นเสียหาย	-การลงซอฟต์แวร์ที่ไม่สมบูรณ์ -การติดไวรัส มัลแวร์ -การติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา	-ไม่สามารถใช้งานโปรแกรมได้ -ระบบปฏิบัติการไม่สามารถใช้งานได้ -ติดไวรัส มัลแวร์ -ถูก Hack เครื่องคอมพิวเตอร์ที่ใช้งาน
3	ความเสี่ยงด้านบุคลากร		
	- บุคลากรของสถาบันขาดความรู้ความเข้าใจเรื่องความปลอดภัยทางด้านสารสนเทศ	-ไม่ทำตามระเบียบปฏิบัติที่ถูกกำหนดไว้ -ขาดความรู้ความเข้าใจเกี่ยวกับความปลอดภัยทางด้านสารสนเทศในการทำงาน -บุคลากรขาดความระมัดระวังในการจัดเก็บ การเข้าถึงข้อมูล การเรียกใช้ข้อมูล การทำลายข้อมูล ที่ไม่ถูกวิธี	-ถูกโจมตี หรือถูก Hack ข้อมูล -ข้อมูลรั่วไหลไปยังภายนอก และส่งผลกระทบต่อหน่วยงาน
4	ความเสี่ยงด้านข้อมูล		
	- ความปลอดภัยของข้อมูล	-เครื่องคอมพิวเตอร์ติดไวรัส มัลแวร์ -อุปกรณ์ภายในเสียหาย -การปฏิบัติงานที่ผิดพลาด -บุคลากรละเลยความปลอดภัยทางด้านสารสนเทศ -การจัดเก็บข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล ยังไม่มีความปลอดภัย -มาตรการความปลอดภัยของข้อมูล -การจัดเก็บ การเข้าถึงข้อมูล การเรียกใช้ข้อมูล การทำลายข้อมูล ที่ไม่ถูกวิธี -ระบบรักษาความปลอดภัยทางเครือข่ายของหน่วยงาน -การถูก Hack ทางเครือข่าย -การทำลายเอกสารและข้อมูลที่ไม่ถูกวิธี	-ข้อมูลสูญหาย -ข้อมูลความสำคัญรั่วไหลหรือสูญหายเอกสาร และทางด้านดิจิทัล -การโจมตีทางด้าน Cyber Security -เอกสารถูกโจรกรรม -ข้อมูลรั่วไหลไปยังภายนอก และส่งผลกระทบต่อหน่วยงาน

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 10/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
5	การปฏิบัติงาน		
	- ขาดความรู้ในการปฏิบัติงาน	-ขาดความรู้ความเข้าใจในการปฏิบัติงาน ด้านต่างๆ เช่น ระเบียบกฎหมายข้อบังคับต่างๆ -ขาดความเข้าใจ ขั้นตอน วิธีการ ในหน้าที่ที่ต้องทำ	-การปฏิบัติงานที่ผิดพลาดเนื่องจากขาดความรู้ความเข้าใจ

แผนปฏิบัติที่ 1 อุปกรณ์คอมพิวเตอร์เสียหาย

คำอธิบายความเสี่ยง อุปกรณ์คอมพิวเตอร์เสียหาย

เจ้าของความเสี่ยง กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

สาเหตุความเสี่ยง

- อายุการใช้งานของเครื่องคอมพิวเตอร์
- การใช้งานหนัก
- ขาดการดูแล บำรุงรักษา
- ขาดแผนการจัดซื้อทดแทน

ผลกระทบของความเสี่ยง

- เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้
- อุปกรณ์ภายในคอมพิวเตอร์เสียหาย

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง


-ดำเนินการอบรมให้ความรู้ในการดูแลรักษาเครื่องคอมพิวเตอร์ การใช้งานเครื่องคอมพิวเตอร์อย่างถูกต้อง การสำรองข้อมูลภายในเครื่องคอมพิวเตอร์ แก่บุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

-กลุ่มงานแผนงาน จัดทำคู่มือการดูแลรักษาคอมพิวเตอร์ ระเบียบปฏิบัติการซ่อมบำรุงคอมพิวเตอร์ และประกาศให้บุคลากรของสำนักงานโครงการ TO BE NUMBER ONEทราบ

- การสำรองข้อมูลที่สำคัญภายในเครื่องคอมพิวเตอร์
- จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ

- กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 11/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 2 อุปกรณ์เครือข่ายเสียหาย

คำอธิบายความเสี่ยง อุปกรณ์เครือข่ายเสียหาย

เจ้าของความเสี่ยง กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

สาเหตุความเสี่ยง

- สภาพแวดล้อมที่ใช้งาน
- อุปกรณ์ชำรุด ขาดการตรวจสอบ ซ่อมบำรุง
- ปัญหาที่เกิดจากภายนอก ซึ่งไม่สามารถควบคุมได้

ผลกระทบของความเสี่ยง

- เครือข่ายอินเทอร์เน็ตในหน่วยงานไม่สามารถใช้งานได้

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง


- อบรมและทำคู่มือวิธีการดูแลอุปกรณ์เครือข่ายคอมพิวเตอร์ และประกาศให้บุคลากรในหน่วยงานทราบ
- ตรวจสอบการทำงานของอุปกรณ์เครือข่ายภายในหน่วยงานเป็นประจำ
- เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศของหน่วยงานดำเนินการตรวจสอบการทำงานของอุปกรณ์เครือข่าย

คอมพิวเตอร์ เป็นประจำ

- จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ

กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 12/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 3 อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย

คำอธิบายความเสี่ยง อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย

เจ้าของความเสี่ยง กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

สาเหตุความเสี่ยง

- ขาดการดูแล บำรุงรักษา
- อายุการใช้งานของเครื่องคอมพิวเตอร์แม่ข่าย
- แผนการจัดซื้ออุปกรณ์ทดแทนไม่ได้ตามแผนที่กำหนด

ผลกระทบของความเสี่ยง


- อุปกรณ์คอมพิวเตอร์แม่ข่ายเสียหาย
- เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถใช้งานได้

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

- จัดทำคู่มือการดูแลบำรุงรักษาและตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย
- จัดทำแผนการกู้คืนระบบ และซ้อมการกู้คืนระบบอย่างสม่ำเสมอ
- ดำเนินการตรวจสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายอย่างน้อยวันละ 1 ครั้ง
- ดำเนินการสำรองข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์แม่ข่าย
- จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ

- กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 13/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 4 อุปกรณ์จัดเก็บข้อมูลกลางเสียหาย

คำอธิบายความเสี่ยง อุปกรณ์จัดเก็บข้อมูลกลางเสียหาย

เจ้าของความเสี่ยง กลุ่มงานแผนงาน

สาเหตุความเสี่ยง

- ขาดการดูแล บำรุงรักษา
- อายุการใช้งานของอุปกรณ์
- ขาดแผนการจัดซื้อทดแทน


ผลกระทบของความเสี่ยง

- อุปกรณ์จัดเก็บข้อมูลกลางเสียหายไม่สามารถใช้งานได้
- ข้อมูลที่ถูกจัดเก็บไว้สูญหาย

แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

- ดำเนินการตรวจสอบการทำงานของอุปกรณ์จัดเก็บข้อมูลกลางอย่างสม่ำเสมอ
- ดำเนินการสำรองข้อมูลอย่างน้อย 1 ครั้งต่อเดือน
- จัดทำแผนการจัดซื้อทดแทนเมื่อครุภัณฑ์มีอายุการใช้งาน 5 ปีขึ้นไป

ผู้รับผิดชอบ กลุ่มงานแผนงาน สำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 14/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 5 ระบบปฏิบัติการคอมพิวเตอร์(Operating System)เสียหาย

คำอธิบายความเสี่ยง ระบบปฏิบัติการคอมพิวเตอร์(Operating System)เสียหายเสียหาย

เจ้าของความเสี่ยง กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

สาเหตุความเสี่ยง

- อายุการใช้งานของเครื่องคอมพิวเตอร์
- อายุการใช้งานของระบบปฏิบัติการ
- การติดไวรัส มัลแวร์
- การลงซอฟต์แวร์ การติดตั้ง Driver ต่างๆ
- ขาดการ Update ระบบปฏิบัติการ
- ระบบปฏิบัติการที่สิ้นสุดการ support
- การใช้ระบบปฏิบัติการ ที่ละเมิดลิขสิทธิ์
- การใช้งานเครื่องคอมพิวเตอร์ที่ไม่ถูกวิธี
- ไม่ติดตั้ง Antivirus และ Updateให้เป็นปัจจุบัน


ผลกระทบของความเสี่ยง

- เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้
- ระบบปฏิบัติการไม่สามารถใช้งานได้
- ข้อมูลที่อยู่ภายในเครื่องสูญหาย

แนวปฏิบัติเพื่อป้องกันความเสี่ยง

- ใช้ระบบปฏิบัติการที่ถูกลิขสิทธิ์
- Update ระบบปฏิบัติการอยู่เสมอ
- ติดตั้ง Antivirus และดำเนินการ Update Antivirus ให้ทันสมัยอยู่เสมอ
- สแกนไวรัสอย่างสม่ำเสมอ
- ระมัดระวังในการใช้งานอุปกรณ์จัดเก็บข้อมูลแบบพกพา (Flash Drive / External Hard Drive) และควรสแกนไวรัสก่อนการใช้งานทุกครั้ง
- จัดอบรมบุคลากรของสถาบันสุขภาพจิตเด็กและวัยรุ่นราชนครินทร์ ในการใช้เครื่องคอมพิวเตอร์และการบำรุงรักษาอย่างถูกวิธี
- ดำเนินการสำรองข้อมูลในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

ผู้รับผิดชอบ กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TOBE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 15/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 6 ซอฟต์แวร์การใช้ประโยชน์งานอื่นๆเสียหาย

คำอธิบายความเสี่ยง ซอฟต์แวร์การใช้ประโยชน์งานอื่นๆเสียหาย

เจ้าของความเสี่ยง กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

สาเหตุความเสี่ยง


- การลงซอฟต์แวร์ที่ไม่สมบูรณ์
 - การติดไวรัส มัลแวร์
 - การติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา
 - การติดตั้งซอฟต์แวร์ผิดลิขสิทธิ์
 - บุคลากรดำเนินการติดตั้งซอฟต์แวร์ด้วยตนเอง
- ผลกระทบของความเสี่ยง
- ไม่สามารถใช้งานโปรแกรมได้
 - ระบบปฏิบัติการไม่สามารถใช้งานได้
 - ติดไวรัส มัลแวร์
 - ถูก Hack เครื่องคอมพิวเตอร์ที่ใช้งาน

แนวปฏิบัติเพื่อป้องกันความเสี่ยง

- ใช้ซอฟต์แวร์ที่ถูกลิขสิทธิ์ หรือใช้ซอฟต์แวร์ประเภท Open Source เพื่อทดแทนการละเมิดลิขสิทธิ์
- ชี้แจงบุคลากร เรื่องห้ามดำเนินการติดตั้งซอฟต์แวร์ด้วยตนเอง

ผู้รับผิดชอบ

กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 16/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 7 บุคลากรของสถาบันฯ ขาดความรู้ความเข้าใจเรื่องความปลอดภัยทางด้านสารสนเทศ

คำอธิบายความเสี่ยง บุคลากรของหน่วยงานขาดความรู้ความเข้าใจเรื่องความปลอดภัยทางด้านสารสนเทศ

เจ้าของความเสี่ยง บุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

สาเหตุความเสี่ยง

-ไม่ทำตามระเบียบปฏิบัติที่กำหนดไว้

-ขาดความรู้ความเข้าใจเกี่ยวกับความปลอดภัยทางด้านสารสนเทศในการทำงาน

-บุคลากรขาดความระมัดระวังในการจัดเก็บ การเข้าถึงข้อมูล การเรียกใช้ข้อมูล การทำลายข้อมูล ที่ไม่ถูกวิธี

ผลกระทบของความเสี่ยง

-ถูกโจมตี หรือถูก Hack ข้อมูล

-ข้อมูลรั่วไหลไปยังภายนอกและส่งผลกระทบต่อสถาบันสุขภาพจิตเด็กและวัยรุ่นราชนครินทร์


แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

-จัดทำระเบียบปฏิบัติด้านการเข้าถึงข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล และดำเนินการสื่อสารแก่

บุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

ผู้รับผิดชอบ

กลุ่มงานแผนงาน และบุคลากรของสำนักงานโครงการ TO BE NUMBER ONE

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 17/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

แผนปฏิบัติที่ 8 ความปลอดภัยของข้อมูล

คำอธิบายความเสี่ยง ความปลอดภัยของข้อมูล

เจ้าของความเสี่ยง กลุ่มงานแผนงาน และกลุ่มงานต่างๆที่ดำเนินการจัดเก็บข้อมูล

สาเหตุความเสี่ยง

- เครื่องคอมพิวเตอร์ติดไวรัส มัลแวร์
- อุปกรณ์ภายในเสียหาย
- การปฏิบัติงานที่ผิดพลาด
- บุคลากรละเลยความปลอดภัยทางด้านสารสนเทศ
- การจัดเก็บข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล ยังไม่มีความปลอดภัย
- การทำลายเอกสารและข้อมูลที่ไม่ถูกวิธี

ผลกระทบของความเสี่ยง

- ข้อมูลสูญหาย
- ข้อมูลความสำคัญรั่วไหลหรือสูญหายเอกสาร และทางด้านดิจิทัล
- การโจมตีทางด้าน Cyber Security
- เอกสารถูกโจรกรรม
- ข้อมูลรั่วไหลไปยังภายนอกและส่งผลกระทบต่อสำนักงานโครงการ TO BE NUMBER ONE


แนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

- จัดทำระเบียบปฏิบัติด้านการเข้าถึงข้อมูลทางด้านกายภาพ และทางด้านดิจิทัล และดำเนินการสื่อสารแก่บุคลากรของสำนักงานโครงการ TO BE NUMBER ONEให้ทราบ
- สื่อสารเรื่องการทำลายเอกสารและข้อมูล

ผู้รับผิดชอบ

- กลุ่มงานแผนงาน และกลุ่มงานต่างๆ ของสำนักงานโครงการ TO BE NUMBER ONE ที่ดำเนินการจัดเก็บ

ข้อมูล

 <p>กรมสุขภาพจิต DEPARTMENT OF MENTAL HEALTH</p>	ระเบียบปฏิบัติ	หน้า: 18/18
	เรื่อง : การบริหารความเสี่ยง	ฉบับที่ : 01 แก้ไขครั้งที่ 00 ประกาศใช้ : 1 กันยายน 2566
ชื่อหน่วยงาน : สำนักงานโครงการ TO BE NUMBER ONE		

สรุปแนวทางปฏิบัติเพื่อป้องกันความเสี่ยง

การบริหารความเสี่ยงของระบบสารสนเทศ เป็นหน้าที่ความรับผิดชอบของบุคลากรทุกคน และ เป็นการป้องกันความเสี่ยงที่ทุกคนต้องช่วยกันปฏิบัติ เพื่อป้องกันความเสี่ยง ดังนี้

1. ด้านฮาร์ดแวร์ (hardware)

- 1.1 เครื่องแม่ข่าย อุปกรณ์เครือข่าย
 - ไม่อนุญาตให้บุคคลภายนอกเข้า
 - เลือกสถานที่ที่เหมาะสม ทั้งสถานที่ และ สภาพอากาศ
- 1.2 ไม่อนุญาตให้ผู้อื่นใช้เครื่องของตนเอง
- 1.3 ตั้งรหัสผ่านเพื่อป้องกันเครื่องคอมพิวเตอร์ และ ข้อมูลความลับของแต่ละฝ่าย
- 1.4 หมั่นดูแลรักษา สังเกตความผิดปกติของเครื่องตนเอง

2. ด้านซอฟต์แวร์ (software)

- ไม่ควรติดตั้งโปรแกรมที่ไม่รู้จักแหล่งที่มา

3. ด้านข้อมูล (Data)

- 3.1 ต้องมีการสำรองข้อมูลที่สำคัญ
- 3.2 ต้องมีความรักษาความปลอดภัยของข้อมูลในแต่ละฝ่าย
- 3.3 มีการจำกัดสิทธิ์ในการเข้าถึงข้อมูล

4. ด้านบุคลากร (people)

- 4.1 ผู้บริหารระบบ
 - ดูแลรักษาเครื่องคอมพิวเตอร์ ระบบเครือข่ายภายในองค์กร
 - ควบคุม ดูแล การใช้งานระบบ
 - รักษาความปลอดภัยของระบบ
- 4.2 ผู้ใช้งาน
 - ดูแลรักษาเครื่องคอมพิวเตอร์ของตนเอง
 - รักษาข้อมูลที่สำคัญของตนเอง/ฝ่าย
