แผนบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ประจำปีงบประมาณ พ.ศ. 2566

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
มีนาคม 2566

สารบัญ

สารบัญ

1 บทนำ

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปีงบประมาณ พ.ศ. 2566 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยให้ความสำคัญในการบริหารจัดการความเสี่ยง เป็นเครื่องมือสำคัญตามหลักการกำกับดูแลกิจการที่ดีช่วยในการบริหารและการตัดสินใจ การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายต่อองค์กร การเปลี่ยนแปลงกระบวนการทำงานโดยการนำเทคโนโลยีสารสนเทศและการสื่อสาร เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การจัดการฐานข้อมูล การใช้เครื่องคอมพิวเตอร์ และอุปกรณ์ การใช้เครือข่ายคอมพิวเตอร์และการสื่อสาร และการติดต่อสื่อสารผ่านระบบเครือข่าย ทั้งนี้ ภายใต้วิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศและการสื่อสารล้วนมีความเสี่ยงซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) มีบทบาทและภารกิจในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นระบบ จึงจำเป็นต้องมีการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้าง ที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร ทำการวิเคราะห์และระบุความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น การจัดลำดับความสำคัญของปัจจัยเสี่ยง การกำหนดแนวทางในการจัดการความเสี่ยง โดยคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสมและองค์กรยอมรับได้

1.2 วัตถุประสงค์การจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

2) เพื่อให้มีการปฏิบัติตามกฎระเบียบ หรือนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างมีระบบและต่อเนื่อง มีแผนงานที่สามารถแก้ไขสถานการณ์ได้ทันท่วงที กรณีเกิดสถานการณ์ฉุกเฉิน เช่น แผนการสำรองและทดสอบกู้คืนข้อมูล แผนเตรียมความพร้อมกรณีฉุกเฉิน เป็นต้น

3) เพื่อให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการมอบหมายเจ้าหน้าที่ผู้รับผิดชอบในการปฏิบัติงานให้มีประสิทธิภาพตามแผนจัดการความเสี่ยงด้านเทคโนโลยีและการสื่อสารของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ให้บรรลุเป้าหมาย เกิดผลการปฏิบัติงานและการป้องกันความเสียหายของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4) เพื่อเป็นแนวทางในการดำเนินงาน การกำกับดูแล การมอบหมาย การติดตามงาน การตรวจทานและประเมินความเสี่ยงฯ ตลอดจนมีการเผยแพร่และประชาสัมพันธ์ให้เกิดความเข้าใจระหว่างผู้ปฏิบัติและผู้บริหาร ในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ผ่านช่องทางเว็บไซต์ ระบบ Intranet และช่องทางอื่นๆ ของ สป.พม.

1.3 เป้าหมายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ มีแผนสำหรับดำเนินการเพื่อจัดการความเสี่ยงฯ ดังนี้

1.3.1 มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.3.2 มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

1.3.3 มีแผนเตรียมความพร้อมกรณีฉุกเฉิน

1.3.4 มีแผนการสำรองและทดสอบกู้คืนข้อมูล

1.4 ขอบเขตการดำเนินงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการโดยคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการจัดทำระบบสำรองข้อมูลและสารสนเทศและการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ตามข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสารสนเทศ ระบบฐานข้อมูลและการจัดเก็บข้อมูล

1.5.2 มีแนวทางในการดูแลบำรุงรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีเสถียรภาพและมีความพร้อมใช้งานอย่างต่อเนื่อง

2 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

บทที่ 2

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

2.1 สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สป.พม. มีครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) อุปกรณ์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา (Notebook) เครื่องสแกนเนอร์ เครื่องพิมพ์ชนิดต่างๆ (Printer) เครื่องสำรองไฟฟ้า (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching) อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

การให้บริการบนระบบเครือข่ายคอมพิวเตอร์ ได้แก่ โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Anti-Virus) โปรแกรมระบบปฏิบัติการจัดการเครือข่าย (Network Software) โปรแกรมระบบปฏิบัติการบนหน้าจอเว็บไซต์ (Web Application Program) โปรแกรมระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์โน้ตบุ๊ก (Operating System) โปรแกรมจัดการสำนักงาน เป็นต้น

นอกจากนี้ ยังได้ส่งข้อมูลจราจรทางคอมพิวเตอร์ (log) แบบเรียลไทม์ ไปยังศูนย์ปฏิบัติการเครือข่าย (Network Operation Center : NOC) เพื่อเฝ้าระวังไม่ให้เกิดการโจมตีเครือข่าย และอุปกรณ์ที่สำคัญ อีกทั้งยังมีการทำ DR Site หรือ Disaster Recovery Site สำรองข้อมูลในกรณีระบบหลักเกิดความเสียหาย

สำหรับระบบสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ที่ให้บริการ ประกอบด้วย ระบบสมุดพกครอบครัวอิเล็กทรอนิกส์ (MSO LogBook) ระบบฐานข้อมูลกลางผู้รับสวัสดิการ พม. (DB Center) กระดานสถานการณ์ทางสังคม (Dashboard) ระบบติดตามการใช้บริการ พม. สถิติด้านสังคม (STAT INFO) สถิติพื้นฐานของการพัฒนามนุษย์ สถิติสายด่วน 1300 นโยบายและแนวปฏิบัติด้านสารสนเทศ เป็นต้น

นอกจากนี้ยังมีระบบ Back office ที่สนับสนุนการปฏิบัติงานของบุคคลกร ประกอบด้วย ระบบทำเนียบหน่วยงาน (Directory) ระบบติดตามแผนงานโครงการ (Tracking) ระบบแบบฟอร์มออนไลน์ (e-form) ระบบการขอใช้ทรัพยากร (E-reservation) ระบบลงเวลาปฏิบัติราชการด้วยลายนิ้วมือ ระบบอินทราเน็ต (Intranet) ระบบบัญชีเงินกองทุน (funds) ระบบงานพัฒนาระบบบริหาร เป็นต้น

2.2 กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุความเสี่ยง วิเคราะห์ ประเมินและจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือองค์กร การบริหาร/จัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสมครอบคลุม 5 ขั้นตอน ดังนี้

1) การระบุความเสี่ยง

2) การวิเคราะห์ความเสี่ยง

3) การกำหนดมาตรการ

4) การติดตามรายงานประเมินผล

5) การทบทวนระบุกรอบเวลา

2.2.1 การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่คณะทำงานฯ และผู้ปฏิบัติงานที่เกี่ยวข้องร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องของโครงการหรือกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายในและภายนอกองค์กร

วิธีการระบุความเสี่ยง มีหลายวิธี เช่น

2.2.1.1 การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

2.2.1.2 การใช้ Checklist

2.2.1.3 การวิเคราะห์สถานการณ์จากการตั้งคำถาม What-if

2.2.1.4 การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ มีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปแบบของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินงานใดๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2.2.2 การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยงประกอบด้วย 4 ขั้นตอน คือ

2.2.2.1 **การกำหนดเกณฑ์การประเมินมาตรฐาน** เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) ซึ่งคณะทำงานฯ ต้องกำหนดเกณฑ์ขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณ

และเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ ได้แก่ สูงมาก (รุนแรงมากที่สุด) สูง (ค่อนข้างรุนแรง) ปานกลาง น้อย และน้อยมาก ส่วนระดับของความเสี่ยงอาจกำหนดเป็น 4 ระดับ (สูง ค่อนข้างสูง ค่อนข้างต่ำ และต่ำ)

2.2.2.2 **การประเมินโอกาสและผลกระทบของความเสี่ยง** เป็นการนำความเสี่ยงและปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้น และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงจะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น ดังตัวอย่างที่ยกมาประกอบข้างล่างนี้

เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) ดังนี้

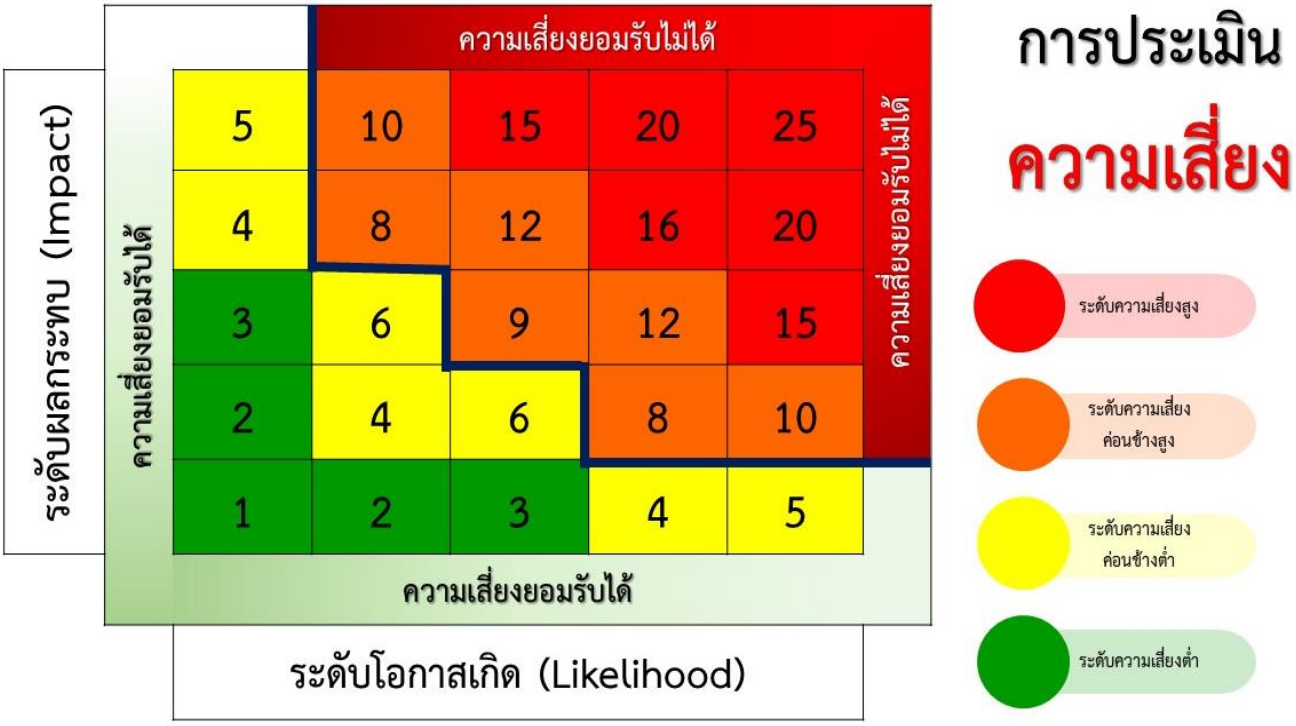
ผลกระทบที่จะเกิด	ความเสียหายที่เกิดขึ้น		ระดับคะแนน
	เชิงคุณภาพ	เชิงปริมาณ	
สูงมาก	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกลงโทษทางวินัย	มากกว่า 10 ล้านบาท	5
สูง	มีการสูญเสียทรัพย์สินอย่างมาก ผู้บริหารถูกตำหนิหรือถูกร้องเรียน	มากกว่า 2.5 แสนบาท ถึง 10 ล้านบาท	4
ปานกลาง	มีการสูญเสียทรัพย์สินมาก เจ้าหน้าที่ถูกร้องเรียนหรือถูกลงโทษทางวินัย	มากกว่า 50,000 บาท ถึง 2.5 แสนบาท	3
น้อย	มีการสูญเสียทรัพย์สินพอสมควร เจ้าหน้าที่ได้รับเสียงบ่นหรือถูกตำหนิ	มากกว่า 1 หมื่นบาท ถึง 5 หมื่นบาท	2
น้อยมาก	มีการสูญเสียทรัพย์สินเล็กน้อย แทบไม่มีผลกระทบเลย	น้อยกว่า 1 หมื่นบาท	1

เกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง ดังนี้

โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้นของความเสี่ยง		ระดับคะแนน
	เชิงคุณภาพ	เชิงปริมาณ	
สูงมาก	มีโอกาสเกิดบ่อยมากเกือบทุกวัน	มากกว่า 1 ครั้งต่อเดือน	5
สูง	มีโอกาสเกิดค่อนข้างสูงหรือบ่อยๆ ทุกเดือน	ระหว่าง 1-6 เดือนต่อครั้ง	4
ปานกลาง	มีโอกาสในการเกิดบางครั้ง(ทุกปี)	ระหว่าง 6-12 เดือนต่อครั้ง	3
น้อย	อาจมีโอกาสเกิด แต่นานๆ ครั้ง (ทุก 5 ปี)	มากกว่า 1 ปีต่อครั้ง	2
น้อยมาก	มีโอกาสเกิดน้อยมาก (แทบไม่เกิดขึ้นเลย)	มากกว่า 5 ปีต่อครั้ง	1

2.2.2.3 **การวิเคราะห์ความเสี่ยง** เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กรว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงที่จะต้องบริหารจัดการความเสี่ยงก่อน ดังนี้

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูง		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	15 - 25
ค่อนข้างสูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป	8 - 14
ค่อนข้างต่ำ		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	4 - 7
ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม	1 - 3



2.2.2.4 **การจัดลำดับความเสี่ยง** เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้แล้ว เลือกความเสี่ยงที่มีระดับสูงหรือค่อนข้างสูงมาจัดทำแผนบริหารจัดการความเสี่ยงฯ

2.2.3 การกำหนดมาตรการจัดการความเสี่ยง

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้บรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ตามแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจจะเกิดขึ้นเพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ด้าน คือ

2.2.3.1 **การควบคุมเพื่อการป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น มีการแบ่งแยกหน้าที่ความรับผิดชอบและการมอบหมายการปฏิบัติงานโดยผู้บังคับบัญชา มีคำสั่งมอบหมายงานและระบุบุคคลอย่างชัดเจน

2.2.3.2 **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์การตรวจนับและการรายงานข้อบกพร่อง เป็นต้น

2.2.3.3 **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จ

2.2.3.4 **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตตามวัตถุประสงค์

หลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงและค่อนข้างสูงมาประเมินมาตรการควบคุมเป็นอันดับแรก โดยใช้ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงหรือค่อนข้างสูงมากำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

2) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

2.2.4 การติดตามและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยง

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ในการปฏิบัติเพื่อลดโอกาสความเสี่ยงหรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงของโครงการหรือกิจกรรมควบคุมความเสี่ยงหรือมีแต่ไม่เพียงพอและนำมาวางแผนจัดการความเสี่ยง ซึ่งทางเลือกในการบริหารความเสี่ยงมีหลายวิธีสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลดการควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยงและเมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยงและการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือกเพื่อการตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสม โดยพิจารณาจากประเด็นต่างๆ ดังนี้

2.2.4.1 พิจารณาว่ายอมรับความเสี่ยงหรือกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

2.2.4.2 เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่ได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

2.2.4.3 กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารจัดการความเสี่ยงฯ

2.2.4.4 ในรอบปีถัดไป ให้พิจารณาผลการบริหารความเสี่ยงในรอบปีก่อนที่จะดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยง ซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กรให้นำมาระบุการควบคุมในแผนบริหารจัดการความเสี่ยงฯ ด้วย

การรายงานผลการวิเคราะห์ ประเมิน และบริหารจัดการความเสี่ยงว่า มีความเสี่ยงที่ยังคงเหลืออยู่หรือไม่ถ้ายังมีเหลืออยู่มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร เสนอต่อผู้บริหารเพื่อทราบและสั่งการ

2.2.5 การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการทบทวน/ติดตามภายหลังจากได้ดำเนินการตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนฯ นั้นมีประสิทธิภาพ

2.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) ได้วิเคราะห์ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางของ COSO (Committee of Sponsoring Organization) แบ่งเป็น 8 ประเภท ดังนี้

2.3.1 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2.3.2 ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกกลุ่ม/ฝ่าย อย่างละเอียดเพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

2.3.3 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายในและมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

2.3.4 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัปเดตให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่ง สป.พม. อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

2.3.5 ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสาร อันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลง

ข้อมูลทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัยสำคัญสำหรับผู้บริหารผู้มีส่วนได้ส่วนเสียโดยตรงรวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากมนุษย์ ภัยจากธรรมชาติหรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

2.3.6 ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงนโยบายของภาครัฐ ผู้บริหารหน่วยงาน เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้ต้องมีการกำหนดยุทธศาสตร์และกลยุทธ์เพื่อรองรับการเปลี่ยนแปลง

2.3.7 ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

2.3.8 ความเสี่ยงด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

2.4 การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) โดยมีหลักการตอบสนองความเสี่ยง 4 ประการ คือ

2.4.1 การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับอาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

2.4.2 การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างาน

ได้ User/Password ที่กำหนดให้แล้ว อาจจะบอก User/Password ของตน ให้ผู้ใต้บังคับบัญชาทราบ และเมื่อผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างานอาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายและหน่วยงานที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นแล้วจึงแก้ไขโดยการกำหนด User/Password ใหม่ให้กับหัวหน้างาน เป็นต้น

2.4.3 การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไปหรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีการควบคุมความสูญเสีย มี 2 วิธี คือ

2.4.3.1 การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคลหรือไวรัสคอมพิวเตอร์มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์และระบบเครือข่าย เป็นต้น

2.4.3.2 การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องวัดอุณหภูมิความร้อนหรือสัญญาณเตือนภัยเพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ให้มีความเสียหายน้อยที่สุดหรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

2.4.4 การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อหมดระยะเวลาการรับประกัน ทั้งนี้ ศทส. สป.พม. จะต้องทำสัญญาการบำรุงรักษาระบบหลังการขายให้ทันก่อนระยะเวลาในการรับประกันจะสิ้นสุด

2.5 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของ สป.พม. มีดังนี้

2.5.1 ปัจจัยภายนอก ได้แก่

2.5.1.1 ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และภัยพิบัติอื่นๆ

2.5.1.2 การขโมยอุปกรณ์เครื่องแม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

2.5.1.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) จากการเคลื่อนย้าย หรือ อื่นๆ

2.5.1.4 ระบบการสื่อสารของระบบเครือข่ายหลักเสียหาย/ขัดข้อง

2.5.1.5 ระบบกระแสไฟฟ้าขัดข้อง/ไฟดับ

2.5.1.6 ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะ เช่น หนู แมลงสาป เป็นต้น

2.5.2 ปัจจัยภายใน ได้แก่

2.5.2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.5.2.2 การถูกไวรัสคอมพิวเตอร์ ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่างๆ

2.5.2.3 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.6 การประเมินความเสียหาย

2.6.1 ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบ ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) เสียหาย และระบบฐานข้อมูลเสียหาย

2.6.2 ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วคราว ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของระบบเครือข่ายคอมพิวเตอร์ขัดข้อง กระแสไฟฟ้าขัดข้อง

2.7 การติดตามและรายงานผล

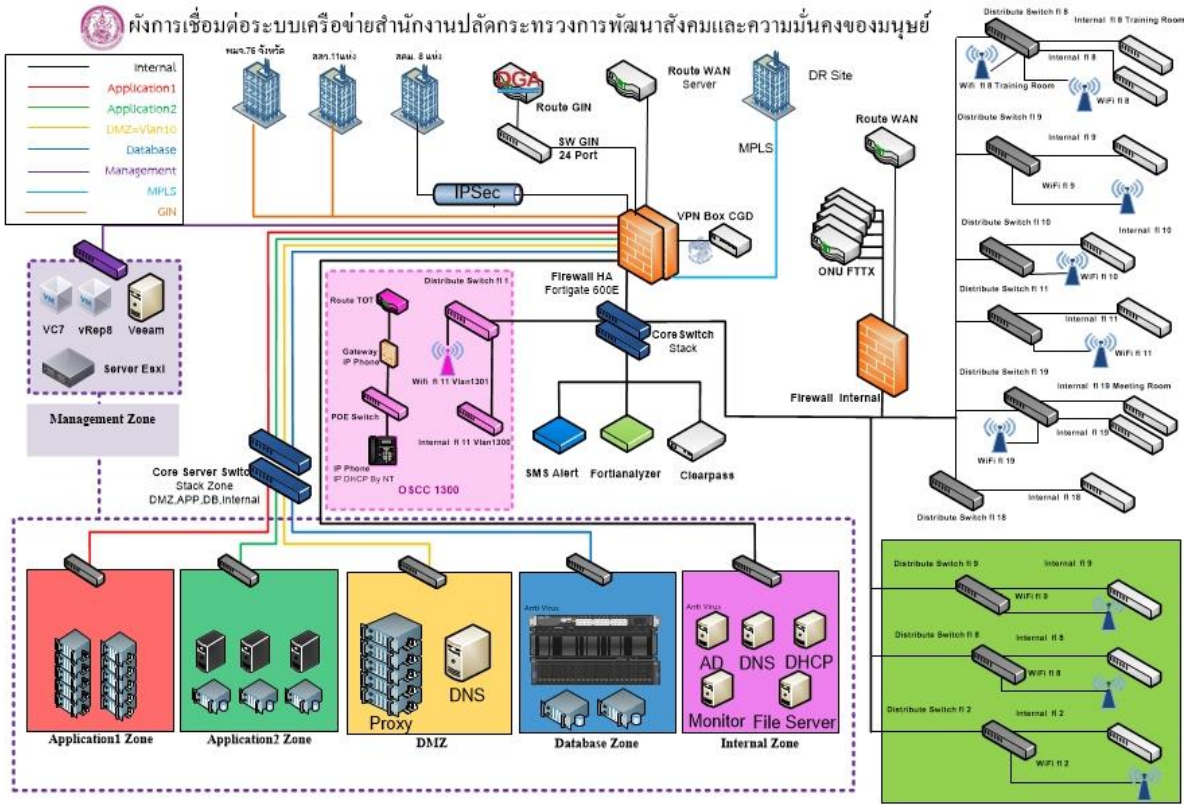
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือนและให้รายงานการเกิดปัญหาและผลการแก้ไขให้ผู้ที่ได้รับมอบหมาย/ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ เจ้าหน้าที่ที่รับผิดชอบจะต้องมีคำสั่งแต่งตั้งจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร สำหรับรูปแบบรายงานใช้รายงานการตรวจรับงานที่ดำเนินการบำรุงรักษาระบบฯ ประจำเดือนทุกเดือน

2.8 ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์ของ สป.พม. ได้มีการพัฒนาและปรับเพิ่มประสิทธิภาพอย่างต่อเนื่องเพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของ สป.พม. ตั้งอยู่ที่อาคารกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เลขที่ 1034 ถนนกรุงเกษม แขวงมหานาค เขตป้อมปราบศัตรูพ่าย กรุงเทพมหานคร มีการเชื่อมโยงเครือข่ายไปยังหน่วยงานภายในส่วนกลางของ สป.พม. และส่วนภูมิภาค สำนักงานพัฒนาสังคมและความมั่นคงของมนุษย์จังหวัด (พมจ.) ทุกจังหวัด

ระบบเครือข่ายคอมพิวเตอร์ของ สป.พม. มีการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเป็นระบบ ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการถูกโจมตีและการบุกรุกเข้ามายังระบบเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรองข้อมูล (Package Filter) ที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ส่วนกลาง สป.พม. จากเครือข่ายภายนอก เช่น เครือข่ายของสำนักงานปลัดกระทรวงฯ เครือข่ายอินเทอร์เน็ต และเครือข่าย GIN เป็นต้น นอกจากนี้ยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone หรือ Demineralized Zone : DMZ) ที่ดูแลเครื่องแม่ข่ายทั้งหมดของ สป.พม. ให้บุคคลภายนอกเข้าถึงได้ เช่น Web Server และ Mail Server เป็นต้น รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของ สป.พม. เพื่อให้ได้รับความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด

ผังระบบเครือข่ายสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์



3

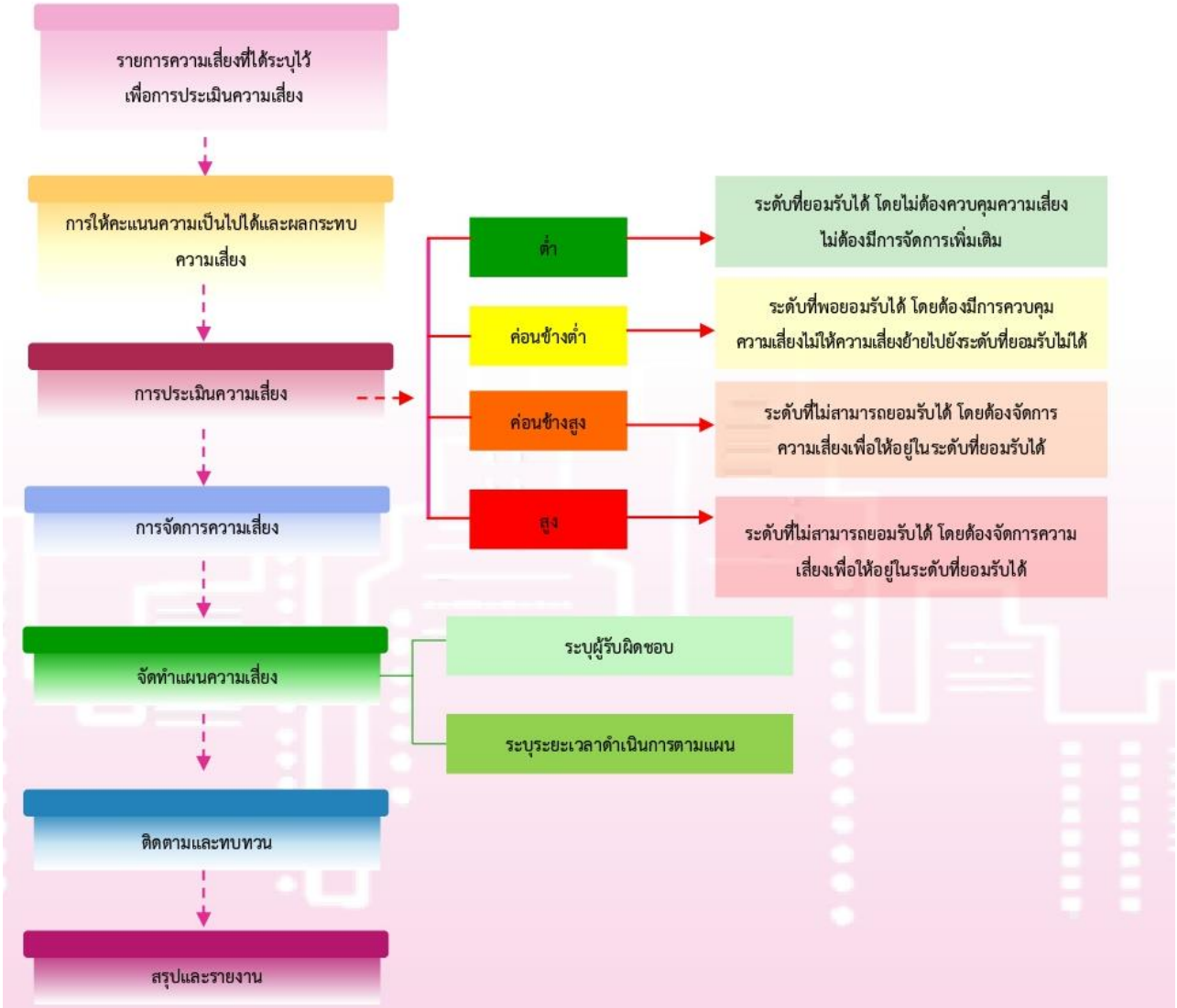
การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

บทที่ 3

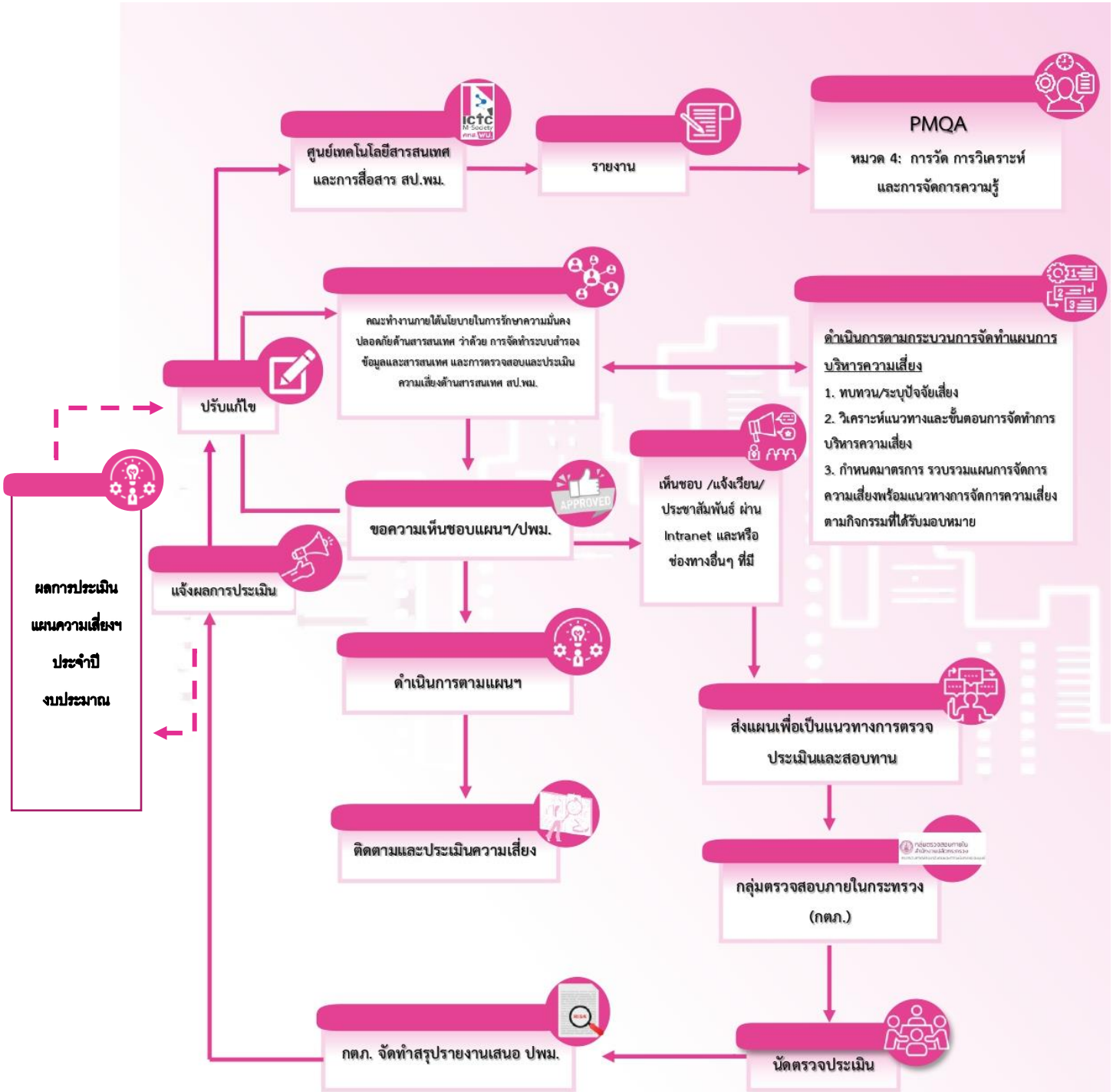
การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สป.พม. ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจเกิดความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงได้มอบหมายให้ ศทส. จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. 2566 โดยกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เริ่มต้นจากการรวบรวมกิจกรรม/ปัจจัยเสี่ยง ที่เกี่ยวข้องกับกระบวนการที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำการศึกษาข้อมูล ระดมความคิดเห็นกับเจ้าหน้าที่ผู้ปฏิบัติงานด้านกิจกรรมต่างๆ ดังนี้

3.1 แนวทางและขั้นตอนการบริหารความเสี่ยง



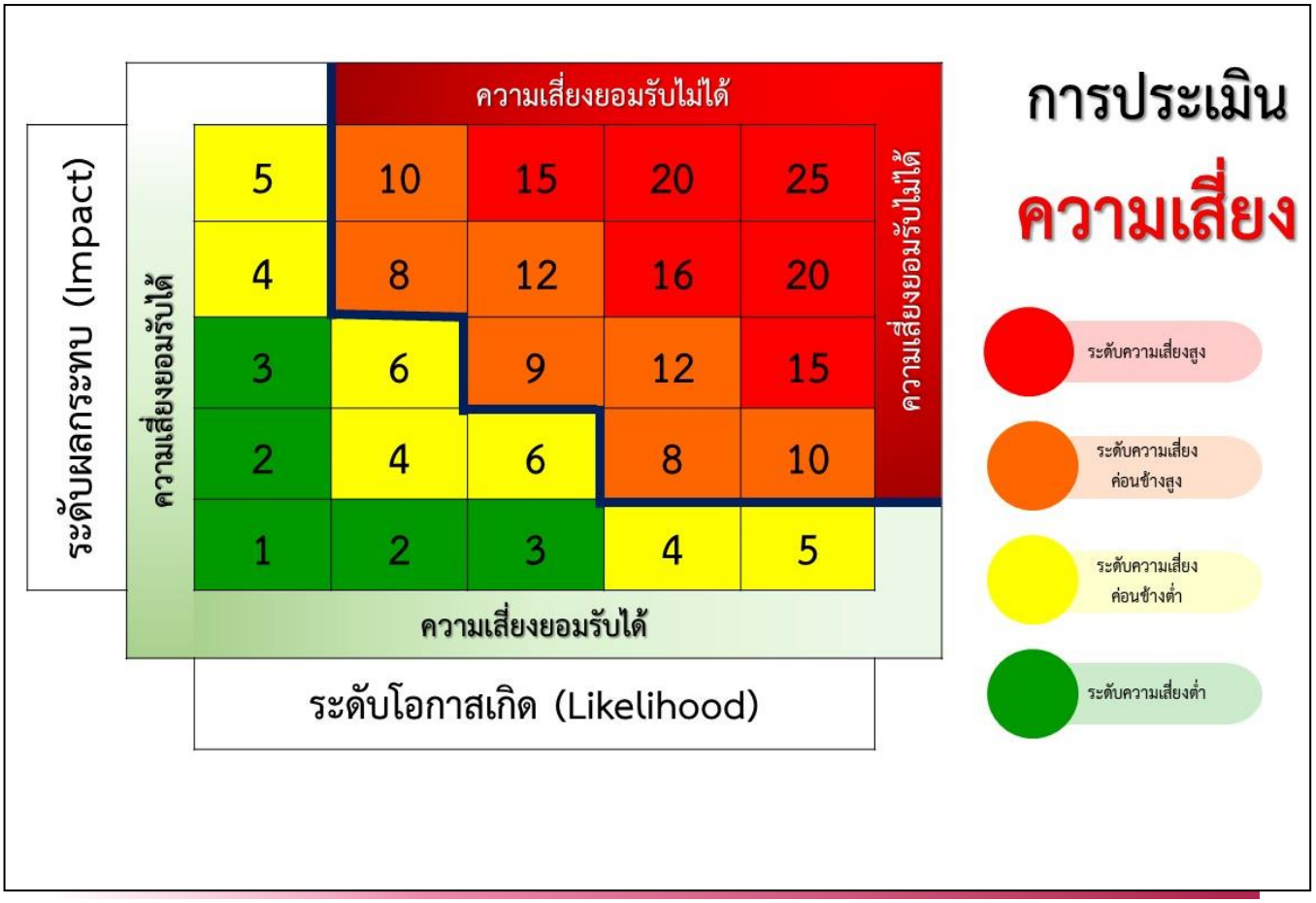
3.2 กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566



3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

การระบุความเสี่ยง (Rick identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่ ศทส. สป.พม. เผชิญอยู่ โดยมีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินความเป็นไปได้และผลกระทบ มีดังนี้

ระดับความเสี่ยง	ระดับสี	คำอธิบาย	คะแนน
สูง		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้	15 - 25
ค่อนข้างสูง		ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป	8 - 14
ค่อนข้างต่ำ		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้	4 - 7
ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม	1 - 3



3.4 ผลการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2565

ลำดับที่	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน
1	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามคำรับรองการปฏิบัติราชการ	2 (เดิม 2)	3 (เดิม 4)	6 (เดิม 8)
2	ถูกตัด/ปรับลดโครงการที่วางแผนไว้ ตามนโยบายการปรับลดงบประมาณของ สป.พม. - โครงการที่จำเป็นต้องดำเนินการถูกตัดตามนโยบายการปรับลดงบประมาณของ สป.พม.	2 (เดิม 3)	3 (เดิม 3)	6 (เดิม 9)
3	การปรับลดวงเงินงบประมาณที่ขอจัดสรร สำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	2 (เดิม 3)	3 (เดิม 3)	6 (เดิม 9)
4	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	2	3	6
5	เกิดช่องโหว่ของซอฟต์แวร์	2	3	6
6	ไฟไหม้ห้องศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	1	5	5
7	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	1	5	5
8	ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลของข้อมูลและระบบฐานข้อมูลครบถ้วน	1	5	5
9	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	1	5	5
10	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	1	5	5
11	ขาดการป้องกันหรือตรวจจับไวรัส	1	5	5
12	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	1	4	4
13	บุคลากรด้านไอทีมีความรู้ ความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	2	2	4
14	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	1	3	3
15	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	1	3	3
16	ไม่มีการกำหนดสิทธิ์และไม่ควบคุมการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	1	3	3

ลำดับที่	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน
17	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีรายการทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	1	3	3
18	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	1	3	3
19	การบริหารจัดการสิทธิ์ การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งาน ขาดประสิทธิภาพ	1	3	3
20	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	1	3	3
21	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	1	3	3
22	การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์	1	3	3
23	การนำเข้าข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และเกิดความผิดพลาดของระบบ (Bug)	1	3	3
24	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	1	3	3
25	ไม่มีบัญชีการเข้าถึงระบบปฏิบัติงาน (Operating System) และโปรแกรมประยุกต์ (Applications)	1	3	3
26	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	1	3	3
27	ผู้บริหารไม่ให้ความสำคัญต่อความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร	1	3	3
28	ผู้รับผิดชอบที่ได้รับมอบหมายไม่ทำการติดตามตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศ	1	3	3
29	การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	1	3	3
30	ผู้ใช้งาน/Users ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	1	3	3
31	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า/ไม่สามารถประกาศผลผู้ชนะการประกวดราคา/สัญญาไม่ตรงตามร่างข้อกำหนด/ไม่มีผู้เข้าประกวดราคาได้ทันเวลา	1	3	3
32	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อโยงข้อมูล	1	2	2

จากตารางการประเมินความเสี่ยงฯ จะเห็นได้ว่าปัจจัยเสี่ยง มีค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ 4 – 7 ซึ่งอยู่ในระดับความเสี่ยงค่อนข้างต่ำ เป็นการคงค่าคะแนนในกิจกรรมที่ไม่สามารถลดค่าคะแนนลงได้ เนื่องจากเป็นความเสี่ยงจากการทำงานในลักษณะคงที่ ซึ่งไม่ก่อให้เกิดปัจจัยเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงานและในบางปัจจัยเสี่ยงมีการเพิ่มเติมหรือปรับเปลี่ยนแนวทางการควบคุมความเสี่ยง เพื่อป้องกันไม่ให้

ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะต้องดำเนินการตามแนวทางการควบคุมความเสี่ยงอย่างต่อเนื่อง

ทั้งนี้ ได้นำข้อสังเกตจากผลการสอบทานและข้อเสนอแนะจากผู้ตรวจสอบภายในของ สป.พม. ในปีงบประมาณ พ.ศ. 2565 มาเป็นแนวทาง ในทบทวนและปรับปรุงแผนบริหารจัดการความเสี่ยงฯ ถ้ามีการเพิ่มกิจกรรมและปัจจัยเสี่ยงก็ให้ระบุเพิ่ม เพื่อให้มีการวิเคราะห์ระบุความเสี่ยงและสามารถลดความเสี่ยงได้ถูกต้องและมีประสิทธิภาพต่อไป ตลอดจนปรับปรุงแผนฯ ให้สอดคล้องกับการเปลี่ยนแปลงทั้งภายในและภายนอกหน่วยงาน ให้มีการอบรมให้ความรู้และเพิ่มทักษะให้แก่เจ้าหน้าที่ปฏิบัติงานเพื่อไม่ให้เกิดข้อผิดพลาดระหว่างการปฏิบัติงาน หรือ ที่หน่วยงานสามารถยอมรับได้ เพื่อลดความเสี่ยงในการใช้งานของผู้ปฏิบัติงาน โดยการประเมินในปีงบประมาณ พ.ศ. 2566 มีการปรับค่าคะแนนลงในกิจกรรมที่สามารถดำเนินการได้ และคงค่าคะแนนในกิจกรรมที่ไม่สามารถลดค่า เนื่องจากการทำงานเป็นความเสี่ยงลักษณะคงที่จึงไม่ก่อให้เกิดปัจจัยเสี่ยงที่ส่งผลกระทบต่อการดำเนินงาน

3.5 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

ปัจจัยเสี่ยง	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
1.การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติและสิ่งแวดล้อมและผลกระทบที่เกิดขึ้น		
1.1 ไฟไหม้ห้องศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
1.2 ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับไฟกระชากจากปลั๊กพ่วง	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
1.3 การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	- เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
1.4 ไม่มีการกำหนดสิทธิ์และไม่ควบคุมการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- มีการขโมยข้อมูลหรืออุปกรณ์ ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. - มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
1.5 ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะ ต่ออุปกรณ์ที่ติดตั้งภายในห้องไฟฟ้าสื่อสารตามชั้นต่างภายในอาคาร และพื้นที่สำนักงาน	- เจ้าหน้าที่ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตของ สป.พม. ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ

ปัจจัยเสี่ยง	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
2. การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ		
2.1 ขาดการทบทวน/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร ให้เป็นปัจจุบัน	- ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย - ขาดข้อมูลบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสารที่เป็นปัจจุจบัน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
2.2 ขาดมาตรการรองรับในการจัดการฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
2.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบุตัวตนผู้ใช้งานระบบ/ผู้ดูแลระบบไม่ได้ - หาผู้กระทำความผิดไม่ได้ - อุปกรณ์จำนวนเพิ่มมากขึ้น จึงอาจทำให้เกิดความผิดพลาดได้มากขึ้น	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
2.4 ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	- ระบบฯ เสียหาย/ขัดข้องไม่สามารถเข้าถึงบริการสารสนเทศได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
2.5 ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
2.6 ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน

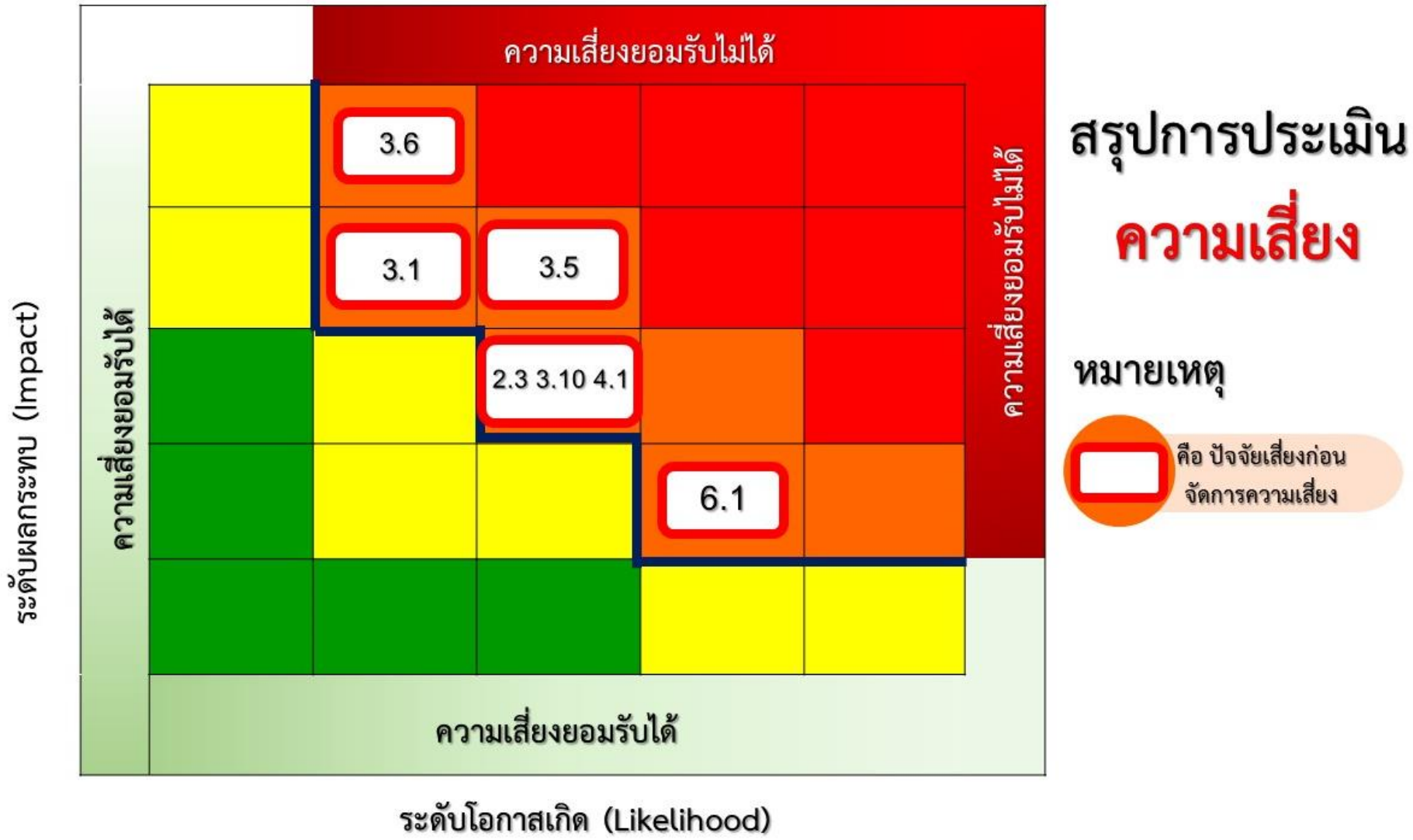
ปัจจัยเสี่ยง	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
3. ด้านระบบสารสนเทศและฐานข้อมูล วัตถุประสงค์ เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศฐานข้อมูลต่างๆ ถูกทำลาย จากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไข เปลี่ยนแปลงข้อมูล ทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้		
3.1 การโจมตีโดยบุคคลที่ ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3.2 ไม่มีการดำเนินการตามแผนการสำรองและทดสอบกู้คืนข้อมูล	- เกิดความเสียหายแก่ระบบข้อมูล/ฐานข้อมูลทำให้ใช้งานไม่ต่อเนื่อง - ไม่สามารถกู้คืนระบบข้อมูล/ฐานข้อมูลได้ เนื่องจากไม่มีการกำหนดแผนสำรองในภาวะฉุกเฉิน	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - หน่วยงาน
3.3 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ - ถูกโจมตีระบบทำให้ไม่สามารถให้บริการได้	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - หน่วยงาน
3.4 การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบ ที่มีการพัฒนาไว้อย่างหลากหลาย - อาจต้องสูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูง เกิดความไม่คุ้มค่า	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3.5 เกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3.6 ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	- อาจเกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ - เกิดช่องโหว่อันเกิดจากไม่มีการอัปเดตเวอร์ชันใหม่ๆ อย่างสม่ำเสมอ ทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง/ในเวลาที่ต้องการ - ผู้ดูแลระบบไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3.7 การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ออกรายงานผิดพลาด	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน

ปัจจัยเสี่ยง	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
3.8 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3.9 ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	- ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3.10 ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	- ไม่มีความมั่นคงปลอดภัยในการเข้าใช้งานเนื่องจากไม่มีการควบคุมการเข้าถึง - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
4. ด้านโปรแกรมคอมพิวเตอร์ <u>วัตถุประสงค์</u> - เพื่อควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัปเดต - เพื่อลดช่องโหว่ที่เกิดจาก Bug ของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์ หมายเหตุ : Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้นๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้		
4.1 ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) หมายเหตุ : Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการ Windows เรียกง่ายๆ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของ Windows เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
4.2 ขาดการป้องกันหรือตรวจจับ Malware	- เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบสารสนเทศและฐานข้อมูล - เกิดผลกระทบต่อการใช้งานเครือข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
5. ด้านบุคลากร <u>วัตถุประสงค์</u> เพื่อควบคุมความเสี่ยงที่เกิดจากการดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงที่เกิดจากความล้มเหลวหรือความไม่เหมาะสมของบุคลากร		
5.1 มีการใช้บัญชีผู้ใช้งาน (username) ร่วมกัน ในการเข้าถึงระบบสารสนเทศและยืนยันตัวตนอินเทอร์เน็ต	- ไม่สามารถระบุตัวตนผู้ใช้งานได้ เมื่อมีผู้ใช้งานกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และเครือข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน

ปัจจัยเสี่ยง	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
	- ไม่สามารถตรวจสอบการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศได้ - ผู้รับผิดชอบที่ได้รับมอบหมายไม่สามารถติดตามตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศได้	
5.2 การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญ ความเชี่ยวชาญ ในการดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
5.3 บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	- เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้ - มีค่าใช้จ่ายในการบำรุงรักษาเพิ่มมากขึ้น	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
5.4 ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญและทักษะในการใช้งานระบบ	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ทำให้งานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ ข้อมูลไม่ถูกนำไปใช้งาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
5.5 ผู้ใช้งาน (Users) ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	ผู้ใช้งาน (Users) ใช้งานเครือข่ายอินเทอร์เน็ตของ สป.พม. ในการเข้าเว็บไซต์ที่ไม่เหมาะสม / ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต / นำอุปกรณ์ที่ไม่ได้รับอนุญาตมาติดตั้ง ทำให้เครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้ และเครือข่ายอินเทอร์เน็ตของหน่วยงานทำงานผิดพลาด	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
6. ด้านงบประมาณ วัตถุประสงค์ เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ /การเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา		
6.1 การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	- ตามนโยบายของหน่วยงานมีการปรับลดงบประมาณโดยลดเป็นเปอร์เซ็นต์เท่าๆ กัน ทำให้โครงการที่จำเป็นจะต้องดำเนินการถูกตัด/ปรับลดไปด้วย - งวดเงิน/งวดงาน ไม่สอดคล้องกัน เนื่องจากการบริหารงบประมาณของภาครัฐและหน่วยงานมีการโอนงวดเงินเป็นเปอร์เซ็นต์ที่เท่ากัน	- หน่วยงานซึ่งเป็นหน่วยรับงบประมาณ

ปัจจัยเสี่ยง	ลักษณะความเสี่ยง ความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
7. ด้านการบริหารจัดการ วัตถุประสงค์ เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี จากการกำกับดูแลที่ดี หรือ ขาดธรรมาภิบาลในองค์กร ขาดการควบคุมที่ดี		
7.1 ความเสี่ยงจากการจัดซื้อจัดจ้าง - กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคาได้ - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา - ผู้รับจ้างไม่ปฏิบัติตามข้อกำหนด	- เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - ไม่สามารถตรวจรับงานได้ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปีได้ ทำให้มีผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน
7.2 แผนเตรียมความพร้อมกรณีฉุกเฉินไม่ครอบคลุมกับสถานการณ์ที่เกิดขึ้น เช่น กรณีเกิดสถานการณ์ ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติ เนื่องจากถูกปิดล้อมสถานที่ทำงาน หน่วยงานถูกตัดกระแสไฟฟ้าทำให้ระบบงานหยุดทำงานไม่สามารถให้บริการได้ เนื่องจากไม่สามารถเข้าระบบจากระยะไกล (Remote) ได้	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน

3.6 การจัดทำแผนภูมิความเสี่ยง (Risk Map) ก่อนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร



3.7 การประเมินแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
1. การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม									
วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น									
1.1	ไฟไหม้ห้องศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	1	5	5	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติ โดยการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้าน	1	5	5
1.2	ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับไฟกระชากจากปลั๊กพ่วง	1	4	4	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS) / แบตเตอรี่สำรองไฟ	1	4	4
1.3	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	1	3	3	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น และมีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ	1	3	3
1.4	ไม่มีการกำหนดสิทธิ์และไม่ควบคุมการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	2	3	6	ควบคุมความเสี่ยง	บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการ ในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง	1	3	3
1.5	ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะ ต่ออุปกรณ์ที่ติดตั้ง	2	2	4	ควบคุมความเสี่ยง	- มีการฉีดยาป้องกันแมลง บริเวณภายในอาคารเป็นประจำ	2	2	4

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
	ภายในห้องไฟฟ้าสื่อสารตามชั้นต่างภายในอาคาร และพื้นที่สำนักงาน					- ตรวจสอบและบำรุงรักษาอุปกรณ์อย่างต่อเนื่อง - จัดพื้นที่สำหรับรับประทานอาหารให้เป็นสัดส่วน			
2. การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ									
2.1	ขาดการทบทวน/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร ให้เป็นปัจจุบัน	1	3	3	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์	1	3	3
2.2	ขาดมาตรการรองรับในการจัดการฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	2	3	6	ควมคุมความเสี่ยง	- มีมาตรการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบ ในรายการครุภัณฑ์ที่มีความสำคัญ - ทดสอบการโจมตีตามมาตรการที่กำหนด	2	2	4
2.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพอาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์	3	3	9	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการ เปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ ทุก 6 เดือน	2	3	6

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
	เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด								
2.4	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	1	3	3	ควบคุมความเสี่ยง	- ระบุข้อกำหนด/ข้อตกลง ระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบหรือ ผอ. ศทส. ทุกครั้งที่ระบบฯ ขัดข้องเพื่อให้แก้ปัญหาได้ทันท่วงที	1	3	3
2.5	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	2	3	6	ควบคุมความเสี่ยง	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และยืนยันตัวบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา - มีการปรับเพิ่มประสิทธิภาพการบริหารจัดการทุกปี	2	2	4
2.6	ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	2	3	6	ควบคุมความเสี่ยง	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ	2	3	6

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
						- บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน			
3. ด้านระบบสารสนเทศและฐานข้อมูล วัตถุประสงค์ เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศฐานข้อมูลต่างๆ ถูกทำลาย จากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้								
3.1	การโจมตีโดยบุคคลที่ ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.	2	4	8	จัดการความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายในหรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	2	3	6

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
						- จัดทำการสำรองข้อมูลระบบฐานข้อมูล อย่างสม่ำเสมอ อย่างน้อยสัปดาห์ละ 1 ครั้ง - จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. ให้สอดคล้องกับสถานการณ์ปัจจุบันอย่างเหมาะสม - การทดสอบการเจาะระบบสารสนเทศที่สำคัญเพื่อหาช่องโหว่ อย่างน้อยปีละ 1 ครั้ง - VA scan เพื่อค้นหาช่องโหว่ของระบบปฏิบัติการ ระบบแอปพลิเคชัน และระบบฐานข้อมูล - ปรับปรุง source code เพื่อปิดช่องโหว่ที่ตรวจพบ หมายเหตุ : VPN (Virtual Private Network) ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้			
3.2	ไม่มีการดำเนินการตามแผนการสำรองและทดสอบกู้คืนข้อมูล	1	5	5	ควบคุมความเสี่ยง	- จัดทำการสำรองข้อมูลแบบอัตโนมัติโดยจัดเก็บ Storage ทุกวัน เฉพาะส่วนที่เพิ่มในแต่ละวัน และจัดเก็บข้อมูลทั้งระบบแบบ Full Backup บน Storage สัปดาห์ละ 1 ครั้ง - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติโดยจัดเก็บใน Hard Disk เป็นประจำทุกเดือน	1	5	5

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
						- มีการทดสอบการกู้คืนข้อมูลของทุกระบบงานอย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการเตรียมความพร้อมหากเกิดสถานการณ์ฉุกเฉิน - มีการควบคุมกำกับการสำรองข้อมูลให้เป็นไปตามแผนพร้อมทั้งการตรวจสอบความสมบูรณ์ในการสำรองข้อมูลทุกครั้ง			
3.3	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	1	5	5	ควบคุมความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึงระบบเครือข่าย - ทบทวน/กำหนดสิทธิ์ VPN ในการเข้าถึงระบบเครือข่ายจากระยะไกล เช่น กำหนดช่วงเวลาในการเข้าใช้ VPN อย่างน้อยปีละ 1 ครั้ง - มีการกำหนดเงื่อนไขการเข้าใช้งานที่ไม่ถูกต้อง เช่น จำกัดจำนวนครั้งของการผิดพลาดในการเข้าใช้งาน เป็นต้น - มีการติดตาม/ตรวจสอบ การเข้าใช้งานของผู้ใช้งานอย่างสม่ำเสมอ	1	5	5
3.4	การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์	1	3	3	ควบคุมความเสี่ยง	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์ และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตามทุกขั้นตอนของการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐาน และ TOR	1	3	3

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
3.5	เกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต	3	4	12	จัดการความเสี่ยง	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ และมีการกำหนดไว้ใน TOR ในการบำรุงรักษาระบบสารสนเทศ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้งานได้รับทราบอย่างต่อเนื่อง - ดำเนินการปรับปรุง version ของระบบปฏิบัติการและบริการของระบบสารสนเทศ ให้เป็นปัจจุบัน	1	4	4
3.6	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	2	5	10	จัดการความเสี่ยง	- จัดทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่องเพื่อปิดช่องโหว่โดยการอัปเดตเวอร์ชันใหม่ๆ อย่างสม่ำเสมอ ทำให้สามารถใช้งานระบบได้อย่างต่อเนื่องและในเวลาที่ต้องการได้ - จัดทำ TOR ในการจัดซื้อจัดจ้างการพัฒนาระบบ ให้ครอบคลุมถึงการอบรมให้ความรู้ในการแก้ไขปัญหา เมื่อระบบขัดข้อง พร้อมทั้งส่งคู่มือระบบการใช้งานและแก้ไขปัญหาให้กับผู้ดูแลระบบ	1	5	5
3.7	การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	2	3	6	ควบคุมความเสี่ยง	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพ	1	3	3

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
						ข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - รวบรวมข้อผิดพลาดที่เกิดขึ้น และปรับปรุงระบบ ให้สามารถป้องกันการนำเข้าข้อมูลที่ผิดพลาดได้			
3.8	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	1	3	3	ควบคุมความเสี่ยง	- ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ - กำหนดนโยบายในการนำเข้าข้อมูล - กำหนดตัวชี้วัด - กำหนดรายการข้อมูลที่สำคัญ - พัฒนาระบบให้ตรงตามความต้องการของผู้ใช้งาน - ประสานความร่วมมือกับผู้รับผิดชอบหลักในการบันทึกข้อมูล	1	3	3
3.9	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	2	2	4	ควบคุมความเสี่ยง	- มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลาง กระทรวง พม. อย่างต่อเนื่อง - มีการติดตามการนำมาตรฐานข้อมูลกลาง กระทรวง พม. ไปใช้อย่างสม่ำเสมอ - มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) - มีการดำเนินงานทบทวน/ปรับปรุงและเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลางกระทรวง พม.	1	2	2

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
						ที่ครอบคลุมภารกิจของกระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ			
3.10	ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	3	3	9	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์ในการเข้าถึง เพื่อทำการจำกัดและควบคุมการเข้าถึง - ใช้งานโปรแกรมเพื่อป้องกันการละเมิด โดยการตรวจสอบสิทธิ์ - มีการทบทวนสิทธิ์เป็นประจำ โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ อย่างน้อยปีละ 1 ครั้ง - ปฏิบัติตามข้อปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. อย่างเคร่งครัด	1	3	3

4. ด้านโปรแกรมคอมพิวเตอร์

<u>วัตถุประสงค์</u>

- เพื่อควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัปเดต
- เพื่อลดช่องโหว่ที่เกิดจาก Bug ของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์

หมายเหตุ : Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้นๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้

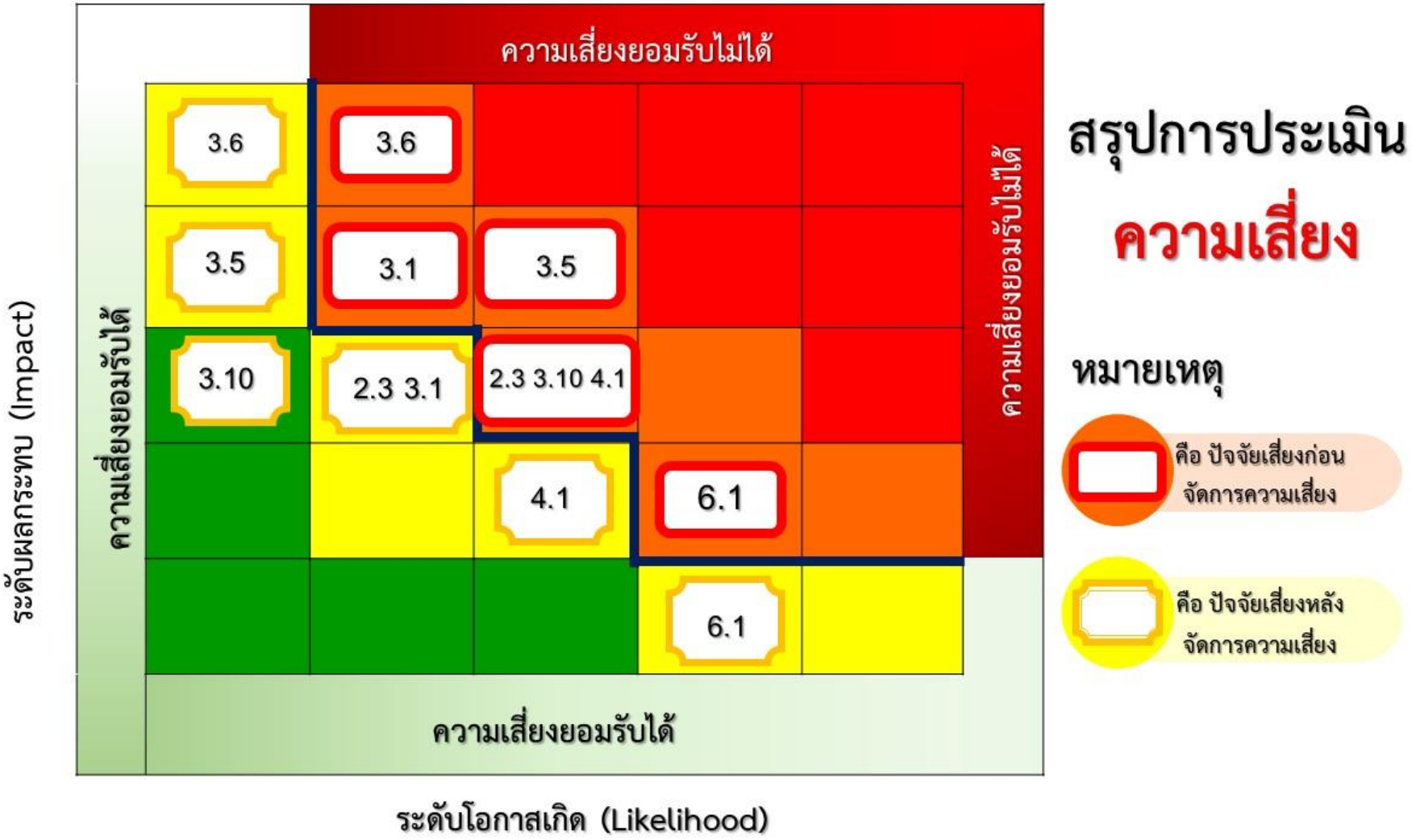
รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
4.1	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	3	3	9	จัดการความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - จัดทำ และส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย	3	2	6
4.2	ขาดการป้องกันหรือตรวจจับ Malware	1	5	5	ควบคุมความเสี่ยง	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ - จัดทำ VLAN เพื่อแบ่งเครือข่ายออกเป็นกลุ่มย่อย - ส่งเสริมให้บุคลากรมีการสำรองข้อมูลที่สำคัญในเครื่อง PC ของตนเองอย่างสม่ำเสมอ	1	4	4
5. ด้านบุคลากร วัตถุประสงค์ เพื่อควบคุมความเสี่ยงที่เกิดจากการดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงที่เกิดจากความล้มเหลวหรือความไม่เหมาะสมของบุคลากร									
5.1	มีการใช้บัญชีผู้ใช้งาน (username) ร่วมกัน ในการเข้าถึงระบบสารสนเทศและยืนยันตัวตนอินเทอร์เน็ต	1	3	3	ควบคุมความเสี่ยง	- ปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม. โดยใช้แบบฟอร์มการขอใช้งานบัญชีผู้ใช้งาน เพื่อการจัดเก็บ Log ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บ	1	3	3

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
						รักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ - ส่งเสริมให้ผู้ใช้งานตระหนักถึงโทษตาม พ.ร.บ. คอมพิวเตอร์ฯ และความเสียหายที่จะเกิดขึ้น - ทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศและอินเทอร์เน็ตอย่างน้อยปีละ 1 ครั้ง			
5.2	การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญ ความเชี่ยวชาญ ในการดูแลบำรุงรักษาระบบ/พัฒนาระบบ	1	3	3	ควบคุมความเสี่ยง	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจน และควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้ - มีการติดตามเพื่อป้องกันการเกิดข้อผิดพลาดและแก้ไขปัญหาได้ทันที โดยมีการประชุมทุกสัปดาห์	1	3	3
5.3	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	2	3	6	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง - มีการจัดทำคู่มือในการปฏิบัติงานเฉพาะด้าน สำหรับผู้ดูแลระบบ เช่น application admin , system admin	2	3	6

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
5.4	ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญและทักษะในการใช้งานระบบ	2	3	6	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีระบบ Call Center/ help desk สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุง หรือตามความต้องการของ User - สร้างความตระหนักถึงประโยชน์ของการนำข้อมูลไปใช้ในการวางแผนและปฏิบัติงาน - กำหนดการใช้งานระบบเป็นตัวชี้วัดหน่วยงานในเชิงคุณภาพ	2	3	6
5.5	ผู้ใช้งาน (Users) ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	1	3	3	ควบคุมความเสี่ยง	- มีนโยบายและแนวทางในการควบคุมการใช้คอมพิวเตอร์ ไม่ให้ใช้เครือข่ายผิดวัตถุประสงค์ - ควบคุมและบังคับใช้อย่างเคร่งครัด พร้อมทั้งกำหนดบทลงโทษ - จัดหาอุปกรณ์ตรวจสอบการเข้าถึงเครือข่ายและตรวจสอบระบบเครือข่ายอย่างสม่ำเสมอ	1	3	3
6. ด้านงบประมาณ วัตถุประสงค์ เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ /การเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา									
6.1	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	4	2	8	จัดการความเสี่ยง	- ปรับโครงการโดยจัดลำดับความสำคัญใหม่ ลดขอบเขตงานลง - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ - บริหารจัดการงบประมาณภายในหน่วยงานให้มีประสิทธิภาพ	4	1	4

รหัส	ปัจจัยเสี่ยง	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
		โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)			โอกาสความถี่ (1)	ผลกระทบความรุนแรง (2)	ระดับคะแนน (1)x(2)
7. ด้านการบริหารจัดการ วัตถุประสงค์ เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี จากการกำกับดูแลที่ดี หรือ ขาดธรรมาภิบาลในองค์กร ขาดการควบคุมที่ดี									
7.1	ความเสี่ยงจากการจัดซื้อจัดจ้าง - กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคาได้ - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา - ผู้รับจ้างไม่ปฏิบัติตามข้อกำหนด	1	4	4	ควบคุมความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการ - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสม เพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด	1	3	3
7.2	แผนเตรียมความพร้อมกรณีฉุกเฉินไม่ครอบคลุมกับสถานการณ์ที่เกิดขึ้น เช่น กรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	1	5	5	ควบคุมความเสี่ยง	- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และทบทวนแผนฯ อย่างน้อยปีละ 1 ครั้ง - มอบหมายผู้รับผิดชอบ และดำเนินการตามแผนฯ อย่างเคร่งครัด	1	3	3

3.8 การจัดทำแผนภูมิความเสี่ยง (Risk Map) หลังการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร



ปีงบประมาณ พ.ศ. 2566 ศทส. ได้ทำการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และได้จัดทำแผนบริหารจัดการความเสี่ยง กำหนดกิจกรรม กำหนดเป้าหมายการดำเนินการ โดยเพิ่มมาตรการจัดการความเสี่ยงและควบคุมความเสี่ยงให้อยู่ในระดับคะแนนที่ยอมรับและควบคุมความเสี่ยงได้ ซึ่งผลจากการวิเคราะห์และประเมินความเสี่ยงฯ สรุปได้ว่า มีปัจจัยเสี่ยงที่อยู่ในระดับคะแนนความเสี่ยงค่อนข้างสูง จำนวน 7 ปัจจัยเสี่ยง ดังนี้

ความเสี่ยงด้านการควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร

รหัส 2.3 ปัจจัยเสี่ยงการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด

ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล

รหัส 3.1 ปัจจัยเสี่ยงการโจมตีโดยบุคคลที่ ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.

รหัส 3.5 ปัจจัยเสี่ยงเกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต

รหัส 3.6 ปัจจัยเสี่ยงขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง

รหัส 3.10 ปัจจัยเสี่ยงไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)

ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

รหัส 4.1 ปัจจัยเสี่ยงละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)

ความเสี่ยงด้านงบประมาณ

รหัส 6.1 ปัจจัยเสี่ยงการปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด

จากนั้น ได้ศึกษาและวิเคราะห์ความเสี่ยงฯ ที่จะเป็นเหตุให้เกิดปัจจัยเสี่ยงใหม่ที่อาจจะทำให้เกิดความเสียหายเพิ่มขึ้น ได้แก่ ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะต่ออุปกรณ์ที่ติดตั้งภายในห้องไฟฟ้าสื่อสารตามชั้นต่างๆ ภายในอาคาร และพื้นที่สำนักงาน ซึ่งอยู่ภายใต้ความเสี่ยงด้านการรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม โดยให้ดำเนินการตามแผนความเสี่ยงฯ เดิมต่อไป และมีการปรับลดค่าคะแนนให้อยู่ในระดับที่ยอมรับได้

3.9 แผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

ปัจจัยเสี่ยง	กิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี 2565			ปี 2566									ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	มค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ความเสี่ยงด้านการควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร														
รหัส 2.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการ เปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ ทุก 6 เดือน	←	-	-	-	-	-	-	-	-	-	-	→	ศทส.
ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล														
รหัส 3.1 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายในหรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	←	-	-	-	-	-	-	-	-	-	-	→	ศทส.

ปัจจัยเสี่ยง	กิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี 2565			ปี 2566									ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	มค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
	- จัดทำการสำรองข้อมูลระบบฐานข้อมูล อย่างสม่ำเสมอ อย่างน้อยสัปดาห์ละ 1 ครั้ง - จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. ให้สอดคล้องกับสถานการณ์ปัจจุบันอย่างเหมาะสม - การทดสอบการเจาะระบบสารสนเทศที่สำคัญเพื่อหาช่องโหว่ อย่างน้อยปีละ 1 ครั้ง - VA scan เพื่อค้นหาช่องโหว่ของระบบปฏิบัติการ ระบบแอปพลิเคชัน และระบบฐานข้อมูล - ปรับปรุง source code เพื่อปิดช่องโหว่ที่ตรวจพบ หมายเหตุ : VPN (Virtual Private Network) ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้													
รหัส 3.5 เกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอและมีการกำหนดไว้ใน TOR ในการบำรุงรักษาระบบสารสนเทศ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้งานได้รับทราบอย่างต่อเนื่อง	←	-	-	-	-	-	-	-	-	-	-	-	→	ศทส.

ปัจจัยเสี่ยง	กิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี 2565			ปี 2566									ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	มค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
	- ดำเนินการปรับปรุง version ของระบบปฏิบัติการและบริการของระบบสารสนเทศ ให้เป็นปัจจุบัน													
รหัส 3.6 ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	- จัดทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่องเพื่อปิดช่องโหว่โดยการอัปเดตเวอร์ชันใหม่ๆ อย่างสม่ำเสมอ ทำให้สามารถใช้งานระบบได้อย่างต่อเนื่องและในเวลาที่ต้องการได้ - จัดทำ TOR ในการจัดซื้อจัดจ้างการพัฒนาระบบ ให้ครอบคลุมถึงการอบรมให้ความรู้ในการแก้ไขปัญหา เมื่อระบบขัดข้อง พร้อมทั้งส่งคู่มือระบบการใช้งานและแก้ไขปัญหาให้กับผู้ดูแลระบบ	←	-	-	-	-	-	-	-	-	-	-	→	ศทส.
รหัส 3.10 ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	- มีการกำหนดสิทธิ์ในการเข้าถึง เพื่อทำการจำกัดและควบคุมการเข้าถึง - ใช้งานโปรแกรมเพื่อป้องกันการละเมิด โดยการตรวจสอบสิทธิ์ - มีการทบทวนสิทธิ์เป็นประจำ โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ อย่างน้อยปีละ 1 ครั้ง - ปฏิบัติตามข้อปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. อย่างเคร่งครัด	←	-	-	-	-	-	-	-	-	-	-	→	ศทส.

ปัจจัยเสี่ยง	กิจกรรมตามแนวทางการจัดการความเสี่ยง	ปี 2565			ปี 2566									ผู้รับผิดชอบ
		ต.ค.	พ.ย.	ธ.ค.	มค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์														
รหัส 4.1 ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - จัดทำ และส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย	←	-	-	-	-	-	-	-	-	-	-	→	ศทส.
ความเสี่ยงด้านงบประมาณ														
รหัส 6.1 การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	- ปรับโครงการโดยจัดลำดับความสำคัญใหม่ ลดขอบเขตงานลง - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ - บริหารจัดการงบประมาณภายในหน่วยงานให้มีประสิทธิภาพ	←	-	-	-	-	-	-	-	-	-	-	→	ศทส.

หมายเหตุ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารประจำปี พ.ศ. 2566 จะเริ่มตั้งแต่ ตุลาคม 2565 – กันยายน 2566 (เป็นการควบคุมตามรอบปีงบประมาณประจำปี พ.ศ. 256

4 สรุปผล และข้อเสนอแนะ

บทที่ 4

สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรมหน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากความเสี่ยงที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อมีการปรับเปลี่ยน โดยเทคโนโลยีสารสนเทศและการสื่อสาร เข้ามามีบทบาทสำคัญเป็นกลไกในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีการปรับเปลี่ยน โดยเทคโนโลยีสารสนเทศและการสื่อสารช่วยทำให้ความซ้ำซ้อนของกระบวนการทำงานลดลง และสามารถให้บริการที่รวดเร็วและการเข้าถึงบริการที่ง่ายขึ้นสะดวกขึ้น ซึ่งในแต่ละวันมีปริมาณข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้กับการปฏิบัติงานของทุกหน่วยงานภายใน สป.พม.

การทบทวนและจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566 เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ หรือความเสี่ยงที่ได้จัดการไปแล้วแต่ยังควบคุมความเสี่ยงต่อ ประกอบการตัดสินใจว่าจะต้องจัดการความเสี่ยง ลดโอกาส/ความเสียหายที่จะเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้ จัดการความเสี่ยงจากความเสี่ยงสูง โดยจะต้องมีมาตรการ แนวทาง/กิจกรรมควบคุม เพื่อให้ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ตามสถานการณ์จริง

4.1 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

การระบุความเสี่ยง (Risk Identification) เป็นการบ่งชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่ สป.พม. เผชิญอยู่ จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในปีงบประมาณ พ.ศ. 2566 มีผลคะแนนที่ได้จัดการความเสี่ยง เพื่อควบคุมและจัดทำแผนความเสี่ยง ให้ไปอยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยเมื่อมีการจัดการความเสี่ยงและควบคุมความเสี่ยงได้ ระดับความเสี่ยงจะมีค่าคะแนนที่ค่อนข้างต่ำ สรุปได้ดังนี้

รหัส	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	คะแนน	แนวทางการจัดการความเสี่ยง
2.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพอาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด	2	3	6	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง
3.1	การโจมตีโดยบุคคลที่ ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.	2	3	6	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง
3.5	เกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต	1	4	4	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง
3.6	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	1	5	5	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง
3.10	ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	1	3	3	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง
4.1	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	3	2	6	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง
6.1	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	4	1	4	จัดทำแผนการจัดการความเสี่ยงและยอมรับความเสี่ยง

4.2 สรุปผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

ปีงบประมาณ พ.ศ. 2566 มีแผนการกำหนดกิจกรรม แนวทาง และกำหนดเป้าหมาย/ความสำเร็จ ในการบริหารจัดการความเสี่ยงฯ ทั้งหมด 4 ประเภท รวมจำนวน 7 ปัจจัยเสี่ยง ดังนี้

1) ความเสี่ยงด้านการควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 1 ปัจจัยเสี่ยง คือ

รหัส 2.3 ปัจจัยเสี่ยงการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบ ขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด ก่อนมีแนวทางควบคุมมีค่าคะแนนที่ 9 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 6 คือ ค่อนข้างต่ำ ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

2) ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล จำนวน 4 ปัจจัยเสี่ยง คือ

รหัส 3.1 ปัจจัยเสี่ยงการโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.ก่อนมีแนวทางควบคุม มีค่าคะแนนที่ 8 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 6 คือ ค่อนข้างต่ำ ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.5 ปัจจัยเสี่ยงเกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดตก่อนมีแนวทางควบคุมมีค่าคะแนนที่ 12 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการ ค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 4 คือ ค่อนข้างต่ำ ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.6 ปัจจัยเสี่ยงขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง ก่อนมีแนวทางควบคุม มีค่าคะแนนที่ 10 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 5 คือ ค่อนข้างต่ำ ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.10 ปัจจัยเสี่ยงไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications) ก่อนมีแนวทางควบคุม มีค่าคะแนนที่ 9 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 3 คือ ต่ำ เนื่องจากได้เพิ่มมาตรการควบคุมความเสี่ยง อาทิ ปฏิบัติตามข้อปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. อย่างเคร่งครัด ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลงจนสามารถควบคุมและยอมรับได้ต่อไป

3) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ จำนวน 1 ปัจจัยเสี่ยง คือ

รหัส 4.1 ปัจจัยเสี่ยงละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) ก่อนมีแนวทางควบคุม มีค่าคะแนนที่ 9 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 6 คือ ค่อนข้างต่ำ ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

4) ความเสี่ยงด้านงบประมาณ จำนวน 1 ปัจจัยเสี่ยง คือ

รหัส 6.1 ปัจจัยเสี่ยงการปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด ก่อนมีแนวทางควบคุม มีค่าคะแนนที่ 8 คือ ค่อนข้างสูง เมื่อได้มีการควบคุมและยอมรับความเสี่ยงแล้ว สามารถจัดการค่าคะแนนปรับลดลงอยู่ในค่าคะแนนที่ 4 คือ ค่อนข้างต่ำ ซึ่งจะต้องมีการควบคุมให้ค่าคะแนนไม่เคลื่อนไปในระดับที่สูงขึ้นหรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

ทั้งนี้ การประเมินความเสี่ยงเป็นไปตามข้อพิจารณาและสอบทานตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. พ.ศ. 2565 โดยทำการวิเคราะห์ ประเมินความเสี่ยง ทบทวนข้อมูลผลการดำเนินงาน ความเพียงพอ ความเชื่อถือได้ของการบริหารจัดการความเสี่ยงฯ ของกลุ่มตรวจสอบภายใน สป.พม. โดยได้ให้ ศทส. ปรับแก้ไขข้อผิดพลาดและคำอธิบายเพิ่มเติม

นอกจากนี้ ในปีงบประมาณ พ.ศ. 2566 ได้มีการเพิ่มเติมปัจจัยเสี่ยงแผนเตรียมความพร้อมกรณีฉุกเฉินไม่ครอบคลุมกับสถานการณ์ที่เกิดขึ้น เช่น กรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง ภายใต้ความเสี่ยงด้านการบริหารจัดการ พร้อมทั้งหาแนวทางในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และมีการยกเลิกความเสี่ยงด้านกลยุทธ์ เนื่องจากได้วิเคราะห์แล้วเห็นว่า การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม. ไม่มีปัจจัยเสี่ยงที่เกี่ยวข้องภายใต้ความเสี่ยงด้านกลยุทธ์ที่จะนำมาบริหารจัดการความเสี่ยง

4.3 ข้อเสนอแนะจากผลการสอบทานของกลุ่มตรวจสอบภายใน สป.พม.

สรุปข้อเสนอแนะในปีงบประมาณ พ.ศ. 2565 ของกลุ่มตรวจสอบภายใน สป.พม. เพื่อเป็นแนวทางในการปรับปรุงการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีดังนี้

จากการวิเคราะห์แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ สป.พม. โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะเห็นได้ว่ามีแนวทางในการควบคุมความเสี่ยง โดยการถ่ายโอนความเสี่ยงให้ภาคเอกชนดำเนินการแทนและยอมรับความเสี่ยง ซึ่งไม่ต้องดำเนินการจัดการความเสี่ยง เนื่องจากความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้ แต่ต้องมีการเฝ้าระวังอย่างต่อเนื่อง รวมทั้งเพิ่มเติมแนวทางการควบคุมความเสี่ยง เพื่อให้ความเสี่ยงที่ยังคงมีอยู่หรือที่อาจจะเกิดขึ้นลดความรุนแรง/ผลกระทบลงได้

ดังนั้น เพื่อให้แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ สป.พม. มีการบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพมากยิ่งขึ้น และไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ สามารถลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร และนำเทคโนโลยีสารสนเทศและการสื่อสารมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุดได้ กลุ่มตรวจสอบภายใน สป.พม. จึงมีข้อเสนอแนะในการดำเนินการ ดังนี้

1) มีการบริหารจัดการความเสี่ยงด้านการดำเนินโครงการอย่างมีประสิทธิภาพ มีแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการ เช่น เป้าหมายของโครงการ ทรัพยากรที่ใช้ ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน

2) จัดลำดับความสำคัญของโครงการให้ชัดเจน เพื่อตอบสนองยุทธศาสตร์ พม. และกำหนดขั้นตอน ขอบเขตหรือกำหนดกรอบแนวทางการบริหารจัดการโครงการ

3) ประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นในกรณีที่ไม่ได้ดำเนินโครงการ

4) การดำเนินโครงการมีการประชาสัมพันธ์เชิงรุก รวดเร็ว สม่ำเสมอ จัดหลักสูตรในการอบรมให้ตอบสนองต่อความต้องการของผู้รับบริการ และให้ได้รับทราบข่าวสารอย่างทั่วถึง

5) เพิ่มเติมปัจจัยเสี่ยงของความเสี่ยงด้านงบประมาณ กรณีมีการปรับลดวงเงินงบประมาณเพื่อให้งบประมาณที่ได้รับสอดคล้องกับสถานการณ์หรือภารกิจที่เปลี่ยนแปลงไป สามารถดำเนินโครงการต่อไปได้ภายในวงเงินงบประมาณที่ได้รับจัดสรร และเกิดประโยชน์แก่หน่วยงาน

6) ค้นหาหรือเพิ่มเติมปัจจัยเสี่ยงของความเสี่ยงด้านกลยุทธ์ที่เกิดจากภายในและภายนอกองค์กร ปัจจัยภายใน เช่น กระบวนการ วิธีการปฏิบัติงาน ความเพียงพอของข้อมูลและเทคโนโลยีสำหรับการให้บริการ เป็นต้น และปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายของรัฐบาล กระแสสังคม การเปลี่ยนแปลงทางเทคโนโลยี เศรษฐกิจ การเมือง เป็นต้น

7) ค้นหาจุดอ่อนหรือช่องว่างในกระบวนการปฏิบัติงานเพื่อจะได้นำมากำหนดปัจจัยเสี่ยงใหม่ๆ และแนวทางหรือวิธีการที่เหมาะสมในการบริหารจัดการความเสี่ยง สำหรับกรณีที่เป็นความเสี่ยงจากการทำงานในลักษณะคงที่ ถึงแม้ว่าจะไม่ก่อให้เกิดผลกระทบต่อการดำเนินงานก็ตาม ซึ่งอาจจะทำให้ค่าคะแนนการประเมินความเสี่ยงลดระดับลงได้

8) จัดการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้แก่บุคลากรทุกระดับ โดยมีการประเมินผลการเข้าอบรมด้วย

9) จัดการฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

10) มีแผนเพื่อเตรียมความพร้อมรับมือภัยคุกคามรูปแบบใหม่ๆ เช่น การโจมตีทางไซเบอร์ ที่อาจจะมีผลกระทบต่อระบบงานที่สำคัญ โดยกำหนดปัจจัยเสี่ยงให้เหมาะสม และสามารถควบคุมหรือจัดการกับปัจจัยเสี่ยงนั้นได้อย่างมีประสิทธิภาพ

11) มีการบริหารจัดการสิทธิ์การเข้าใช้งานในระบบเทคโนโลยีสารสนเทศของบุคลากร สป.พม. จะต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน การโอน ย้าย หรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องทราบถึงการเปลี่ยนแปลงสิทธิ์ดังกล่าว

ภาคผนวก

ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ ได้กำหนดให้ หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐดำเนินการ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานในสังกัด เป็นไปในทิศทางเดียวกัน กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ จึงเห็นควรกำหนดแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ว่าด้วยการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗”

ข้อ ๒ ประกาศนี้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

หน่วยงาน หมายความว่า หน่วยงานในสังกัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

/ สิทธิ์ของ ...

สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงานของรัฐนั้นๆ

(๓) กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

/ ข้อ ๕ ...

ข้อ ๕ นโยบายการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๖ นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และมีการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิ์ของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗ นโยบายการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

/ (๓) การควบคุม ...

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘ นโยบายการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

/ ข้อ ๙ ...

ข้อ ๙ นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย ที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๐ นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

/ (๓) การควบคุม ...

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๑ นโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๒ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อยดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๓ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ในกรณีระบบเทคโนโลยีสารสนเทศ

/ และการสื่อสาร ...

และการสื่อสารของหน่วยงานเกิดความเสียหาย หรือเป็นอันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตามแนวทางต่อไปนี้

(๑) ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

(๒) ผู้อำนวยการสำนัก/กอง/ศูนย์ หรือเทียบเท่า ที่รับผิดชอบการบริหารงานด้านสารสนเทศของหน่วยงาน มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยกำหนดมาตรการ และกำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานต้องจัดทำแนวปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวง

ข้อ ๑๕ หน่วยงานต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๗ พฤศจิกายน พ.ศ. ๒๕๕๗

(นายวิเชียร ชวลิต)

ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

เรื่องที่ 11

ข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้หน่วยงานมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจจะเกิดขึ้น ทำให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน โดยการตรวจสอบและประเมินความเสี่ยงนั้น จะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **คณะทำงาน** หมายถึง คณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการจัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สป.พม.
3. **ผู้รับการตรวจประเมิน** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
4. **ผู้ตรวจสอบภายในหน่วยงานของรัฐ** (Internal Auditor) หมายถึง เจ้าหน้าที่ของกลุ่มตรวจสอบภายใน สป.พม. ที่ได้รับมอบหมาย

ข้อปฏิบัติ

1. การดำเนินงาน

1.1 แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการจัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สป.พม. ประกอบด้วยกลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธาน

1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ

1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน และเตรียมความพร้อมเพื่อรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ สป.พม.

1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผน

1.6 ทบทวน/ปรับปรุงแผน ปีละ 1 ครั้ง

2. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ สป.พม. ปีละ 1 ครั้ง โดยดำเนินการให้สอดคล้องตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

2.2 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ สป.พม. ให้ดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor)

2.3 กำหนดขอบเขตและขั้นตอนปฏิบัติสำหรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ สป.พม.

2.4 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ สป.พม. ที่มีความสำคัญหรือเป็นข้อมูลส่วนบุคคล มีข้อจำกัด ดังนี้

2.4.1 ผู้ตรวจสอบภายในหน่วยงานของรัฐ สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบในลักษณะที่อ่านได้เพียงอย่างเดียว

2.4.2 ในกรณีที่ผู้ตรวจสอบภายในหน่วยงานของรัฐจำเป็นต้องเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้ จะต้องดำเนินการด้วยวิธีการที่ปลอดภัย

2.4.3 มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบภายในหน่วยงานของรัฐทำงานบนข้อมูลสำเนา

2.4.4 มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

2.4.5 มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

2.5 ผู้ตรวจสอบภายในหน่วยงานของรัฐ สรุปรายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของ สป.พม. เสนอต่อ ปพม. และ ศทส. เพื่อรับทราบ

2.6 ทบทวน/ปรับปรุงการดำเนินงานตามที่ผู้ตรวจสอบภายในหน่วยงานของรัฐให้ข้อเสนอแนะต่อไป

คำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ที่ ๙๙ /๒๕๖๕

เรื่อง แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ว่าด้วยการจัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ตามประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗ ประกาศใช้เมื่อวันที่ ๗ พฤศจิกายน ๒๕๕๗ ข้อ ๑๑ และข้อ ๑๒ กำหนดให้หน่วยงานต้องมีการจัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบกับข้อปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ และข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) กำหนดให้มีการแต่งตั้งคณะทำงาน เพื่อเป็นกลไกในการขับเคลื่อนการทำงาน ให้เป็นไปด้วยความเรียบร้อยและบรรลุตามวัตถุประสงค์ จึงมีคำสั่งดังต่อไปนี้

๑. ให้ยกเลิกคำสั่ง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๑๐/๒๕๖๔ เรื่อง แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศว่าด้วยการจัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๒. แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ว่าด้วยการจัดทำระบบสำรองข้อมูลและสารสนเทศ และการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ โดยมีองค์ประกอบ และอำนาจหน้าที่ ดังต่อไปนี้

๒.๑ องค์ประกอบ

๒.๑.๑ นางสุดา สุหลง ประธาน
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๑.๒ นายพูนพัฒน์ ขันธาโรจน์ คณะทำงาน
ผู้อำนวยการกลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร

๒.๑.๓ นางสาวทัศวรรณ จันทร์อ่อน คณะทำงาน
รักษาการผู้อำนวยการกลุ่มการพัฒนาระบบสารสนเทศ

/๒.๑.๔ นาง...

๒.๑.๔ นางสปัณณ์ภักค์ วัฒนพิพัฒน์กุล คณะทำงาน
ผู้อำนวยการกลุ่มการวิเคราะห์ข้อมูล

๒.๑.๕ จ่าสิบเอกฤทธิเดช แสงแจ่ม คณะทำงาน
นักวิชาการคอมพิวเตอร์ชำนาญการ

๒.๑.๖ นายจำเริญ นิจจรัลกุล คณะทำงาน
เจ้าพนักงานสื่อสารชำนาญงาน

๒.๑.๗ นางสาวสุกัญญา ฉัตรกระโทก คณะทำงาน
นักพัฒนาสังคมปฏิบัติการ

๒.๑.๘ นางกฤติกา พันธ์รัตน์กุล คณะทำงาน
นักวิเคราะห์นโยบายและแผนชำนาญการ และเลขานุการ

๒.๑.๙ นางสาวสมอุษา วิไลพันธุ์ คณะทำงาน
นักวิเคราะห์นโยบายและแผนชำนาญการ และผู้ช่วยเลขานุการ

๒.๒ อำนาจหน้าที่

๒.๒.๑ จัดทำ/ทบทวนแผน ดังต่อไปนี้

(๑) แผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม.

(๒) แผนเตรียมความพร้อมกรณีฉุกเฉิน สป.พม.

(๓) แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.

๒.๒.๒ มอบหมายเจ้าหน้าที่ปฏิบัติงานตามแผน

๒.๒.๓ ติดตาม และประเมินผลการดำเนินงานตามแผน

๒.๒.๔ ดำเนินการในส่วนที่เกี่ยวข้องภายใต้ข้อปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ และข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ สป.พม.

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒ พฤศจิกายน พ.ศ. ๒๕๖๕

(นางสุดา สุหลง)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

บันทึกข้อความ

ส่วนราชการ กลุ่มตรวจสอบภายใน สำนักงานปลัดกระทรวง ฯ โทร. ๐ ๒๒๐๒ ๙๐๖๑
ที่ พม ๐๒๒๓/ ๙๙๖ **วันที่** ๒๙ กันยายน ๒๕๖๕
เรื่อง รายงานผลการสอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

เรียน ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๑. เรื่องเดิม

ตามแผนการตรวจสอบ ประจำปีงบประมาณ พ.ศ.๒๕๖๕ ของกลุ่มตรวจสอบภายใน กำหนดให้กลุ่มตรวจสอบภายในดำเนินการสอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ปีงบประมาณ พ.ศ. ๒๕๖๕ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร นั้น

๒. ข้อเท็จจริง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ได้ส่งแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๕ เพื่อให้กลุ่มตรวจสอบภายในสอบทานและประเมินความเสี่ยงของแผนฯ ดังกล่าว ตามหนังสือ ที่ พม ๐๒๑๐/๓๑๒ ลงวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๕

๓. ข้อพิจารณา

กลุ่มตรวจสอบภายใน ได้พิจารณาและสอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ปีงบประมาณ พ.ศ. ๒๕๖๕ โดยทำการวิเคราะห์ ประเมินความเสี่ยง ทบทวนข้อมูลผลการดำเนินงาน ความเพียงพอ ความเชื่อถือได้ของการบริหารจัดการความเสี่ยง จากการสอบทาน พบว่ามีการดำเนินการตามแผนฯ ต่อเนื่องจากปีงบประมาณ พ.ศ.๒๕๖๔ ซึ่งมีปัจจัยเสี่ยงทั้งสิ้น ๓๒ ปัจจัยเสี่ยง และมีค่าคะแนนการประเมินความเสี่ยงตามรายปัจจัยเสี่ยง คงเดิมจำนวน ๒๙ ปัจจัยเสี่ยง สำหรับ ๓ ปัจจัยเสี่ยงที่เดิมมีค่าคะแนนอยู่ในระดับความเสี่ยงตามเกณฑ์การประเมินค่อนข้างสูง คือ มีค่าคะแนนเท่ากับ ๘ และ ๙ ซึ่งเป็นระดับที่ไม่สามารถยอมรับได้ โดย ศทส.ได้ดำเนินการจัดการความเสี่ยงปรับปรุงค่าคะแนนให้ลดลง เท่ากับ ๖ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ปัจจัยเสี่ยงดังกล่าว ได้แก่

๑. ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามคำรับรองการปฏิบัติราชการ

๒. ถูกตัด/ปรับลดโครงการที่วางแผนไว้ และโครงการที่จำเป็นต้องดำเนินการ ถูกตัดตามนโยบายการปรับลดงบประมาณของ สป.พม.

๓.การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่าง ๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด

สำหรับปัจจัยเสี่ยงอื่นๆปรากฏตามรายงานผลการสอบทานที่แนบ และเพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๕ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้นและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิด

ประโยชน์...

ประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการตามข้อเสนอแนะในรายงานผลการสอบทานฯ ที่แนบมาพร้อมนี้

๔. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดลงนามในแบบรายงานสรุปสำหรับผู้บริหารในรายงานผลการสอบทานฯที่แนบมาพร้อมนี้ด้วยแล้ว

(นางสาวมีนรดา ค้าสม)
ผู้ตรวจสอบภายในกระทรวง

- เห็นชอบตามข้อ ๓.
- ลงนามแล้ว

(นางพัชรี อาระยะกุล)
ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๓๐ ก.ย. ๒๕๖๕

ที่ พม ๐๒๒๓/ ๑๐๕๖

เรียน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

กลุ่มตรวจสอบภายใน ขอส่งรายงานผลการสอบทานแผนการจัดการความเสี่ยงฯ ของ ศทส. สป.พม. ประจำปีงบประมาณ พ.ศ.๒๕๖๕ ตามหนังสือ ที่ พม ๐๒๒๓/๙๘๖ ลงวันที่ ๒๘ กันยายน ๒๕๖๕ มาเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางสาวมีนรดา ค้าสม)
ผู้ตรวจสอบภายในกระทรวง
- 6 ต.ค. 2565

รายงานสรุปสำหรับผู้บริหาร
การสอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
ปีงบประมาณ พ.ศ. ๒๕๖๕

๑. ความเป็นมา

ตามแผนการตรวจสอบ ประจำปีงบประมาณ พ.ศ.๒๕๖๕ กำหนดให้กลุ่มตรวจสอบภายใน สอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ.๒๕๖๕

๒. วัตถุประสงค์ของการตรวจสอบ

๑. เพื่อสอบทานความเชื่อถือได้ และถูกต้องของข้อมูลของการจัดทำแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ว่าเป็นไปตามมาตรฐาน

๒.เพื่อประเมินความมีประสิทธิภาพ ประสิทธิผลของแผนการจัดการความเสี่ยง

๓. เพื่อประเมินว่ามีการปฏิบัติตามยุทธศาสตร์ นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๔. เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบฐานข้อมูล ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์

๕. เพื่อประเมินความเพียงพอของระบบควบคุมภายใน ด้านเทคโนโลยีสารสนเทศ และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๖. เพื่อให้มั่นใจว่าการบริหารจัดการความเสี่ยง สามารถดำเนินการได้ตามแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.ให้อยู่ในระดับที่ยอมรับได้

๓. ขอบเขตการสอบทานแผนบริหารความเสี่ยง

๑. สอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปี ๒๕๖๕ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ประเมินความเสี่ยงตามแผนการจัดการความเสี่ยงฯ ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคารที่ทำการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เลขที่ ๑๐๓๔ ถนนกรุงเกษม แขวงมหานาค เขตป้อมปราบศัตรูพ่าย กรุงเทพมหานคร

๔. ระยะเวลาของการสอบทาน

ระหว่างวันที่ ๗ - ๙ กันยายน ๒๕๖๕

๕. วิธีการประเมินผลการบริหารความเสี่ยง

๑. ศึกษากฎหมายและระเบียบที่เกี่ยวข้องกับแผนการจัดการความเสี่ยง

๒. ประเมินผลการบริหารจัดการความเสี่ยงที่ได้ดำเนินการว่าสามารถบรรลุเป้าหมายตามภารกิจหลัก

๓. สอบทานความเพียงพอ ความเชื่อถือได้ของการจัดทำแผนการจัดการความเสี่ยงของกิจกรรมที่ประเมินในปีปัจจุบัน

๔. วิเคราะห์ทบทวนข้อมูล ผลการดำเนินงานตามแผนการจัดการความเสี่ยงว่าสามารถทำให้ความเสี่ยงที่ยังคงเหลืออยู่นั้นลดลงหรืออยู่ในระดับที่ยอมรับได้

๕. รายงานผลการสอบทาน ความเพียงพอ ความเชื่อถือได้ของการจัดทำแผนการจัดการความเสี่ยง

รายละเอียด...

รายละเอียดวิธีการประเมินผลแผนการจัดการความเสี่ยงฯ

๑.ทบทวนเอกสาร (Documentation review)

โดยการรวบรวมและตรวจสอบความเป็นปัจจุบัน ข้อบกพร่องที่สามารถนำไปสู่ความผิดพลาด หรือความไม่เหมาะสม ในการควบคุมความมั่นคงปลอดภัยของสารสนเทศ ดังต่อไปนี้

๑) แนวนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศ

๒) การออกแบบระบบเครือข่ายคอมพิวเตอร์

๓) ขั้นตอนการปฏิบัติงานในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์

๔) แผนการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศและระบบเครือข่ายคอมพิวเตอร์

๕) ข้อตกลงหรือสัญญาที่เกี่ยวข้องกับการบำรุงรักษา หรือการเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์

๖) แผนการตอบสนองต่อภัยคุกคามทางระบบเครือข่ายคอมพิวเตอร์ (Incident response plan)

๒. การสัมภาษณ์ (Interview)

จัดทำข้อคำถามเพื่อสอบถามเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศที่เคยเกิดขึ้นในอดีต ผลกระทบที่เคยได้รับ ความถี่ในการเกิดเหตุการณ์ ความสูญเสีย และข้อกังวลเกี่ยวกับความเสี่ยงของระบบ และองค์ประกอบของระบบที่อาจเกิดขึ้นในอนาคต เพื่อใช้สัมภาษณ์ผู้ที่เกี่ยวข้อง ได้แก่

๑) เจ้าของระบบงาน (System owner)

๒) ผู้พัฒนาระบบงาน (System Developer)

๓) ผู้ดูแลระบบงาน (System custodian)

๔) ผู้ใช้งาน (User)

๓. การสังเกตการณ์ (Observation)

๑) สังเกตความเสี่ยงในขั้นตอนการปฏิบัติงานของเจ้าหน้าที่ในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์

๒) สังเกตความเสี่ยงในสภาพแวดล้อมทางกายภาพ ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคารที่ทำการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เลขที่ ๑๐๓๔ ถนนกรุงเกษม แขวงมหานาค เขตป้อมปราบศัตรูพ่าย กรุงเทพมหานคร และห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ (ห้อง Server) ชั้น ๘ อาคารที่ทำการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ผลการสอบทานแผนการจัดการความเสี่ยง

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ.๒๕๖๕ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการดำเนินการอย่างต่อเนื่องจากปีงบประมาณที่ผ่านมา โดยที่แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ.๒๕๖๕ ได้นำข้อเสนอแนะจากกลุ่มตรวจสอบภายใน สป.พม. เป็นแนวทางในการดำเนินงาน วิเคราะห์ ประเมินความเสี่ยง ทบทวนข้อมูลผลการดำเนินการ ความเพียงพอ ความเชื่อถือได้ของแผนฯดังกล่าว เพื่อลดความเสี่ยงในการปฏิบัติงานให้มากยิ่งขึ้น

จากการประเมินแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ.๒๕๖๕ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พบว่ามีปัจจัยเสี่ยงคงเดิมทั้งสิ้น ๓๒ ปัจจัยเสี่ยง ไม่มีความเสี่ยงและปัจจัยเสี่ยงใหม่ แต่เพิ่มมาตรการจัดการความเสี่ยงและแนวทางการควบคุมความเสี่ยงให้อยู่ในระดับคะแนนที่ยอมรับได้ มีค่าคะแนนการประเมินความเสี่ยงตามรายปัจจัยเสี่ยงคงเดิม จำนวน ๒๙ ปัจจัยเสี่ยง สำหรับ ๓ ปัจจัยเสี่ยง ที่เดิมมีค่าคะแนนอยู่ในระดับความเสี่ยงตามเกณฑ์

การประเมินค่อนข้างสูง คือ มีค่าคะแนนเท่ากับ ๘ และ ๙ ซึ่งเป็นระดับที่ไม่สามารถยอมรับได้ โดย ศทส.ได้ดำเนินการจัดการความเสี่ยง และเพิ่มเติมแนวทางการควบคุมความเสี่ยง ปรับปรุงค่าคะแนนให้ลดลง เท่ากับ ๖ ทุกปัจจัยเสี่ยง ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ปัจจัยเสี่ยงดังกล่าว ได้แก่

๑. ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามคำรับรองการปฏิบัติราชการ

๒. ถูกตัด/ปรับลดโครงการที่วางแผนไว้ และโครงการที่จำเป็นต้องดำเนินการ ถูกตัดตามนโยบายการปรับลดงบประมาณของ สป.พม.

๓.การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับดำเนินโครงการต่าง ๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด

สรุปเป็นตารางได้ดังนี้

1. ตารางแสดง**การปรับลดค่าคะแนน**การประเมินความเสี่ยง ๓ ปัจจัยเสี่ยง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๑.	ด้านบุคลากร	๐๒๙	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามคำรับรองการปฏิบัติราชการ	๒ (เดิม ๒)	๓ (เดิม ๔)	๖ (เดิม ๘)	จัดการความเสี่ยง	- บรรจุโครงการในลักษณะที่เป็นโครงการสำคัญตามยุทธศาสตร์สอดคล้องตามภารกิจของ สป.พม. - บรรจุในแผนปฏิบัติการของ ศทส. และ สป.พม. - มีแนวทางในการสื่อสาร เชิญผู้เชี่ยวชาญหรือผู้ทรงคุณวุฒิถ่ายทอดองค์ความรู้ให้ผู้บริหารเข้าใจถึงประโยชน์อย่างเป็นรูปธรรม มีการใช้ทรัพยากรร่วมกันอย่างมีประสิทธิภาพ
๒.	ด้านกลยุทธ์	๐๓๐	-ถูกตัด/ปรับลดโครงการที่วางแผนไว้ ตามนโยบายการปรับลดงบประมาณของ สป.พม. - โครงการที่จำเป็นต้องดำเนินการถูกตัดตามนโยบายการปรับลดงบประมาณของ สป.พม.	๒ (เดิม ๓)	๓ (เดิม ๓)	๖ (เดิม ๙)	จัดการความเสี่ยง	- จัดลำดับความสำคัญของโครงการให้อยู่ในลำดับต้นๆที่จำเป็นต้องดำเนินงาน -ต้องมีการจัดทำความเสี่ยงแนบไปกับโครงการ และให้มีการถ่วงน้ำหนักของโครงการที่เป็นโครงการประเภทเดียวกัน -ชี้แจงผลกระทบที่ไม่ได้ดำเนินโครงการและยอมรับความเสี่ยง
๓.	ด้านงบประมาณ	๐๓๑	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่าง ๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่	๒ (เดิม ๓)	๓ (เดิม ๓)	๖ (เดิม ๙)	จัดการความเสี่ยง	-ปรับโครงการโดยจัดลำดับความสำคัญใหม่ลดขอบเขตงานลง -ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ
			จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด					

จะเห็นได้ว่า เมื่อปรับค่าคะแนนการประเมินความเสี่ยงลง และเพิ่มแนวทางการควบคุมความเสี่ยง ระดับคะแนนจะอยู่ในระดับความเสี่ยงค่อนข้างต่ำ ตามเกณฑ์การประเมิน ดังนี้

คะแนน	ระดับความเสี่ยง	คำอธิบาย
๑๕ – ๒๕	สูง	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
๘ – ๑๔	ค่อนข้างสูง	ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
๔ – ๗	ค่อนข้างต่ำ	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
๑ – ๓	ต่ำ	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ซึ่งจะต้องดำเนินการตามแนวทางการควบคุมความเสี่ยงของแต่ละปัจจัยเสี่ยงต่อไป เพื่อป้องกันมิให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้

สำหรับปัจจัยเสี่ยงอื่นที่มีค่าคะแนนการประเมินความเสี่ยงตามรายปัจจัยเสี่ยงคงเดิม จำนวน ๒๙ ปัจจัยเสี่ยง เป็นการคงค่าคะแนนในกิจกรรมที่ไม่สามารถลดค่าคะแนนลงได้ เนื่องจากเป็นความเสี่ยงจากการทำงานในลักษณะคงที่ จึงไม่ก่อให้เกิดปัจจัยเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงานและในบางปัจจัยเสี่ยงมีการเพิ่มเติมหรือปรับเปลี่ยนแนวทางการควบคุมความเสี่ยง สรุปเป็นตารางได้ ดังนี้

2. ตารางแสดง**ค่าคะแนน**การประเมินความเสี่ยงคงที่ จำนวน ๒๙ ปัจจัยเสี่ยง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๑.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๐๑	ไฟไหม้ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)	๑	๕	๕	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติเป็นการจ้างบริษัทดำเนินการบำรุงรักษา เนื่องจากมีความเชี่ยวชาญเฉพาะด้าน
๒.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๐๒	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	๑	๓	๓	ควบคุมความเสี่ยง	ตรวจสอบระบบสำรองไฟฟ้า (UPS) /แบตเตอรี่สำรองไฟ
๓.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๐๓	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	๑	๓	๓	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณภูมิ/ความชื้น มีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้น ผ่านระบบควบคุมอย่างสม่ำเสมอ
๔.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๐๔	ไม่มีการกำหนดสิทธิ์และไม่ควบคุมการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	๑	๓	๓	ควบคุมความเสี่ยง	-บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการ ในเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง -มีระบบกลอนประตูไฟฟ้าและระบบสแกนลายนิ้วมือเข้าออกทุกครั้ง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการ	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๕.	การรักษา ความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๐๕	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕	ควบคุมความเสี่ยง	-จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (IT Contingency Plan) -จัดทำระบบการสำรองข้อมูลและสารสนเทศ -จัดทำแผน/ใช้แผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ของ สป.พม.
๖.	การควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร	๐๖	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	๑	๓	๓	ควบคุมความเสี่ยง	-จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ -จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ศทส.
๗.	การควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร	๐๗	ขาดแผนรองรับระบบฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	๑	๓	๓	ควบคุมความเสี่ยง	-มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ -มีการประชุมติดตามและสรุปผลการปฏิบัติงานทุกเดือน -จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ -ทดสอบการโจมตีตามแผนที่กำหนดจริง
๘.	การควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร	๐๘	การบริหารจัดการสิทธิ์ การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆระดับผู้ใช้งาน ขาดประสิทธิภาพ	๑	๓	๓	ควบคุมความเสี่ยง	-มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน-ผู้ดูแลระบบ/admin -มีการทบทวนสิทธิ์เป็นประจำทุก ๖ เดือน โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข
๙.	การควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร	๐๙	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	๑	๓	๓	ควบคุมความเสี่ยง	-ระบุข้อกำหนด/ข้อตกลง ระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย -มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก -มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล -มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก -มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบหรือ ผอ.ศทส.ทุกครั้งที่ระบบขัดข้องเพื่อให้แก้ปัญหาได้ทันท่วงที
๑๐.	การควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร	๐๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	๓	๓	ควบคุมความเสี่ยง	-ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่โดยมีระบบพิสูจน์และยืนยันตัวบุคคล -มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา -มีการปรับเพิ่มประสิทธิภาพ การบริหารจัดการทุก ๆ ปี

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการ	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)×(๒)		
๑๑.	การควบคุมเทคโนโลยีสารสนเทศและการสื่อสาร	๐๑๑	-ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๒	๓	๖	ควบคุมความเสี่ยง	-มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall -ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ -บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ -ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ -ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ -เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ -ติดตามและรายงานผลทุก ๓ เดือน
๑๒.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๒	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) ตัวอย่าง ที่เกิดขึ้นจริงจากการดำเนินงาน เช่น มีการเจาะระบบของเว็บไซต์ของ สนง.พมจ.	๑	๔	๔	ควบคุมความเสี่ยง	-ติดตั้งโปรแกรมป้องกันไวรัสและ Patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อับเดท -ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ -เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทุก ๖ เดือน -มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ -ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ -จัดทำการสำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง
๑๓.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๓	ไม่มีการดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลของข้อมูลและระบบฐานข้อมูลครบถ้วน	๑	๕	๕	ควบคุมความเสี่ยง	-จัดทำการสำรองข้อมูลแบบอัตโนมัติโดยจัดเก็บ Storage ทุกวัน เฉพาะส่วนที่เพิ่มในแต่ละวัน และจัดเก็บข้อมูลทั้งระบบแบบ Full Backup บน Storage สัปดาห์ละ ๑ ครั้ง -จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติโดยจัดเก็บใน Hard Disk เป็นประจำทุกเดือน -มีการทดสอบการกู้คืนข้อมูลของทุกระบบงาน อย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการเตรียมความพร้อมหากเกิดสถานการณ์ฉุกเฉิน -มีการควบคุมกำกับการสำรองข้อมูลให้เป็นไปตามแผนพร้อมทั้งการตรวจสอบความสมบูรณ์ในการสำรองข้อมูลทุกครั้ง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการ	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๑๔.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๔	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๕	๕	ควบคุมความเสี่ยง	-มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง อธิบายเพิ่มเติม VPN (Virtual Private Network) ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้
๑๕.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๕	การกำหนดมาตรฐานในการพัฒนาซอฟแวร์	๑	๓	๓	ควบคุมความเสี่ยง	-จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ -ระบุมาตรฐานการพัฒนาซอฟต์แวร์ และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR -ควบคุม ติดตามทุกขั้นตอนการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐานและ TOR
๑๖.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๖	เกิดช่องโหว่ของซอฟต์แวร์	๒	๓	๖	ควบคุมความเสี่ยง	-ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ -Update Software ระบบต่างๆ อย่างสม่ำเสมอ -ติดตามข่าวสารด้านความมั่นคงฯ ปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง
๑๗.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๗	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	๑	๕	๕	ควบคุมความเสี่ยง	-ทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง เพื่อปิดช่องโหว่จากการอัพเดทเวอร์ชั่นใหม่ๆ อย่างสม่ำเสมอ ทำให้สามารถใช้ระบบได้อย่างต่อเนื่องและใช้ในเวลาที่ต้องการได้
๑๘.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๘	การนำเข้าข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	๑	๓	๓	ควบคุมความเสี่ยง	มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูลให้เป็นไปตามธรรมาภิบาล ข้อมูลภาครัฐ (Data Governance)
๑๙.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๑๙	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	๑	๓	๓	ควบคุมความเสี่ยง	ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่อง และรายงานให้ผู้บริหารทราบ
๒๐.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๒๐	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	๑	๒	๒	ควบคุมความเสี่ยง	-มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลางกระทรวง พม. อย่างต่อเนื่อง -มีการติดตามการนำมาตรฐานข้อมูลกลางกระทรวง พม. ไปใช้อย่างสม่ำเสมอ -มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) -มีการดำเนินงานทบทวน/ปรับปรุงและเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลางกระทรวง พม. ที่ครอบคลุมภารกิจของกระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุมที่เพิ่มขึ้น
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
								-มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ ได้แก่ ระบบบริหารสำนักงาน (Back Office) ระบบฐานข้อมูลกลางผู้รับสวัสดิการจาก พม. (DB Center) ระบบแลกเปลี่ยนข้อมูลกลาง การจัดสวัสดิการของกระทรวง (MSO Linkage) และระบบให้ความช่วยเหลือผู้ประสบปัญหาทางสังคม (MSO welfare)
๒๑.	ด้านระบบสารสนเทศและฐานข้อมูล	๐๒๑	ไม่มีบัญชีการเข้าถึงระบบปฏิบัติงาน (Operating System) และโปรแกรมประยุกต์ (Applications)	๑	๓	๓	ควบคุมความเสี่ยง	-มีการกำหนดสิทธิ์ในการเข้าถึงเพื่อทำการจำกัดและควบคุมการเข้าถึง -ใช้งานโปรแกรมเพื่อป้องกันการละเมิดโดยการตรวจสอบสิทธิ์ -มีการทบทวนสิทธิ์เป็นประจำโดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข -มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ ทุก 6 เดือน -ปฏิบัติตามข้อปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.อย่างเคร่งครัด
๒๒.	ด้านโปรแกรมคอมพิวเตอร์	๐๒๒	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) หมายเหตุ Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดร์เรียกง่ายๆ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์ เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น	๑	๓	๓	ควบคุมความเสี่ยง	-สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง ตามกฎหมาย -กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำ และส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ -จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย
๒๓.	ด้านโปรแกรมคอมพิวเตอร์	๐๒๓	ขาดการป้องกันหรือตรวจจับไวรัส	๑	๕	๕	ควบคุมความเสี่ยง	-จัดหาและติดตั้งโปรแกรมป้องกันไวรัส -Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ
๒๔	ด้านโปรแกรมคอมพิวเตอร์	๐๒๔	ผู้บริหารไม่ให้ความสำคัญต่อความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร	๑	๓	๓	ควบคุมความเสี่ยง	-มีแนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ -มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร -มีแนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ -รายงานผู้บริหารอย่างสม่ำเสมอ
								เพื่อรับทราบและความสำคัญในการจัดการความเสี่ยง เนื่องจากจำเป็นต้องทำไม่ทำไม่ได้
๒๕	ด้านบุคลากร	๐๒๕	ผู้รับผิดชอบที่ได้รับมอบหมายไม่ทำการติดตามตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศ	๑	๓	๓	ควบคุมความเสี่ยง	-ปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม. (แบบฟอร์มการขอใช้งานบัญชีผู้ใช้งาน การจัดเก็บ Log) -ปฏิบัติตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารว่าด้วยหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ -รายงานผลการติดตามตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศ

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุมที่เพิ่มขึ้น
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๒๖.	ด้านบุคลากร	๐๒๖	การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓	ควบคุมความเสี่ยง	-มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) -มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน -มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจน และควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้
๒๗.	ด้านบุคลากร	๐๒๗	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	๒	๒	๔	ควบคุมความเสี่ยง	-อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที -มีการจ้าง บุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน -มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง
๒๘.	ด้านบุคลากร	๐๒๘	ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๑	๓	๓	ควบคุมความเสี่ยง	-อบรมการใช้งานระบบงาน -จัดทำคู่มือสำหรับปฏิบัติงาน -มีระบบ Call Center สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ -จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุง หรือตามความต้องการของ User
๒๙.	ด้านการบริหารจัดการ	๐๓๒	กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน -อนุมัติโครงการล่าช้า -ไม่สามารถประกาศผลผู้ชนะการประกวดราคา -สัญญาไม่ตรงตามร่างข้อกำหนด -ไม่มีผู้เข้าประกวดราคาได้ทันเวลา	๑	๓	๓	ควบคุมความเสี่ยง	-จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด -ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญ/ความเร่งด่วน -ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง -จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด

จากตารางจะเห็นได้ว่าปัจจัยเสี่ยงในลำดับที่ ๑ ๕ ๑๑ ๑๒ ๑๓ ๑๔ ๑๖ ๑๗ ๒๓ และ ๒๗ มีค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ – ๗ ซึ่งอยู่ในระดับความเสี่ยงค่อนข้างต่ำ เป็นการคงค่าคะแนนในกิจกรรมที่ไม่สามารถลดค่าคะแนนลงได้ เนื่องจากเป็นความเสี่ยงจากการทำงานในลักษณะคงที่ ซึ่งไม่ก่อให้เกิดปัจจัยเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงานและในบางปัจจัยเสี่ยงมีการเพิ่มเติมหรือปรับเปลี่ยนแนวทางการควบคุมความเสี่ยง เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะต้องดำเนินการตามแนวทางการควบคุมความเสี่ยงอย่างต่อเนื่อง

ข้อเสนอแนะ

เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๕ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้นและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.ดำเนินการดังนี้

๑. มีการบริหารจัดการความเสี่ยงด้านการดำเนินโครงการอย่างมีประสิทธิภาพ มีแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการ เช่น เป้าหมายของโครงการ ทรัพยากรที่ใช้ ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน

๒. จัดระดับความสำคัญของโครงการให้ชัดเจน เพื่อตอบสนองยุทธศาสตร์ พม.และกำหนดขั้นตอน ขอบเขตหรือกำหนดกรอบแนวทางการบริหารจัดการโครงการ

๓. ประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ ประเมินความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้น กรณีไม่ได้ดำเนินโครงการ

๔. การดำเนินโครงการมีการประชาสัมพันธ์เชิงรุก รวดเร็ว สม่ำเสมอ จัดหลักสูตรในการอบรมให้ตอบสนองต่อความต้องการของผู้รับบริการ และให้ได้รับทราบข่าวสารอย่างทั่วถึง

๕. เพิ่มเติมปัจจัยเสี่ยงของกิจกรรมด้านงบประมาณ กรณีมีการปรับลดวงเงินงบประมาณเพื่อให้งบประมาณที่ได้รับสอดคล้องกับสถานการณ์หรือภารกิจที่เปลี่ยนแปลงไป สามารถดำเนินโครงการต่อไปได้ภายในวงเงินงบประมาณที่ได้รับจัดสรร เกิดประโยชน์แก่หน่วยงาน

๖. ค้นหาหรือเพิ่มเติมปัจจัยเสี่ยงด้านกลยุทธ์ที่เกิดจากภายในและภายนอกองค์กร ปัจจัยภายใน เช่น กระบวนการ วิธีการปฏิบัติงาน ความเพียงพอของข้อมูลและเทคโนโลยีสำหรับการให้บริการ เป็นต้น ปัจจัยภายนอก เช่น การเปลี่ยนแปลงนโยบายของรัฐบาล กระแสสังคม การเปลี่ยนแปลงทางเทคโนโลยี เศรษฐกิจ การเมือง เป็นต้น

๗. ค้นหาจุดอ่อนหรือช่องว่างในกระบวนการปฏิบัติงานเพื่อจะได้นำมากำหนดปัจจัยเสี่ยงใหม่ๆ และแนวทางหรือวิธีการที่เหมาะสมในการบริหารจัดการความเสี่ยง สำหรับกรณีที่เป็นความเสี่ยงจากการทำงานในลักษณะคงที่ ถึงแม้ว่าจะไม่ก่อให้เกิดผลกระทบต่อการดำเนินงานก็ตาม ซึ่งอาจจะทำให้ค่าคะแนนการประเมินความเสี่ยงลดระดับลงได้

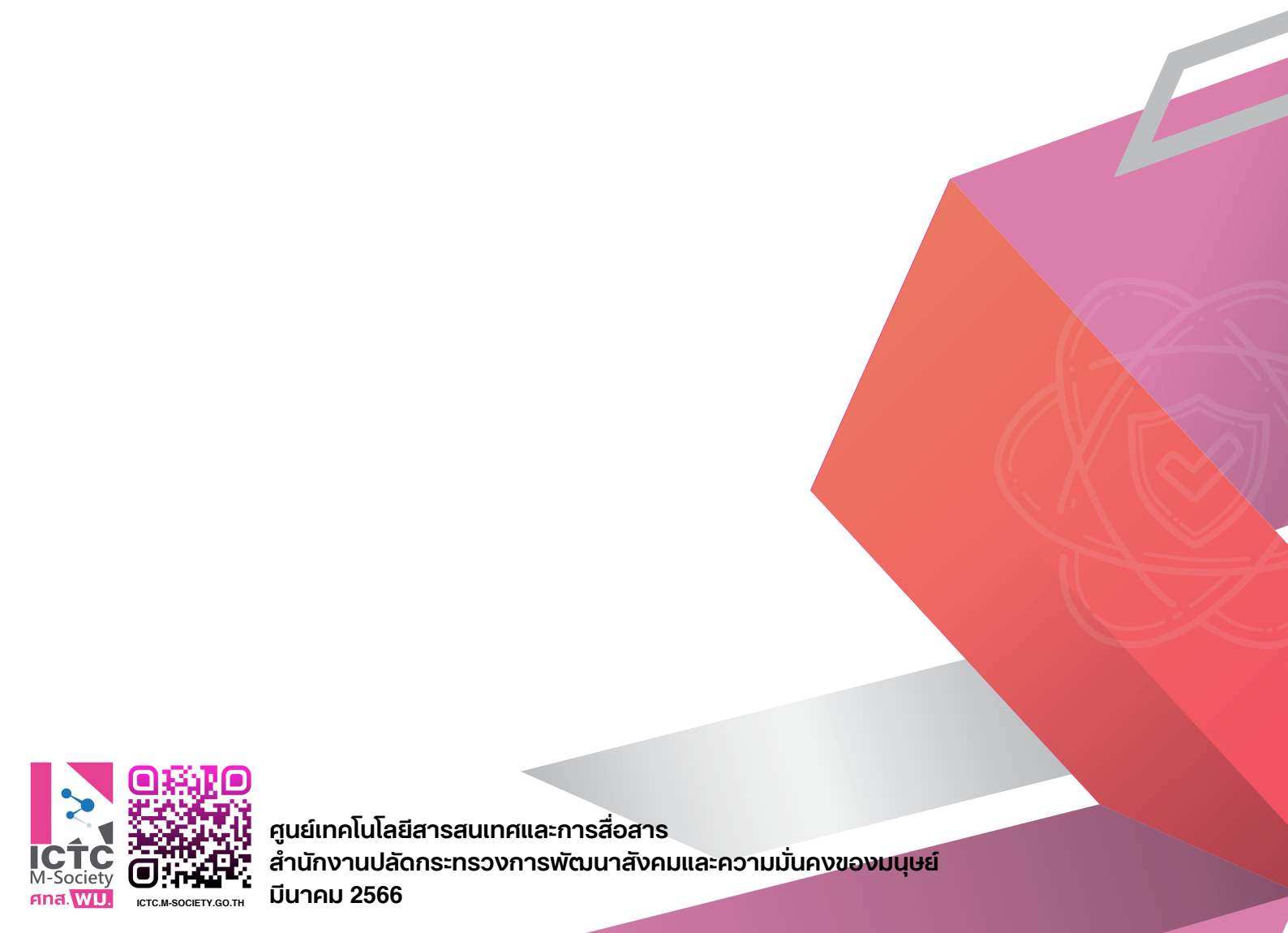
๘.จัดการอบรมและพัฒนาความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ให้แก่บุคลากรทุกระดับ โดยมีการประเมินผลการเข้าอบรมด้วย

๙.จัดการฝึกอบรมบุคลากรที่เกี่ยวข้องกับงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑๐. มีแผนเพื่อเตรียมความพร้อมรับมือภัยคุกคามรูปแบบใหม่ ๆ เช่น การโจมตีทางไซเบอร์ที่อาจจะมีผลกระทบต่อระบบงานที่สำคัญ โดยกำหนดปัจจัยเสี่ยงให้เหมาะสม และสามารถควบคุมหรือจัดการกับปัจจัยเสี่ยงนั้นได้อย่างมีประสิทธิภาพ

๑๑. มีการบริหารจัดการสิทธิ์การเข้าใช้งานในระบบเทคโนโลยีสารสนเทศของบุคลากร สป.พม. จะต้องปรับปรุงให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน การโอน ย้าย หรือสิ้นสุดการจ้างงาน รวมทั้งต้องมีการสื่อสารให้ผู้เกี่ยวข้องทราบถึงการเปลี่ยนแปลงสิทธิ์ ดังกล่าว

คำสั่งผู้บริหาร	ผู้สอบทานและรายงาน
ลงชื่อ.....	ลงชื่อ.....
(นางพัชรี อาระยะกุล)	(นางสาวมีนรดา ค้าสม)
ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์	ผู้ตรวจสอบภายในกระทรวง



ICTC.M-SOCIETY.GO.TH

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
มีนาคม 2566