แผนบริหารจัดการ ความเสี่ยง

ด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

RISK:2567

เกณฑ์การประเมินความเสี่ยง

- ระดับความเสี่ยงสูง
- ระดับความเสี่ยงค่อนข้างสูง
- ระดับความเสี่ยงค่อนข้างต่ำ
- ระดับความเสี่ยงต่ำ

ศทส. สป.พม.
มิถุนายน 2567

สารบัญ

สารบัญ (ต่อ)

เรื่อง **หน้า**

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปีงบประมาณ พ.ศ. 2567 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ โดยให้ความสำคัญในการบริหารจัดการความเสี่ยง เป็นเครื่องมือสำคัญตามหลักการกำกับดูแลกิจการที่ดีช่วยในการบริหารและการตัดสินใจ การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายต่อองค์กร การเปลี่ยนแปลงกระบวนการทำงานโดยการนำเทคโนโลยีสารสนเทศและการสื่อสาร เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การจัดการฐานข้อมูล การใช้เครื่องคอมพิวเตอร์และอุปกรณ์ การใช้เครือข่ายคอมพิวเตอร์และการสื่อสาร และการติดต่อสื่อสารผ่านระบบเครือข่าย ทั้งนี้ ภายใต้วิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศและการสื่อสารล้วนมีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร

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

1.2 วัตถุประสงค์การจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

2) เพื่อให้มีการปฏิบัติตามกฎระเบียบ หรือนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม. อย่างมีระบบและต่อเนื่อง มีแผนงานที่สามารถแก้ไขสถานการณ์ได้ทันท่วงทีกรณีเกิดสถานการณ์ฉุกเฉิน เช่น แผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. แผนรองรับกรณีฉุกเฉินและบริหารความต่อเนื่องในสภาวะวิกฤติ สป.พม. เป็นต้น

3) เพื่อให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการมอบหมายเจ้าหน้าที่ผู้รับผิดชอบในการปฏิบัติงานให้มีประสิทธิภาพตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ให้บรรลุเป้าหมาย เกิดผลการปฏิบัติงานและการป้องกันความเสียหายของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4) เพื่อเป็นแนวทางในการดำเนินงาน การกำกับดูแล การมอบหมาย การติดตามงาน การตรวจทานและประเมินความเสี่ยงฯ ตลอดจนมีการเผยแพร่และประชาสัมพันธ์ผ่านช่องทางเว็บไซต์ ระบบ Intranet และช่องทางอื่นๆ ของ สป.พม. เพื่อให้เกิดความเข้าใจระหว่างผู้ปฏิบัติและผู้บริหาร ในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ของ สป.พม.

1.3 เป้าหมายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ มีแผนสำหรับดำเนินการเพื่อจัดการความเสี่ยงฯ ดังนี้

1.3.1 มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม.

1.3.2 มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

1.3.3 มีแผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม.

1.3.4 มีแผนรองรับกรณีฉุกเฉินและบริหารความต่อเนื่องในสภาวะวิกฤติ สป.พม.

1.4 ขอบเขตการดำเนินงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม. ภายใต้ข้อปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดำเนินการโดยคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 สป.พม. มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสารสนเทศ ระบบฐานข้อมูลและการจัดเก็บข้อมูล

1.5.2 สป.พม. มีแนวทางในการดูแลบำรุงรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีเสถียรภาพและมีความพร้อมใช้งานอย่างต่อเนื่อง

บทที่ 2

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

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 ประเมินและจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือองค์กร 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 เพื่อลดความสูญเสียที่เกิดขึ้นในอดีต ทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2.2.2 การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

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

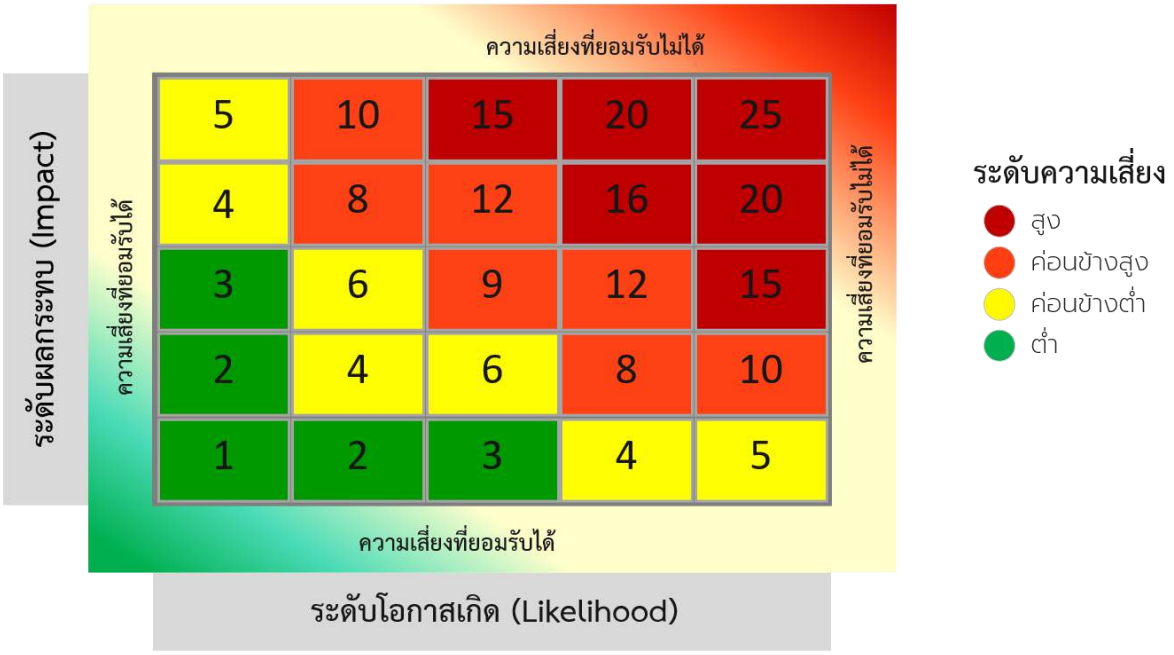
เกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง ดังนี้

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

- การประเมินความเสี่ยง -



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 ด้วยการรายงานผลการวิเคราะห์ ประเมิน และบริหารจัดการความเสี่ยงว่า มีความเสี่ยงที่ยังคงเหลืออยู่หรือไม่ ถ้ายังมีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร เสนอต่อผู้บริหารเพื่อทราบและสั่งการ

2.2.5 การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการทบทวน/ติดตามภายหลังจากได้ดำเนินการตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนฯ นั้นมีประสิทธิภาพ

2.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) ได้วิเคราะห์ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. 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 การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากมนุษย์ ภัยจากธรรมชาติ

หรือเหตุการณ์ใดๆ 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 ความเสี่ยงจากภัยคุกคามไซเบอร์

ภัยคุกคามไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใดๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) กระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP) ที่ใช้โดยผู้คุกคาม

2.4.1 อาชญากรรมคอมพิวเตอร์ ผู้ก่อการร้ายทางไซเบอร์ การจารกรรมทางไซเบอร์

2.4.2 Ransomware (แรนซัมแวร์) เป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่างๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่างๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์โดยมีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware

2.4.3 Phishing (ฟิชชิง) คือ การโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่างๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่น การส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังดีนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่นๆ ของเป้าหมาย เช่น ข้อมูลการเงิน ข้อมูลรหัสระบบต่างๆ ที่เป็นข้อมูลส่วนบุคคล

2.4.4 Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือ ซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น

2.4.4.1 Virus (ไวรัส) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศ โดยมุ่งเน้นในการโจมตี ขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้

2.4.4.2 Worms (เวิร์ม) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศ ที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอก โดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่าย จนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้

2.4.4.3 Trojan (โทรจัน) เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับ เปลี่ยนแปลง แก้ไขข้อมูล ซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศ หรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้

2.4.4.4 Spyware (สปายแวร์) คือ ซอฟต์แวร์ประสงค์ร้าย ที่ทำงานอย่างลับๆ บนคอมพิวเตอร์ และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล

2.4.4.5 Adware (แอดแวร์) คือ ซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัย

2.4.5 Data leaks (ข้อมูลรั่วไหล) ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้

2.4.6 ภัยธรรมชาติ ได้แก่ น้ำท่วม แผ่นดินไหว พายุเข้า

2.4.7 สภาพแวดล้อม ได้แก่ ระบบไฟฟ้าขัดข้อง อุณหภูมิไม่เหมาะสม ความชื้นจากเครื่องปรับอากาศ โครงสร้างพื้นฐานถูกทำลาย

2.5 การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ หมายถึง การดำเนินการในการป้องกันภัยคุกคามไซเบอร์ โดยใช้มาตรการและกระบวนการบริหารความเสี่ยง เพื่อวิเคราะห์ภัยคุกคามไซเบอร์ ประเมินความเสี่ยงที่อาจจะเกิดขึ้น โดยการจัดหา จัดทำมาตรการ จัดหาวัสดุอุปกรณ์ เพื่อป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ หมายถึง วิธีการ มาตรการ หรือการดำเนินการใดๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งานของอุปกรณ์และข้อมูลภายในระบบสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

2.6 การตอบสนองความเสี่ยง

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

2.6.1 การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้นโดยมิได้คิดทบทวนถึงผลที่จะได้รับอาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

2.6.2 การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่กำหนดให้แล้ว อาจจะบอก User/Password ของตน ให้ผู้ใต้บังคับบัญชาทราบ และเมื่อผู้ใต้บังคับบัญชาทราบ User/Password ของหัวหน้างานอาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายและหน่วยงานที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นแล้วจึงแก้ไขโดยการกำหนด User/Password ใหม่ให้กับหัวหน้างาน เป็นต้น

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

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

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

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

2.7 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของ สป.พม. มีดังนี้

2.7.1 ปัจจัยภายนอก ได้แก่

2.7.1.1 ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และภัยพิบัติอื่นๆ

2.7.1.2 การขโมยอุปกรณ์เครื่องแม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

2.7.1.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) จากการเคลื่อนย้าย หรือ อื่นๆ

2.7.1.4 ระบบการสื่อสารของระบบเครือข่ายหลักเสียหาย/ขัดข้อง

2.7.1.5 ระบบกระแสไฟฟ้าขัดข้อง/ไฟดับ

2.7.1.6 ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะ เช่น หนู แมลงสาป เป็นต้น

2.7.2 ปัจจัยภายใน ได้แก่

2.7.2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.7.2.2 การถูกไวรัสคอมพิวเตอร์ ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่างๆ

2.7.2.3 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.8 การประเมินความเสียหาย

2.8.1 ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบ ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) เสียหาย และระบบฐานข้อมูลเสียหาย

2.8.2 ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วคราว ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของระบบเครือข่ายคอมพิวเตอร์ขัดข้อง กระแสไฟฟ้าขัดข้อง

2.9 การติดตามและรายงานผล

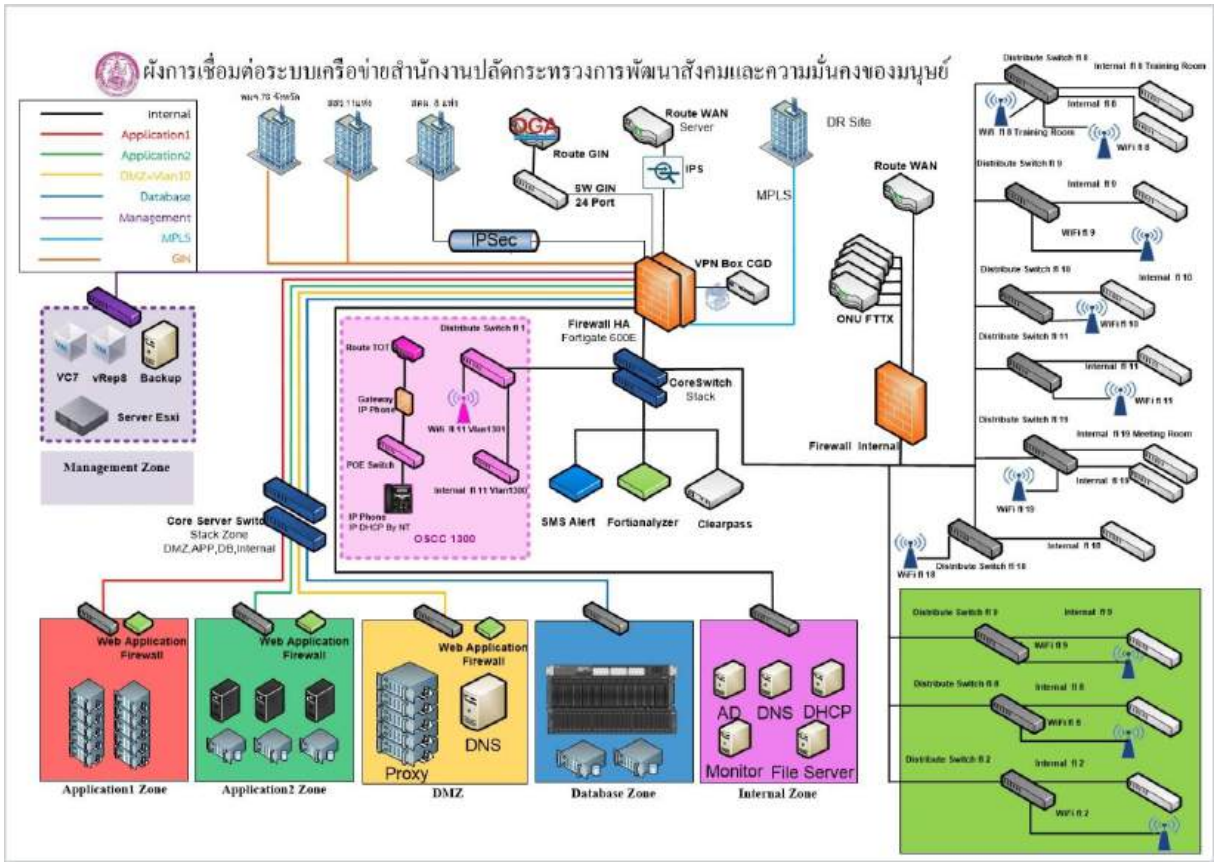
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการ หรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน ให้รายงานการเกิดปัญหาและผลการแก้ไข ให้ผู้ที่ได้รับมอบหมาย/ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ เจ้าหน้าที่ที่รับผิดชอบจะต้องมีคำสั่งแต่งตั้งจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร สำหรับรูปแบบรายงานใช้รายงานการตรวจรับงานที่ดำเนินการบำรุงรักษาระบบฯ ประจำเดือนทุกเดือน

2.10 ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์ของ สป.พม. ได้มีการพัฒนาและปรับเพิ่มประสิทธิภาพอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของ สป.พม. ตั้งอยู่ที่อาคารกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เลขที่ 1034 ถนนกรุงเกษม แขวงมหานาค เขตป้อมปราบศัตรูพ่าย กรุงเทพมหานคร มีการเชื่อมโยงเครือข่ายไปยังหน่วยงานภายในส่วนกลางของ สป.พม. และส่วนภูมิภาคสำนักงานพัฒนาสังคมและความมั่นคงของมนุษย์จังหวัด (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. เช่น Web Server และ Mail Server เป็นต้น รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบ Client-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของ สป.พม. เพื่อให้ได้รับความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด

ผังระบบเครือข่ายสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

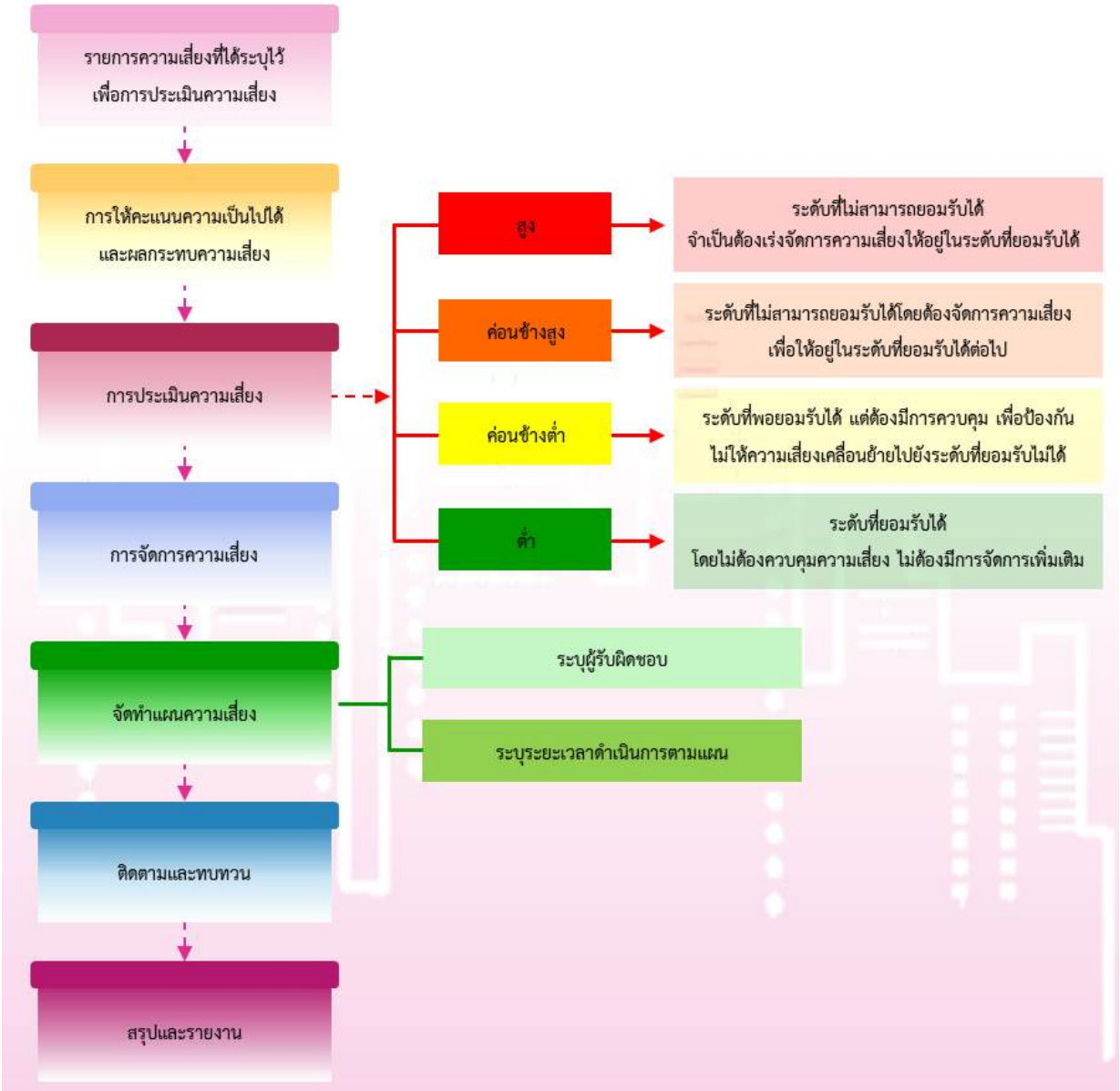


บทที่ 3

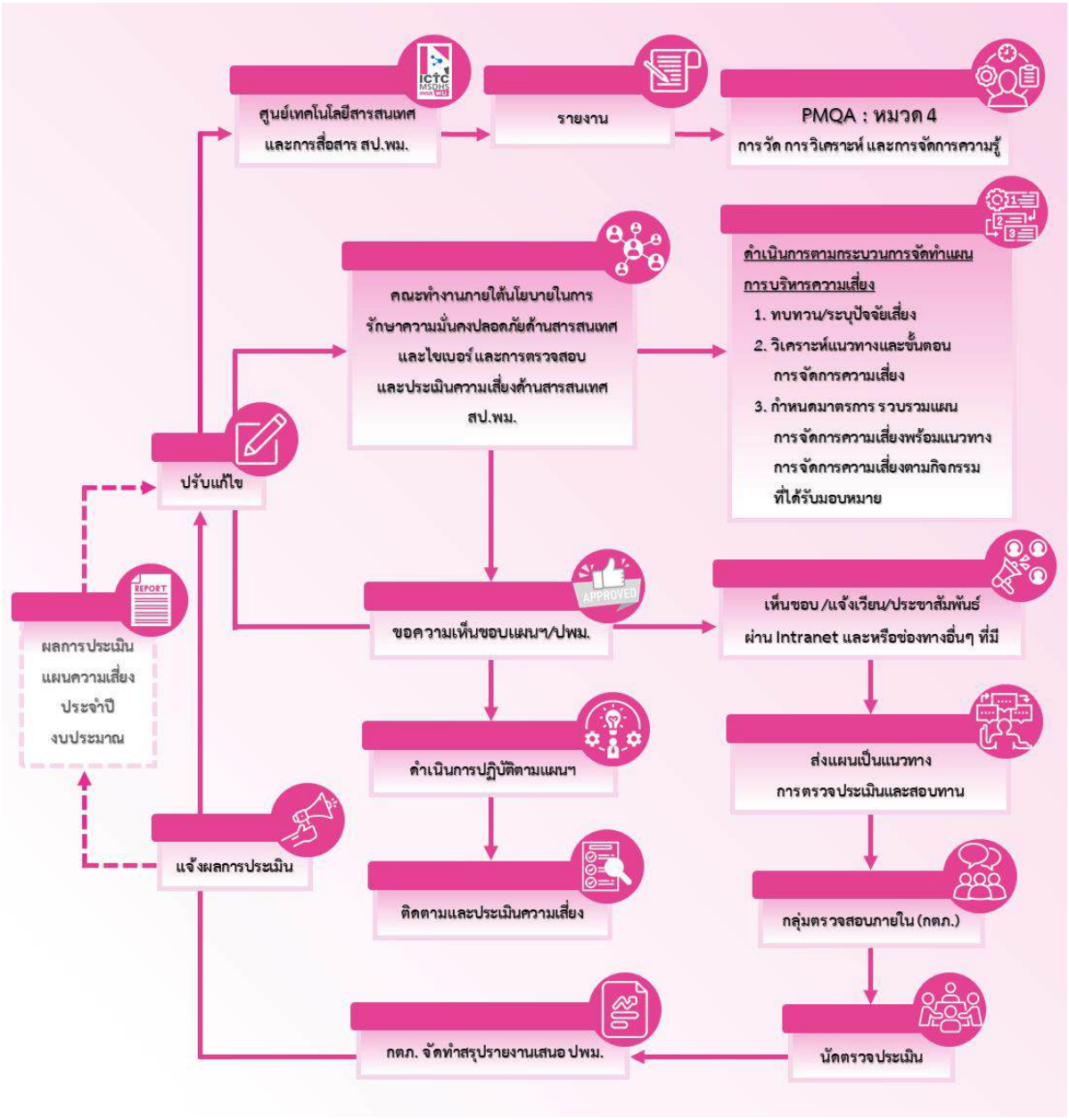
การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

สป.พม. ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจเกิดความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงได้มอบหมายให้ ศทส. จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567 โดยกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. เริ่มต้นจากการรวบรวมกิจกรรม/ปัจจัยเสี่ยง ที่เกี่ยวข้องกับกระบวนการที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำการศึกษาข้อมูล ระดมความคิดเห็นกับเจ้าหน้าที่ผู้ปฏิบัติงานด้านกิจกรรมต่างๆ ดังนี้

3.1 แนวทางและขั้นตอนการบริหารความเสี่ยง



3.2 กระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

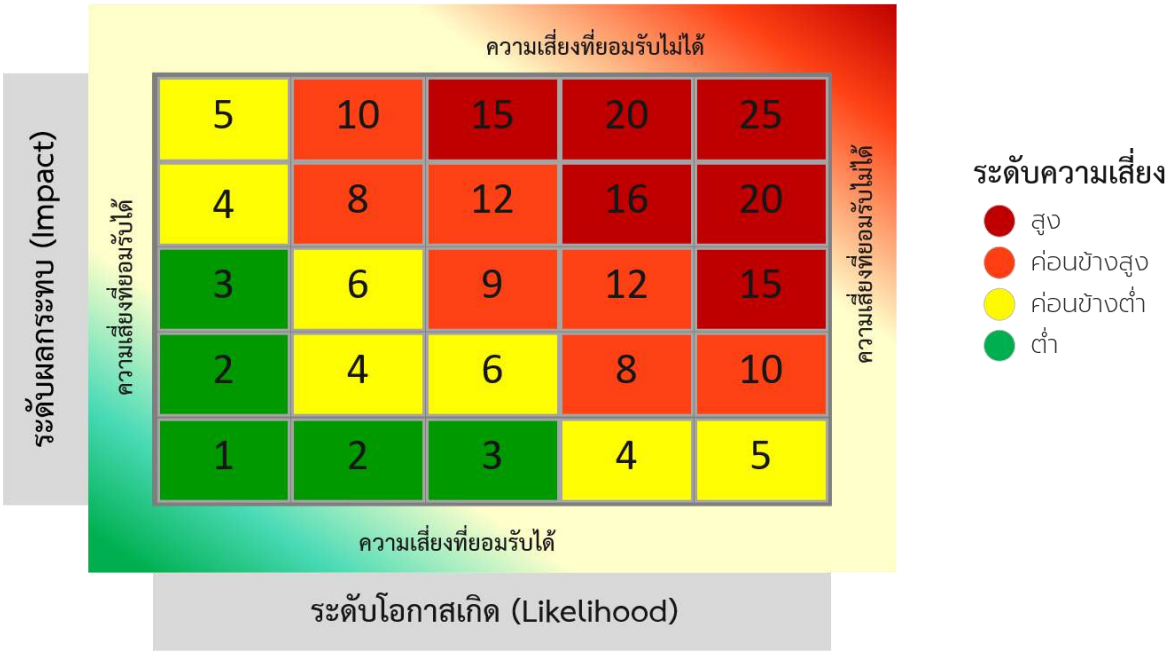


3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

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

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

- การประเมินความเสี่ยง -



3.4 ผลการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2566

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
1. การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม **<u>วัตถุประสงค์</u>** เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติและสิ่งแวดล้อมและผลกระทบที่เกิดขึ้น					
1.1 ไฟไหม้ห้องศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่ายอุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติ โดยการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้าน	1	5	5
1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ ไฟกระชากจากปลั๊กพ่วง	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้	ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS)/แบตเตอรี่สำรองไฟ	1	4	4
1.3 การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์	- เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น มีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ	1	3	3
1.4 ไม่มีการกำหนดสิทธิ์และไม่ควบคุมการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่าย	- มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. - มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการ ในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง	1	3	3
1.5 ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะต่ออุปกรณ์ที่ติดตั้งภายในห้องไฟฟ้าสื่อสารตามชั้นต่างๆ ภายในอาคารและพื้นที่สำนักงาน	- เจ้าหน้าที่ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตของ สป.พม. ได้	- มีการฉีดยาป้องกันแมลง บริเวณภายในอาคารเป็นประจำ - ตรวจสอบและบำรุงรักษาอุปกรณ์อย่างต่อเนื่อง - จัดพื้นที่สำหรับรับประทานอาหารให้เป็นสัดส่วน	2	2	4

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
2. การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ **<u>วัตถุประสงค์</u>** เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้งและไวรัสคอมพิวเตอร์ อย่างสม่ำเสมอ					
2.1 ขาดการทบทวน/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร ให้เป็นปัจจุบัน	- ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย - ขาดข้อมูลบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสารที่เป็นปัจจุจบัน	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ศทส.	1	3	3
2.2 ขาดมาตรการรองรับในการจัดการฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ - ทดสอบการโจมตีตามแผนที่กำหนดจริง	2	2	4
2.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบ ขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ในกรณีที่เกิดความผิดพลาด	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสาร'ทั้งระบบ - ระบุตัวตนผู้ใช้งานระบบ/ผู้ดูแลระบบไม่ได้ - หาผู้กระทำความผิดไม่ได้ - อุปกรณ์จำนวนเพิ่มมากขึ้น จึงอาจทำให้เกิดความผิดพลาดได้มากขึ้น	มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ ทุก 6 เดือน	2	3	6
2.4 ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการ ระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ระบบฯ เสียหาย/ขัดข้องไม่สามารถเข้าถึงบริการสารสนเทศได้	- ระบุข้อกำหนด/ข้อตกลง ระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก	1	3	3

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้		- มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบหรือ ผอ. ศทส. ทุกครั้งที่ระบบฯ ขัดข้องเพื่อให้แก้ปัญหาได้ทันท่วงที			
2.5 ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และยืนยันตัวบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา - มีการปรับเพิ่มประสิทธิภาพการบริหารจัดการทุกๆ ปี	2	2	4
2.6 ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือ และให้บริการไม่มีประสิทธิภาพ	มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตาม และรายงานผล ทุก 3 เดือน	2	3	6

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
3. ด้านระบบสารสนเทศและฐานข้อมูล **<u>วัตถุประสงค์</u>** เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศฐานข้อมูลต่างๆ ถูกทำลาย จากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้					
3.1 การโจมตีโดยบุคคลที่ ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป - ข้อมูลสารสนเทศและการทำงานของระบบส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - จัดทำการสำรองข้อมูลระบบฐานข้อมูล อย่างสม่ำเสมออย่างน้อยเดือนละ 1 ครั้ง - จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. ให้สอดคล้องกับสถานการณ์ปัจจุบันอย่างเหมาะสม - การทดสอบการเจาะระบบสารสนเทศที่สำคัญ เพื่อหาช่องโหว่อย่างน้อยปีละ 1 ครั้ง - VA scan เพื่อค้นหาช่องโหว่ของระบบปฏิบัติการ ระบบแอปพลิเคชัน และระบบฐานข้อมูล - ปรับปรุง source code เพื่อปิดช่องโหว่ที่ตรวจพบ หมายเหตุ : VPN (Virtual Private Network) ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้	2	3	6

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
3.2 ไม่มีการดำเนินการตามแผนการสำรองและทดสอบกู้คืนข้อมูล	- เกิดความเสียหายแก่ระบบข้อมูล/ฐานข้อมูลทำให้ใช้งานไม่ต่อเนื่อง - ไม่สามารถกู้คืนระบบข้อมูล/ฐานข้อมูลได้ไม่มีการกำหนดแผนสำรองในภาวะฉุกเฉิน	- จัดทำการสำรองข้อมูลแบบอัตโนมัติโดยจัดเก็บ Storage ทุกวัน เฉพาะส่วนที่เพิ่มในแต่ละวัน และจัดเก็บข้อมูลทั้งระบบแบบ Full Backup บน Storage สัปดาห์ละ 1 ครั้ง - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติโดยจัดเก็บใน Hard Disk เป็นประจำทุกเดือน - มีการทดสอบการกู้คืนข้อมูลของทุกระบบงาน อย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการเตรียมความพร้อมหากเกิดสถานการณ์ฉุกเฉิน - มีการควบคุมกำกับการสำรองข้อมูลให้เป็นไปตามแผนพร้อมทั้งการตรวจสอบความสมบูรณ์ในการสำรองข้อมูลทุกครั้ง	1	5	5
3.3 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลายเกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ - ถูกโจมตีระบบทำให้ไม่สามารถให้บริการได้	- 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	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบที่มีการพัฒนาไว้อย่างหลากหลาย - อาจต้องสูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูงเกิดความไม่คุ้มค่า	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์ และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตาม ทุกขั้นตอนการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐานและ TOR	1	3	3

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
3.5 เกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต	- ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ และมีการกำหนดไว้ใน TOR ในการบำรุงรักษาระบบสารสนเทศ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง - ดำเนินการปรับปรุง version ของระบบปฏิบัติการและบริการของระบบสารสนเทศให้เป็นปัจจุบัน	1	4	4
3.6 ขาดการบำรุงรักษาโปรแกรมหรือระบบงานอย่างต่อเนื่อง	- อาจเกิดข้อขัดข้องจนระบบไม่สามารถทำงานได้ - เกิดช่องโหว่อันเกิดจากไม่มีการอัปเดตเวอร์ชันอย่างสม่ำเสมอ ทำให้ไม่สามารถใช้ระบบได้อย่างต่อเนื่อง/ในเวลาที่ต้องการ - ผู้ดูแลระบบไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้	- ทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่องเพื่อปิดช่องโหว่จากการอัพเดทเวอร์ชั่นใหม่ๆ อย่างสม่ำเสมอ ทำให้สามารถใช้ระบบได้อย่างต่อเนื่องและใช้ในเวลาที่ต้องการได้ - จัดทำ TOR ในการจัดซื้อจัดจ้างการพัฒนาระบบ ให้ครอบคลุมถึงการอบรมให้ความรู้ในการแก้ไขปัญหา เมื่อระบบขัดข้อง พร้อมทั้งส่งคู่มือระบบการใช้งานและแก้ไขปัญหาให้กับผู้ดูแลระบบ	1	5	5
3.7 การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ออกรายงานผิดพลาด	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - รวบรวมข้อผิดพลาดที่เกิดขึ้น และปรับปรุงระบบ ให้สามารถป้องกันการนำเข้าข้อมูลที่ผิดพลาดได้	1	3	3
3.8 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ - กำหนดนโยบายในการนำเข้าข้อมูล - กำหนดตัวชี้วัด	1	3	3

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. 2567

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
		- กำหนดรายการข้อมูลที่สำคัญ - พัฒนาระบบให้ตรงตามความต้องการของผู้ใช้งาน - ประสานความร่วมมือกับผู้รับผิดชอบหลักในการบันทึกข้อมูล			
3.9 ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูล เพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	- ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลาง กระทรวง พม. อย่างต่อเนื่อง - มีการติดตามการนำมาตรฐานข้อมูลกลาง กระทรวง พม. ไปใช้อย่างสม่ำเสมอ - มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) - มีการดำเนินงานทบทวน/ปรับปรุงและเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลางกระทรวง พม. ที่ครอบคลุมภารกิจของกระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ	1	2	2
3.9 ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	- ไม่มีความมั่นคงปลอดภัยในการเข้าใช้งานเนื่องจากไม่มีการควบคุมการเข้าถึง - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้	- มีการกำหนดสิทธิ์ในการเข้าถึง เพื่อทำการจำกัดและควบคุมการเข้าถึง - ใช้งานโปรแกรมเพื่อป้องกันการละเมิด โดยการตรวจสอบสิทธิ์ - มีการทบทวนสิทธิ์เป็นประจำ โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ อย่างน้อยปีละ 1 ครั้ง	1	3	3

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
		- ปฏิบัติตามข้อปฏิบัติในการควบคุม การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. อย่างเคร่งครัด			
4. ด้านโปรแกรมคอมพิวเตอร์ **<u>วัตถุประสงค์</u>** ควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อับเดท เพื่อลดช่องโหว่ที่เกิดจาก Bugของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบหรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์ **หมายเหตุ** Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้น ๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้					
4.1 ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) **หมายเหตุ :** Utility Program คือ ระบบโปรแกรมที่ติดมาพร้อมระบบปฏิบัติการ Windows เรียกง่ายๆ ว่าเป็นโปรแกรมที่ช่วยดูแลการทำงานของ Windows เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำและส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย	3	2	6
4.2 ขาดการป้องกันหรือตรวจจับ Malware	- เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบสารสนเทศและฐานข้อมูล - เกิดผลกระทบต่อการใช้งานเครือข่าย	จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ - จัดทำ VLAN เพื่อแบ่งเครือข่ายออกเป็นกลุ่มย่อย - ส่งเสริมให้บุคลากรมีการสำรองข้อมูลที่สำคัญในเครื่อง PC ของตนเองอย่างสม่ำเสมอ	1	4	4
5. ด้านบุคลากร **<u>วัตถุประสงค์</u>** เพื่อควบคุมความเสี่ยงที่เกิดจากการดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ เป็นความเสี่ยงที่เกิดจากความล้มเหลวหรือความไม่เหมาะสมของบุคลากร					
5.1 มีการใช้บัญชีผู้ใช้งาน	- ไม่สามารถระบุตัวตนผู้ใช้งานได้ เมื่อมีผู้ใช้งาน	ปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน	1	3	3

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
(username) ร่วมกัน ในการเข้าถึงระบบสารสนเทศและยืนยันตัวตนอินเทอร์เน็ต	กระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และเครือข่าย -ไม่สามารถตรวจสอบการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศได้ - ผู้รับผิดชอบที่ได้รับมอบหมายไม่สามารถติดตามตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศได้	สารสนเทศ สป.พม. โดยใช้แบบฟอร์มการขอใช้งานบัญชีผู้ใช้งานเพื่อการจัดเก็บ Log ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ - ส่งเสริมให้ผู้ใช้งานตระหนักถึงโทษตาม พ.ร.บ.คอมพิวเตอร์ฯ และความเสียหายที่จะเกิดขึ้น - ทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศและอินเทอร์เน็ตอย่างน้อยปีละ 1 ครั้ง			
5.2 การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญ ความเชี่ยวชาญในการดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไข ทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจน และควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้ - มีการติดตามเพื่อป้องกันการผิดพลาด และให้เกิดการแก้ไขปัญหาได้ทันที โดยมีการประชุมทุกๆ สัปดาห์	1	3	3
5.3 บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	- เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้ - มีค่าใช้จ่ายในการบำรุงรักษาเพิ่มมากขึ้น	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง - มีการจัดทำคู่มือในการปฏิบัติงานเฉพาะด้าน สำหรับผู้ดูแลระบบ เช่น application admin , system admin	2	3	6
5.4 ผู้ใช้งาน/users ไม่มีความรู้ความชำนาญและทักษะในการใช้งานระบบ	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนดทำให้เกิดข้อขัดข้องไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ ทำให้งานติดขัด	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีระบบ Call Center สำหรับให้คำปรึกษาเกี่ยวกับการใช้งาน	2	3	6

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
	- ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งานทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบัน ขาดความน่าเชื่อถือ ข้อมูลไม่ถูกนำไปใช้งาน	ระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุง หรือตามความต้องการของ User - สร้างความตระหนักถึงประโยชน์ของการนำข้อมูลไปใช้ในการวางแผนและปฏิบัติงาน - กำหนดการใช้งานระบบเป็นตัวชี้วัดหน่วยงานในเชิงคุณภาพ			
5.5 ผู้ใช้งาน (Users) ใช้คอมพิวเตอร์/เครือข่าย ผิดวัตถุประสงค์	- ผู้ใช้งาน (Users) ใช้งานเครือข่ายอินเทอร์เน็ตของ สป.พม. ในการเข้าเว็บไซต์ที่ไม่เหมาะสม/ติดตั้งโปรแกรมที่ไม่ได้รับอนุญาต/นำอุปกรณ์ที่ไม่ได้รับอนุญาตมาติดตั้ง ทำให้เครือข่ายอินเทอร์เน็ตไม่สามารถใช้งานได้และเครือข่ายอินเทอร์เน็ตของหน่วยงานทำงานผิดพลาด	- มีนโยบายและแนวทางในการควบคุมการใช้คอมพิวเตอร์ไม่ให้ใช้เครือข่ายผิดวัตถุประสงค์ - ควบคุมและบังคับใช้อย่างเคร่งครัด พร้อมทั้งกำหนดบทลงโทษ - จัดหาอุปกรณ์ตรวจสอบการเข้าถึงเครือข่ายและตรวจสอบระบบเครือข่ายอย่างสม่ำเสมอ	1	3	3
6. ด้านงบประมาณ **<u>วัตถุประสงค์</u>** เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ /การเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา					
6.1 การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	- ตามนโยบายของหน่วยงานมีการปรับลดงบประมาณ โดยลดเป็นเปอร์เซ็นต์เท่าๆ กัน ทำให้โครงการที่จำเป็นจะต้องดำเนินการถูกตัด/ปรับลดไปด้วย - งวดเงิน/งวดงาน ไม่สอดคล้องกัน เนื่องจากการบริหารงบประมาณของภาครัฐและหน่วยงานมีการโอนงวดเงินเป็นเปอร์เซ็นต์ที่เท่ากัน	- ปรับโครงการโดยจัดลำดับความสำคัญใหม่ ลดขอบเขตงานลง - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ - บริหารจัดการงบประมาณภายในหน่วยงานให้มีประสิทธิภาพ	4	1	4

ปัจจัยเสี่ยง	ลักษณะความเสี่ยงความเสียหายที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาสความถี่	ผลกระทบความรุนแรง	ระดับคะแนน
7. ด้านการบริหารจัดการ **<u>วัตถุประสงค์</u>** เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี จากการกำกับดูแลที่ดี หรือ ขาดธรรมาภิบาลในองค์กร ขาดการควบคุมที่ดี					
7.1 ความเสี่ยงจากการจัดซื้อจัดจ้าง - กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคาได้ - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา - ผู้รับจ้างไม่ปฏิบัติตามข้อกำหนด	- เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง - ไม่สามารถตรวจรับงานได้ - ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปีได้ ทำให้มีผลกระทบต่อการรายงานผลตัวชี้วัดขององค์กร	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการ - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนด โดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสม เพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด	1	3	3
7.2 แผนเตรียมความพร้อมกรณีฉุกเฉินไม่ครอบคลุมกับสถานการณ์ที่เกิดขึ้น เช่น กรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	เจ้าหน้าที่ไม่สามารถเข้าไปปฏิบัติงานได้ตามปกติ เนื่องจากถูกปิดล้อมสถานที่ทำงาน หน่วยงานถูกตัดกระแสไฟฟ้า ทำให้ระบบงานหยุดทำงาน ไม่ให้บริการได้ เนื่องจากไม่สามารถเข้าระบบจากระยะไกล (Remote) ได้	- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และทบทวนแผนฯ อย่างน้อยปีละ 1 ครั้ง - มอบหมายผู้รับผิดชอบและดำเนินการตามแผนฯ อย่างเคร่งครัด	1	3	3

3.5 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
1. ด้านกายภาพและสิ่งแวดล้อม วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อม และผลกระทบที่เกิดขึ้น	1.1	ไฟไหม้ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบ
	1.2	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้ (การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
	1.3	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
	1.4	- มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต - ประตูปิดไม่สนิท - อุปกรณ์ควบคุมการเข้าถึงเสีย	- มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. - มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ
2. ด้านบุคลากร วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	2.1	ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึงและการใช้งานระบบสารสนเทศ	มีความเสี่ยงที่อาจเกิดความเสียหายกับระบบสารสนเทศ ทำให้ระบบสารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูลรั่วไหล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.2	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
	2.3	ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบหรือเปลี่ยนผู้ปฏิบัติงานบ่อย	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนด ทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ งานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งาน ทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ ข้อมูลไม่ถูกนำไปใช้งาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.4	การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	- ข้อมูลของหน่วยงานเกิดการรั่วไหลอันเนื่องมาจากผู้รับจ้างประมาทเลินเล่อ ขาดความตระหนักในการดูแลข้อมูลสำคัญระหว่างการบำรุงรักษา/พัฒนาระบบ - หน่วยงานได้รับความเสียหายด้านภาพลักษณ์และชื่อเสียง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.5	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญ ดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไข ทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้งและไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ	3.1	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.2	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.3	การบริหารจัดการสิทธิ์ การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศ และการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับ ผู้ใช้งานขาดประสิทธิภาพ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบุตัวตนผู้ใช้งานไม่ได้ - หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถระบุตัวตนผู้ใช้งานตัวจริงได้
	3.4	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	เกิดความเสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถเข้าถึงระบบสารสนเทศ จากภายนอกได้ - เครื่องคอมพิวเตอร์แม่ข่าย ไม่สามารถเข้าถึงอินเทอร์เน็ตได้

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
	3.5	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.6	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไข เปลี่ยนแปลง หรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไข เปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.7	ขาดการป้องกันหรือตรวจจับไวรัส	เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบเครือข่าย ระบบสารสนเทศและฐานข้อมูล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
4. ด้านโปรแกรมคอมพิวเตอร์ วัตถุประสงค์ : ควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัปเดท เพื่อลดช่องโหว่ที่เกิดจาก Bug ของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์ *หมายเหตุ Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้นๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้	4.1	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) (Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดส์ เรียกง่ายๆ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์ เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น)	- หน่วยงาน/บุคคล ต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
5. ด้านระบบข้อมูล วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูลต่างๆ	5.1	ไม่มีการจัดทำบัญชีรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง	- ไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที - เมื่อระบบเสียหายไม่สามารถหาสาเหตุได้ - ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
ถูกทำลายจากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทั้งจากคน ธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้	5.2	ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบุตัวตนผู้ใช้งานได้ไม่ได้ - หาผู้กระทำความผิดไม่ได้ - การถูกยึดครองระบบจากผู้ไม่หวังดี (Hacker)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.3	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ใช้บริการทั่วไปไม่มีประสิทธิภาพ - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.4	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบ เนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - หน่วยงาน
	5.5	การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์ไม่มีความชัดเจน	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบที่มีการพัฒนาไว้อย่างหลากหลาย - สูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูง เกิดความไม่คุ้มค่า	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.6	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.7	เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.8	การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ
	5.9	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
6. ด้านกลยุทธ์ วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการกำหนดนโยบาย กลยุทธ์ ที่ทำให้แผนการดำเนินงานไม่สามารถบรรลุวัตถุประสงค์องค์กร	6.1	ทิศทาง/แนวทางการพัฒนาด้านเทคโนโลยีสารสนเทศไม่ชัดเจน/ไม่สอดคล้องกับภารกิจ ขาดการบูรณาการร่วมกัน	ไม่สามารถลดความซ้ำซ้อนของกระบวนการหรือระบบงานได้ ทำให้ขาดประสิทธิภาพในการดำเนินงานและการใช้งบประมาณไม่คุ้มค่า	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน
7. ด้านการเงิน (งบประมาณ) วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ/การเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลาเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลา	7.1	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด ทำให้ได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ขาดงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน
8. ด้านการบริหารจัดการ วัตถุประสงค์ : เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี	8.1	- กระบวนการจัดซื้อ จัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคา - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา	การดำเนินโครงการเกิดความล่าช้า ทำให้ขาดประสิทธิภาพในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน

3.6 การประเมินแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
1. ด้านกายภาพและสิ่งแวดล้อม											
<u>วัตถุประสงค์</u> : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น											
1.1	ไฟไหม้ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	1	5	5	ควบคุมความเสี่ยง	- ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งานและตรวจสอบระบบดับเพลิงอัตโนมัติ เป็นการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้าน แผนฉุกเฉินกรณีไฟไหม้	1	2	2
1.2	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้ (การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไป โดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	2	4	8	จัดการความเสี่ยง	- ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS)/แบตเตอรี่สำรองไฟเป็นประจำทุก 3 เดือน - มีแผนการบำรุงรักษาระบบไฟฟ้าของอาคารสถานที่ ปีละ 1 ครั้ง	1	2	2

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
1.3	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	1	4	4	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น มีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้น ผ่านระบบควบคุมอย่างสม่ำเสมอ	1	3	3
1.4	- มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต - ประตูปิดไม่สนิท - อุปกรณ์ควบคุมการเข้าถึงเสีย	- มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. - มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	3	4	12	จัดการความเสี่ยง	- บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท - ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน	1	3	3
2. ด้านบุคลากร **<u>วัตถุประสงค์</u>** : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ											
2.1	ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วนในการบริหารจัดการสิทธิ์การเข้าถึงและการใช้งานระบบสารสนเทศ	มีความเสี่ยงที่อาจเกิดความเสียหายกับระบบสารสนเทศ ทำให้ระบบสารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูลรั่วไหล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	4	8	จัดการความเสี่ยง	มีการบริหารจัดการการควบคุมและเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก	1	3	3

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
								- การมอบหมายหน้าที่ ความรับผิดชอบที่ชัดเจน - การกำกับติดตามการดำเนินงาน			
2.2	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง	1	2	2
2.3	ผู้ใช้งาน/users ไม่มีความรู้ความชำนาญและทักษะการใช้งานระบบหรือเปลี่ยนผู้ปฏิบัติงานบ่อย	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนด ทำให้เกิดข้อขัดข้องไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ งานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งาน ทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ ข้อมูลไม่ถูกนำไปใช้งาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีช่องทางการแจ้งเหตุผ่านแอปพลิเคชัน LINE - มีระบบ Call Center สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุงตามความต้องการของ User	1	2	2
2.4	การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	- ข้อมูลของหน่วยงานเกิดการรั่วไหล อันเนื่องมาจากผู้รับจ้างประมาทเลินเล่อ ขาดความตระหนักในการดูแลข้อมูลสำคัญระหว่างการบำรุงรักษา/พัฒนาระบบ - หน่วยงานได้รับความเสียหายด้านภาพลักษณ์และชื่อเสียง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	4	8	จัดการความเสี่ยง	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน มีการทำข้อตกลงการห้ามเปิดเผยข้อมูล (NDA) และการใช้หรือประมวลผลข้อมูลส่วนบุคคล (DPA)	1	3	3

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
2.5	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญ ดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไข ทำให้ต้องขยายเวลาทำงานและไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาด ทำให้เกิดการแก้ไขปัญหาได้ทันที โดยมีการประชุมทุกๆ สัปดาห์ - มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจนและควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้	1	2	2
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร **<u>วัตถุประสงค์</u>** : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ											
3.1	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	1	3	3	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ศทส.	1	2	2
3.2	ขาดแผนรองรับระบบฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	1	5	5	ควมคุมความเสี่ยง	- มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ	1	3	3
3.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบุตัวตนผู้ใช้งานไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถระบุตัวตนผู้ใช้งานตัวจริงได้	3	3	9	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน	2	2	4

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ ที่ใช้จัดการ ความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผล กระทบ	ระดับ			โอกาส	ผล กระทบ	ระดับ
	และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับผู้ใช้งาน ขาดประสิทธิภาพ	- หาผู้กระทำความผิดไม่ได้						โดยการเปลี่ยนแปลง/ปรับปรุง/เพิ่มเติม/ แก้ไข '- มีการติดตามและจัดทำรายงานผลการ กำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน			
3.4	ระบบเครือข่ายสื่อสารหลัก สำหรับศูนย์ปฏิบัติการระบบ แม่ข่ายและเครือข่าย คอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับ ผู้ให้บริการได้	เกิดความเสียหาย/ขัดข้อง ไม่สามารถเข้าถึง บริการสารสนเทศจากระยะไกล (Remote) ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ ไม่สามารถเข้าถึงระบบ สารสนเทศจากภายนอกได้ - เครื่องคอมพิวเตอร์แม่ข่าย ไม่สามารถเข้าถึงอินเทอร์เน็ต ได้	1	5	5	ควบคุม ความเสี่ยง	- ให้มีการระบุเกี่ยวกับระดับการให้บริการ ที่ชัดเจนในข้อกำหนด/ข้อตกลงกับผู้ ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่าย สื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตาม ดูแล - มีสัญญาการบำรุงรักษาและการแก้ไข ปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบ หรือ ผอ. ศทส. ทุกครั้งที่ระบบขัดข้อง เพื่อให้แก้ปัญหาได้ทันท่วงที	1	2	2
3.5	ขาดการควบคุมอุปกรณ์ คอมพิวเตอร์และอุปกรณ์ สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งาน อุปกรณ์คอมพิวเตอร์พกพาและเครือข่าย คอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบ เครือข่ายคอมพิวเตอร์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	2	6	ควบคุม ความเสี่ยง	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และ อุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และ ยืนยันตัวบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการ อุปกรณ์พกพา - มีการปรับเพิ่มประสิทธิภาพการบริหาร จัดการทุกๆ ปี	2	1	2

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. 2567

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
3.6	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	5	5	25	ควบคุมความเสี่ยง	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตาม เพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน - เช่าบริการศูนย์รับมือและตอบสนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการจ้างเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์	2	3	6

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
3.7	ขาดการป้องกันหรือตรวจจับไวรัส	เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบเครือข่าย ระบบสารสนเทศและฐานข้อมูล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ	2	2	4
4. ด้านโปรแกรมคอมพิวเตอร์ **<u>วัตถุประสงค์</u> :** ควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัพเดท เพื่อลดช่องโหว่ที่เกิดจาก Bugของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์ หมายเหตุ Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้น ๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้										
4.1	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) (Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดส์ เรียกง่ายๆ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์ เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น)	- หน่วยงาน/บุคคล ต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุมคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	2	6	ควบคุมความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำ และส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย	2	1	2

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
5. ด้านระบบข้อมูล											
<u>วัตถุประสงค์</u> : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูล ต่างๆ ถูกทำลาย จาก ผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ ใด ๆที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้											
5.1	ไม่มีการจัดทำบัญชีรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง	- ไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที - เมื่อระบบเสียหายไม่สามารถหาสาเหตุได้ - ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	จัดทำ/ทบทวนรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง	1	2	2
5.2	ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบุตัวตนผู้ใช้งานได้ไม่ได้ - หาผู้กระทำความผิดไม่ได้ - การถูกยึดครองระบบจากผู้ไม่หวังดี (Hacker)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง/ปรับปรุง/เพิ่มเติม/แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ - ระบุคุณลักษณะทางเทคนิค ในการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบ ภายใต้ขอบเขตงานการพัฒนาระบบสารสนเทศ	2	2	4

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
5.3	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ใช้บริการทั่วไปไม่มีประสิทธิภาพ - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	5	5	25	จัดการความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - สำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง	2	3	6
5.4	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - หน่วยงาน	4	3	12	ควบคุมความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกล ในการเข้าถึง (VPN หรือ Virtual Private Network คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้)	2	2	4

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
								- การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งานทุก 6 เดือน			
5.5	การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์ไม่มีความชัดเจน	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบที่มีการพัฒนาไว้อย่างหลากหลาย - สูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูง เกิดความไม่คุ้มค่า	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	2	6	ควบคุมความเสี่ยง	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์และคุณสมบัติ ผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตามทุกขั้นตอนของการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐาน	2	1	2
5.6	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	2	6	ควบคุมความเสี่ยง	- มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลางกระทรวง พม. อย่างต่อเนื่อง - มีการติดตามการนำมาตรฐานข้อมูลกลางกระทรวง พม. ไปใช้อย่างสม่ำเสมอ - มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) - มีการดำเนินงานทบทวน/ปรับปรุงและเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลางกระทรวง พม. ที่ครอบคลุมภารกิจของ	2	1	2

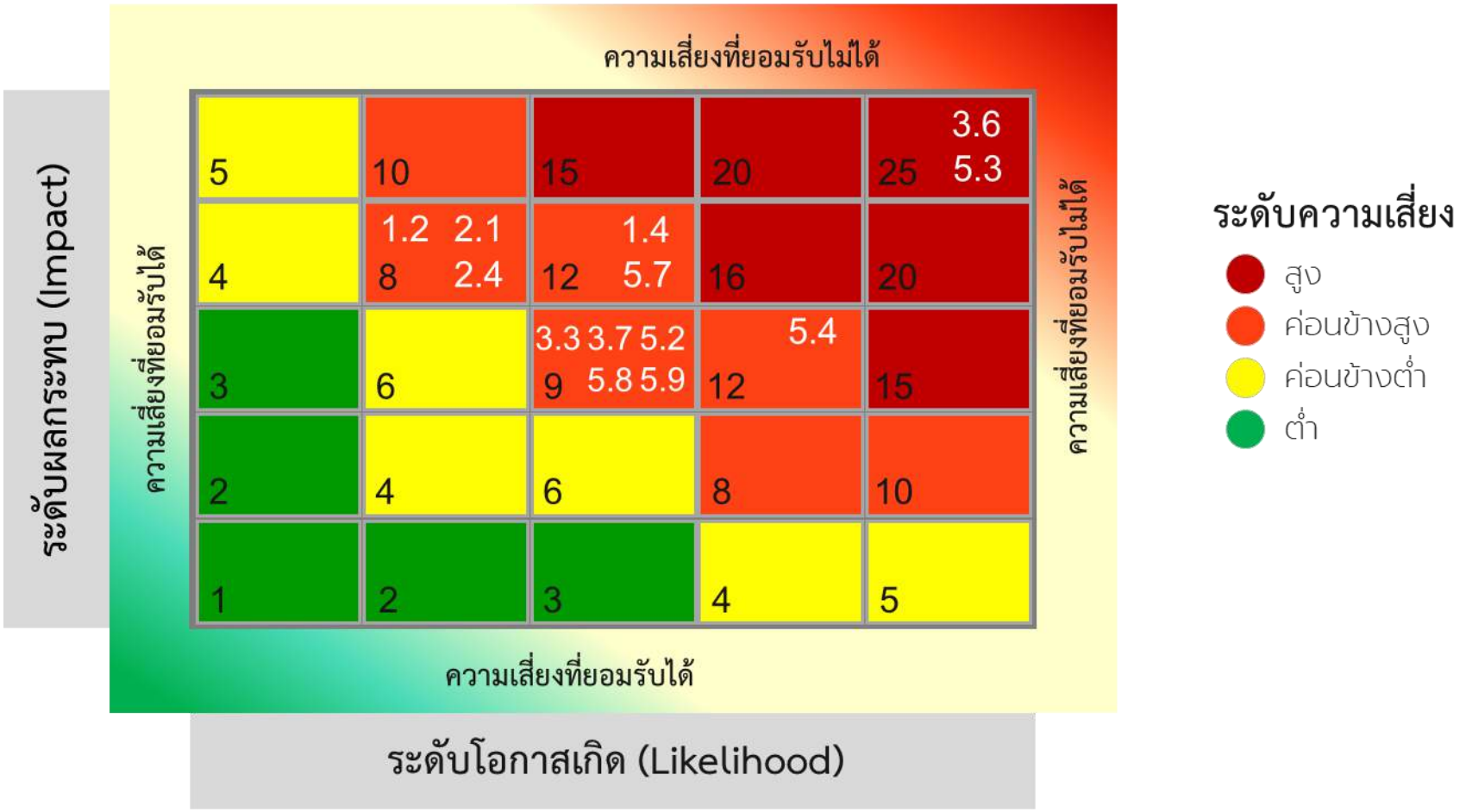
รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
								กระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ			
5.7	เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	4	12	จัดการความเสี่ยง	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง	2	2	4
5.8	การนำเข้าข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล	2	2	4
5.9	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ	2	2	4

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
6. ด้านกลยุทธ์											
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการกำหนดนโยบาย กลยุทธ์ ที่ทำให้แผนการดำเนินงานไม่สามารถบรรลุวัตถุประสงค์องค์กร											
6.1	ทิศทาง/แนวทางการพัฒนาด้านเทคโนโลยีสารสนเทศไม่ชัดเจน/ไม่สอดคล้องกับภารกิจ ขาดการบูรณาการร่วมกัน	ไม่สามารถลดความซ้ำซ้อนของกระบวนการหรือระบบงานได้ ทำให้ขาดประสิทธิภาพในการดำเนินงานและการใช้งบประมาณไม่คุ้มค่า	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน	3	2	6	ควบคุมความเสี่ยง	- จัดทำ/ทบทวน สถาปัตยกรรมองค์กรของหน่วยงาน (Enterprise Architecture : EA) - นำสถาปัตยกรรมองค์กรของหน่วยงานมาใช้เป็นกรอบแนวทางในการพัฒนาระบบเทคโนโลยีสารสนเทศของหน่วยงาน - ส่งเสริมและสนับสนุนให้บุคลากรทุกระดับเข้าใจและให้ความสำคัญในการจัดทำ	2	1	2
7. ด้านการเงิน (งบประมาณ)											
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ/การเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลาเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลา											
7.1	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด ทำให้ได้รับการสนับสนุน	ขาดงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน	3	2	6	ควบคุมความเสี่ยง	- จัดลำดับความสำคัญของโครงการที่จำเป็นต้องดำเนินการให้อยู่ในลำดับต้นๆ - จัดทำความเสี่ยงแนบไปกับโครงการ และให้มีการถ่วงน้ำหนักของโครงการที่เป็นโครงการประเภทเดียวกัน - ชี้แจงผลกระทบหากไม่ได้ดำเนินโครงการและการยอมรับความเสี่ยง - ปรับลดขอบเขตงานลง ตามงบประมาณที่ได้รับ - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ	3	1	3

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สนพ. ประจำปีงบประมาณ พ.ศ. 2567

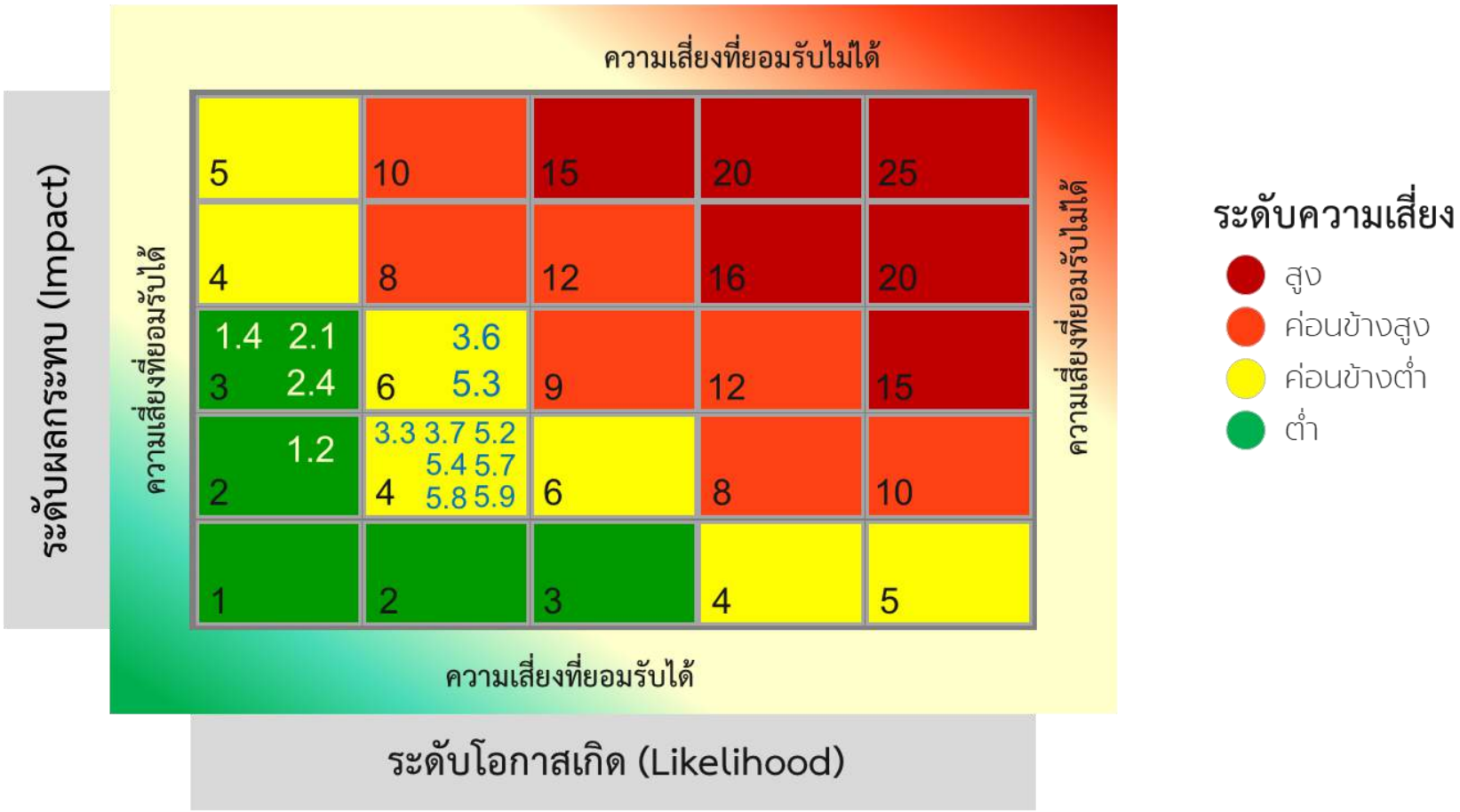
รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่อาจจะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับ			โอกาส	ผลกระทบ	ระดับ
8. ด้านการบริหารจัดการ											
<u>วัตถุประสงค์</u> : เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี											
8.1	กระบวนการจัดซื้อ จัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคา - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา	การดำเนินโครงการเกิดความล่าช้า ทำให้ขาดประสิทธิภาพในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน	3	2	6	ควบคุมความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญ/ความเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด	2	2	4

- แผนภูมิความเสี่ยง (Risk Map) ก่อนการจัดการความเสี่ยง -



3.8 การจัดทำแผนภูมิความเสี่ยง (Risk Map) หลังการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

- แผนภูมิความเสี่ยง (Risk Map) หลังการจัดการความเสี่ยง -



สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์
ประจำปีงบประมาณ พ.ศ. 2567

ปีงบประมาณ พ.ศ. 2567 ศทส. ได้ทำการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ และได้จัดทำแผนบริหารจัดการความเสี่ยง กำหนดกิจกรรม เป้าหมายการดำเนินการ โดยเพิ่มมาตรการจัดการความเสี่ยงและควบคุมความเสี่ยงให้อยู่ในระดับคะแนนที่ยอมรับได้ ซึ่งผลจากการวิเคราะห์และประเมินความเสี่ยง สรุปได้ดังนี้

ความเสี่ยงที่มีคะแนนอยู่ในระดับค่อนข้างสูง 11 ปัจจัยเสี่ยง คือ

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

รหัส 1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ ค่าคะแนนระดับ 8

รหัส 1.4 มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต ประตูปิดไม่สนิท อุปกรณ์ควบคุมการเข้าถึงเสีย ค่าคะแนนระดับ 12

ความเสี่ยงด้านบุคลากร

รหัส 2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึงและการใช้งานระบบสารสนเทศ ค่าคะแนนระดับ 8

รหัส 2.4 การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน ค่าคะแนนระดับ 8

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร

รหัส 3.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับ ผู้ใช้งานขาดประสิทธิภาพ ค่าคะแนนระดับ 9

รหัส 3.7 ขาดการป้องกันหรือตรวจจับไวรัส ค่าคะแนนระดับ 9

ความเสี่ยงด้านระบบข้อมูล

รหัส 5.2 ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย การทบทวนสิทธิ์ผู้ใช้งาน การบริหารจัดการรหัสผ่าน การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี ค่าคะแนนระดับ 9

รหัส 5.4 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง ค่าคะแนนระดับ 12

รหัส 5.7 เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ ค่าคะแนนระดับ 12

รหัส 5.8 การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug) ค่าคะแนนระดับ 9

รหัส 5.9 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน ค่าคะแนนระดับ 9

ความเสี่ยงที่มีคะแนนอยู่ในระดับสูง 2 ปัจจัยเสี่ยง คือ

ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร

รหัส 3.6 ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ค่าคะแนนระดับ 25

ความเสี่ยงด้านระบบข้อมูล

รหัส 5.3 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย ค่าคะแนนระดับ 25

3.9 แผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2567												ผู้รับผิดชอบ
		ต.ค.66	พ.ย.66	ธ.ค.66	ม.ค.67	ก.พ.67	มี.ค.67	เม.ย.67	พ.ค.67	มิ.ย.67	ก.ค.67	ส.ค.67	ก.ย.67	
1. ด้านกายภาพและสิ่งแวดล้อม **วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น**														
1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS)/แบตเตอรี่สำรองไฟเป็นประจำทุก 3 เดือน - มีแผนการบำรุงรักษาระบบไฟฟ้าของอาคารสถานที่ปีละ 1 ครั้ง													ศทส.
1.4 มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต - ประตูปิดไม่สนิท - อุปกรณ์ควบคุมการเข้าถึงเสีย	- บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการ ในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท - ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน													ศทส.
2. ด้านบุคลากร **วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ**														
2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์การเข้าถึงและการใช้งานระบบสารสนเทศ	มีการบริหารจัดการการควบคุมและเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก - การมอบหมายหน้าที่ความรับผิดชอบที่ชัดเจน - การกำกับติดตามการดำเนินงาน													ศทส.

แผนปฏิบัติการบริหารจัดการความเสี่ยงฯ ประจำปีงบประมาณ พ.ศ. 2567 (ต่อ)

ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2567												ผู้รับผิดชอบ
		ต.ค.66	พ.ย.66	ธ.ค.66	ม.ค.67	ก.พ.67	มี.ค.67	เม.ย.67	พ.ค.67	มิ.ย.67	ก.ค.67	ส.ค.67	ก.ย.67	
2.4 การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน มีการทำข้อตกลงการห้ามเปิดเผยข้อมูล (NDA) และการใช้หรือประมวลผลข้อมูลส่วนบุคคล (DPA)													ศทส.
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร **วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ**														
3.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับ ผู้ใช้งานขาดประสิทธิภาพ	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง/ปรับปรุง/เพิ่มเติม/แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ													ศทส.
3.6 ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตาม เพื่อ Update อย่างสม่ำเสมอ													ศทส.

แผนปฏิบัติการบริหารจัดการความเสี่ยงฯ ประจำปีงบประมาณ พ.ศ. 2567 (ต่อ)

ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2567												ผู้รับผิดชอบ
		ต.ค.66	พ.ย.66	ธ.ค.66	ม.ค.67	ก.พ.67	มี.ค.67	เม.ย.67	พ.ค.67	มิ.ย.67	ก.ค.67	ส.ค.67	ก.ย.67	
	- ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผลทุก 3 เดือน - เช่าบริการศูนย์รับมือและตอบสนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการจ้างเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์													
3.7 ขาดการป้องกันหรือตรวจจับไวรัส	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ													ศทส.
5. ด้านระบบข้อมูล **วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูลต่างๆ ถูกทำลาย จากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน ธรรมชาติหรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยงบูรณาการหรือออกรายงานได้**													
5.2 ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง ปรับปรุง													ศทส.

แผนปฏิบัติการบริหารจัดการความเสี่ยงฯ ประจำปีงบประมาณ พ.ศ. 2567 (ต่อ)

ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2567												ผู้รับผิดชอบ
		ต.ค.66	พ.ย.66	ธ.ค.66	ม.ค.67	ก.พ.67	มี.ค.67	เม.ย.67	พ.ค.67	มิ.ย.67	ก.ค.67	ส.ค.67	ก.ย.67	
- การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี	เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ - ระบุคุณลักษณะทางเทคนิคในการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบภายใต้ขอบเขต												
5.3 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย	- ติดตั้งโปรแกรมป้องกันไวรัสและ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - สำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมออย่างน้อยเดือนละ 1 ครั้ง												ศทส.
5.4 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง (VPN หรือ Virtual Private Network คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมา													ศทส.

แผนปฏิบัติการบริหารจัดการความเสี่ยงฯ ประจำปีงบประมาณ พ.ศ. 2567 (ต่อ)

ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2567												ผู้รับผิดชอบ
		ต.ค.66	พ.ย.66	ธ.ค.66	ม.ค.67	ก.พ.67	มี.ค.67	เม.ย.67	พ.ค.67	มิ.ย.67	ก.ค.67	ส.ค.67	ก.ย.67	
	เพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้) - การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งานทุก 6 เดือน													
5.7 เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง													ศทส.
5.8 การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล													ศทส.
5.9 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่อง และรายงานให้ผู้บริหารทราบ													ศทส.

หมายเหตุ ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปี พ.ศ. 2567 จะเริ่มตั้งแต่ตุลาคม 2566 – กันยายน 2567 (เป็นการควบคุมตามรอบปีงบประมาณประจำปี พ.ศ. 2567)

บทที่ 4

สรุปผลและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากความเสี่ยงที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อมีการปรับเปลี่ยน โดยเทคโนโลยีสารสนเทศและการสื่อสาร เข้ามามีบทบาทสำคัญเป็นกลไกในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีการปรับเปลี่ยน โดยเทคโนโลยีสารสนเทศและการสื่อสารช่วยทำให้ความซ้ำซ้อนของกระบวนการทำงานลดลง และสามารถให้บริการที่รวดเร็ว และการเข้าถึงบริการที่ง่ายขึ้นสะดวกขึ้น ซึ่งในแต่ละวันมีปริมาณข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้กับการปฏิบัติงานของทุกหน่วยงานภายใน สป.พม.

การประเมินความเสี่ยงจากภัยคุกคามไซเบอร์ การบริหารจัดการความเสี่ยงมีบทบาทสำคัญในการปกป้องข้อมูล ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ที่เป็นสินทรัพย์ของ สป.พม. และยังรวมถึงการปกป้อง สป.พม. ให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงของ สป.พม. จะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ที่เหมาะสมและได้มาตรฐานเพื่อปกป้อง สป.พม. จากความเสียหายที่อาจเกิดขึ้นได้

การทบทวนและจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567 เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ หรือความเสี่ยงที่ได้จัดการไปแล้วแต่ยังควบคุมความเสี่ยงต่อ ประกอบการตัดสินใจว่าจะต้องจัดการความเสี่ยง ลดโอกาส/ความเสียหายที่จะเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ จัดการความเสี่ยงจากความเสี่ยงสูง โดยจะต้องมีมาตรการ แนวทาง/กิจกรรมควบคุมเพื่อให้ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ตามสถานการณ์จริง

4.1 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

การระบุความเสี่ยง (Risk Identification) เป็นการบ่งชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่ สป.พม. เผชิญอยู่ จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและ ภัยไซเบอร์ ในปีงบประมาณ พ.ศ. 2567 มีผลคะแนนที่ได้จัดการความเสี่ยง เพื่อควบคุมและจัดทำแผนความเสี่ยง ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยเมื่อมีการจัดการความเสี่ยงและควบคุมความเสี่ยงได้ ระดับความเสี่ยงจะมีค่าคะแนนที่ค่อนข้างต่ำ และ ต่ำ ที่สรุปได้ดังนี้

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับ	
1. ด้านกายภาพและสิ่งแวดล้อม วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อม และผลกระทบที่เกิดขึ้น	1.2	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	1	2	2	- ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS)/แบตเตอรี่สำรองไฟ เป็นประจำทุก 3 เดือน - มีแผนการบำรุงรักษาระบบไฟฟ้าของอาคารสถานที่ ปีละ 1 ครั้ง
	1.4	- มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต - ประตูปิดไม่สนิท - อุปกรณ์ควบคุมการเข้าถึงเสีย	1	3	3	- บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท - ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน
2. ด้านบุคลากร วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	2.1	ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์การเข้าถึงและการใช้งานระบบสารสนเทศ	1	3	3	มีการบริหารจัดการการควบคุมและเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก - การมอบหมายหน้าที่ความรับผิดชอบที่ชัดเจน - การกำกับติดตามการดำเนินงาน
	2.4	การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	1	3	3	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน มีการทำข้อตกลงการห้ามเปิดเผยข้อมูล (NDA) และการใช้หรือประมวลผลข้อมูลส่วนบุคคล (DPA)

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับ	
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้งและไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ	3.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับผู้ใช้งานขาดประสิทธิภาพ	2	2	4	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง/ปรับปรุง/เพิ่มเติม/แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ
	3.6	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	2	3	6	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตาม เพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน - เช่าบริการศูนย์รับมือและตอบสนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการจ้างเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์
	3.7	ขาดการป้องกันหรือตรวจจับไวรัส	2	2	4	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ
5. ด้านระบบข้อมูล วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศฐานข้อมูลต่างๆ ถูกทำลาย จากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน ธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึง	5.2	ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย '- การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อมีการล็อกอินผิดเพื่อป้องกันการโจมตี	2	2	4	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการ เปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับ	
ความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยงบูรณาการหรือออกรายงานได้						- ระบุคุณลักษณะทางเทคนิค ในการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึง เพื่อใช้งานระบบ ภายใต้ขอบเขตงานการพัฒนาระบบสารสนเทศ
	5.3	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย	2	3	6	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - สำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมออย่างน้อยเดือนละ 1 ครั้ง
	5.4	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	2	2	4	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง (VPN หรือ Virtual Private Network คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้) - การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งานทุก 6 เดือน
	5.7	เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	2	2	4	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง
	5.8	การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	2	2	4	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล
	5.9	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	2	2	4	ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่อง และรายงานให้ผู้บริหารทราบ

4.2 สรุปผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

ปีงบประมาณ พ.ศ. 2567 มีแผนการกำหนดกิจกรรม แนวทาง และกำหนดเป้าหมาย/ความสำเร็จ ในการบริหารจัดการความเสี่ยงฯ ทั้งหมด 4 ประเภท รวมจำนวน 13 ปัจจัยเสี่ยง ดังนี้

1) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม ปัจจัยเสี่ยง จำนวน 2 ปัจจัย คือ

รหัส 1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ ระบบฐานข้อมูลเกิดความเสียหายได้ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 8 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 2 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

รหัส 1.4 มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต ประตูปิดไม่สนิท อุปกรณ์ควบคุมการเข้าถึงเสีย ซึ่งความเสียหายที่อาจเกิดขึ้น คือ มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 12 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

2) ความเสี่ยงด้านบุคลากร ปัจจัยเสี่ยง จำนวน 2 ปัจจัย คือ

รหัส 2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึงและการใช้งานระบบสารสนเทศ ทำให้มีความเสี่ยงที่อาจเกิดความเสียหายกับระบบสารสนเทศ ทำให้ระบบสารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูลรั่วไหล ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 8 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

รหัส 2.4 การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน ข้อมูลของหน่วยงานเกิดการรั่วไหล อันเนื่องมาจากผู้รับจ้างประมาทเลินเล่อ ขาดความตระหนักในการดูแลข้อมูลสำคัญระหว่างการบำรุงรักษา/พัฒนาระบบ หน่วยงานได้รับความเสียหายด้านภาพลักษณ์และชื่อเสียง ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 8 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร ปัจจัยเสี่ยง จำนวน 3 ปัจจัย คือ

รหัส 3.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับ ผู้ใช้งานขาดประสิทธิภาพ เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ ระบุตัวตนผู้ใช้งานไม่ได้ หาผู้กระทำความผิดไม่ได้ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลด

ค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.6 ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 25 คือ สูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 6 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.7 ขาดการป้องกันหรือตรวจจับไวรัส เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบเครือข่าย ระบบสารสนเทศและฐานข้อมูล ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

4) ความเสี่ยงด้านระบบข้อมูล ปัจจัยเสี่ยง จำนวน 6 ปัจจัย คือ

รหัส 5.2 ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย การทบทวนสิทธิ์ผู้ใช้งาน การบริหารจัดการรหัสผ่าน การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ ระบุตัวตนผู้ใช้งานได้ไม่ได้ หาผู้กระทำความผิดไม่ได้ การถูกยึดครองระบบจากผู้ไม่หวังดี (Hacker) ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.3 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ใช้บริการทั่วไปไม่มีประสิทธิภาพ ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 25 คือ สูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 6 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.4 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งาน

ที่ทำให้เกิดความเสียหายต่อระบบได้ ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 12 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.7 เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์ ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 12 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.8 การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug) ข้อมูลไม่มีคุณภาพ ไม่สามารถเชื่อมโยงข้อมูลได้ ไม่สามารถออกรายงานได้ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.9 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน ไม่มีข้อมูลในฐานข้อมูล ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

4.3 ข้อเสนอแนะจากผลการสอบทานของกลุ่มตรวจสอบภายใน สป.พม.

สรุปข้อเสนอแนะในปีงบประมาณ พ.ศ. 2566 ของกลุ่มตรวจสอบภายใน สป.พม. เพื่อเป็นแนวทางในการปรับปรุงการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและ ภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2567 ให้มีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้น และไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ดำเนินการ ดังนี้

1. ความเสี่ยงที่ ศทส. เห็นว่าจะต้องมีการจัดการความเสี่ยงและหาแนวทางมาตรการ ควบคุม ป้องกัน แก้ไข เพื่อลดความถี่โอกาสการเกิดความเสี่ยงลดลง มีจำนวน 4 ปัจจัยเสี่ยง ได้แก่

1) การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุกๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพ แนวทางการจัดความเสี่ยงโดยการกำหนดสิทธิ์การเข้าถึงข้อมูล และมีการทบทวน การติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน และกรณีที่มีการเปลี่ยนแปลง โอน ย้าย ลาออก หรือเกษียณอายุ เห็นควรให้ทาง ศทส. ควรประสานข้อมูลทางกองกลาง เพื่อรีบดำเนินการทบทวนสิทธิ์ในทันที เพื่อป้องกันการใช้งานระบบโดยไม่ได้รับอนุญาต

2) การละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) ควรมีการกำหนดสิทธิ์ตัวผู้ใช้โปรแกรม และกำหนดความสำคัญของระบบงาน เพื่อเป็นการควบคุมการใช้งาน การกำหนดผู้ควบคุมการใช้ ป้องกันการสูญหายของข้อมูล

3) การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) การเข้าถึงข้อมูลโดยผู้ที่ไม่มีสิทธิ์หรือ Hacker ควรกำหนดสิทธิ์การเข้าใช้งาน และควรมีการจัดเก็บ log การเข้าถึงระบบงานและข้อมูล

4) ด้านบุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ ควรมีการจัดทำแผนพัฒนาบุคลากรด้านไอที เพื่อให้มีความรู้ความเข้าใจสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

2. กรณีที่ความเสี่ยงลดลงจากเดิม ต้องมีแนวทางการควบคุม มีการกำหนดเกณฑ์การประเมินความเสี่ยงให้ครบถ้วน และควรมีเครื่องมือที่ใช้ในการควบคุมที่ทำให้ความเสี่ยงลดลงอย่างมีนัยสำคัญจนทำให้เปลี่ยนเป็นระดับความเสี่ยงที่ยอมรับได้

3. กรณีที่ระดับความเสี่ยงเพิ่มขึ้นและต้องมีการควบคุมความเสี่ยง ควรมีการเฝ้าระวังและติดตามอย่างต่อเนื่องเพื่อไม่ให้ความเสี่ยงเพิ่มขึ้น หากมีความเสี่ยงเพิ่มขึ้นจะต้องมีการบริหารจัดการในทันที

4. ให้มีการกำหนดแผนปฏิบัติการ โดยมีการกำหนดระยะเวลาเริ่มต้น และระยะเวลาที่ดำเนินการเสร็จสิ้น มีการติดตามผลการปฏิบัติงานตามแผนและรายงานผลการบริหารความเสี่ยงต่อผู้บริหารให้ครบถ้วน

- ภาคผนวก -

บันทึกข้อความ

ส่วนราชการ กลุ่มตรวจสอบภายใน สำนักงานปลัดกระทรวง ฯ โทร. ๐ ๒๒๐๒ ๙๐๖๑

ที่ พม ๐๒๒๓/ ๕๕๐ **วันที่** ๑๖ ตุลาคม ๒๕๖๖

เรื่อง รายงานผลการสอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

เรียน ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๑. เรื่องเดิม

ตามแผนการตรวจสอบ ประจำปีงบประมาณ พ.ศ.๒๕๖๖ กำหนดให้กลุ่มตรวจสอบภายในสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ดำเนินการสอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร นั้น

๒. ข้อเท็จจริง

ตามหนังสือ ที่ พม ๐๒๑๐/ว ๕๕๖ ลงวันที่ ๓๑ มีนาคม ๒๕๖๖ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ได้แจ้งเวียนแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป. พม. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖

๓. ข้อพิจารณา

กลุ่มตรวจสอบภายใน ได้สอบทานแผนบริหารจัดการความเสี่ยงของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ปีงบประมาณ พ.ศ. ๒๕๖๖ โดยทำการวิเคราะห์ ประเมินความเสี่ยง ทบทวนข้อมูลการดำเนินงานความเพียงพอ ความเชื่อถือได้ของแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร จากการสอบทานพบว่ามีการดำเนินการตามแผนฯ ซึ่งมีปัจจัยเสี่ยงทั้งสิ้น ๓๑ ปัจจัยเสี่ยง เป็นความเสี่ยงมีค่าคะแนนการประเมินความเสี่ยงตามรายปัจจัยเสี่ยงคงเดิมจำนวน ๑๘ ปัจจัยเสี่ยง โดยมีการปรับค่าคะแนนจากเดิมจำนวน ๑๓ ปัจจัยความเสี่ยง ประกอบด้วย

๓.๑ การปรับเพิ่มค่าคะแนน ๘ ปัจจัยเสี่ยง ความถี่และโอกาสที่เกิดเพิ่มขึ้น มีค่าคะแนนอยู่ระหว่าง ๔ - ๗ คะแนน ซึ่งอยู่ในระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ และค่าคะแนนการประเมินความเสี่ยงที่มีค่าคะแนนอยู่ในระดับ ๖ เป็นความเสี่ยงที่ทางศูนย์เทคโนโลยีเห็นว่าจะต้องมีการจัดการความเสี่ยงและหาแนวทางมาตรการ ควบคุม ป้องกัน แก้ไข เพื่อลดความถี่โอกาสการความเสี่ยงลดลง จำนวน ๔ ปัจจัยเสี่ยง ได้แก่

๑) การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพกรณีที่ระดับความเสี่ยงเพิ่มขึ้นและต้องมีการควบคุมความเสี่ยงอาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด

กรณีที่ระดับความเสี่ยงเพิ่มขึ้นและแนวทางการจัดความเสี่ยง โดยการกำหนดสิทธิ์การเข้าถึงข้อมูล และมีการทบทวน การติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก ๖ เดือน และกรณีที่มีการเปลี่ยนแปลงโอน ย้าย ลาออก หรือเกษียณอายุ เห็นควรให้ทางศูนย์เทคโนโลยีและการสื่อสารควรประสานข้อมูลทางกองกลางเพื่อรีบดำเนินการทบทวนสิทธิ์ในทันที เพื่อป้องกันการใช้งานระบบโดยไม่ได้รับอนุญาต

๒) ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) นอกจากที่มีแนวทางการควบคุมกำหนดแล้วควรมีการกำหนดสิทธิ์ตัวผู้ใช้โปรแกรม และกำหนดความสำคัญของระบบงาน เพื่อเป็นการควบคุมการใช้งาน การกำหนดผู้ควบคุมการใช้ ป้องกันการสูญหายของข้อมูล

๓) การโจมตี ...

ที่ พม ๐๒๒๓/๙๐๖

เรียน ผอ. ศูนย์เทคโนโยลีสารสนเทศและการสื่อสาร

กลุ่มตรวจสอบภายใน ขอส่งรายงานผลการสอบทานแผนการจัดการความเสี่ยงฯ ของ ศทส.สป.พม. ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ ตามหนังสือ ที่ พม ๐๒๑๐/ว ๕๕๖ ลงวันที่ ๓๑ มีนาคม ๒๕๖๖ มาเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางสาวมีนรดา ค้าสม)
ผู้ตรวจสอบภายในกระทรวง
25 ต.ค. 2566

๓) การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) การเข้าถึงข้อมูลโดยผู้ที่ไม่มีสิทธิ์หรือ Hacker นอกจากมีแนวทางการควบคุมกำหนดแล้ว ควรกำหนดสิทธิการเข้าใช้งาน และควรมีการจัดเก็บ log การเข้าถึงระบบงานและข้อมูล

๔.) ด้านบุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ นอกจากแนวทางควบคุมแล้ว ควรมีการจัดทำแผนพัฒนาบุคลากรด้านไอที เพื่อให้มีความรู้ความเข้าใจสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

๓.๒. การปรับลดค่าคะแนนการประเมินความเสี่ยง ๔ ปัจจัยเสี่ยง ความเสี่ยงที่ลดลงมีแนวทางการควบคุม การที่ความเสี่ยงลดลงจากเดิมต้องมีการกำหนดเกณฑ์การประเมินความเสี่ยงให้ครบถ้วนและระดับความเสี่ยงที่ยอมรับได้ และควรมีเครื่องมือที่ใช้ในการควบคุมที่ทำให้ความเสี่ยงลดลงอย่างมีนัยสำคัญจนทำให้เปลี่ยนเป็นระดับความเสี่ยงที่ยอมรับได้

๓.๓. เพิ่มปัจจัยความเสี่ยงใหม่ ๑ ปัจจัยเสี่ยง การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม ค่าคะแนนการประเมินความเสี่ยงเท่ากับ ๔ ค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับความเสี่ยงค่อนข้างต่ำ ยังอยู่ในระดับที่ยอมรับได้ ตามแนวทางการควบคุมที่กำหนด

๓.๔ กรณีที่ระดับความเสี่ยงเพิ่มขึ้นและต้องมีการควบคุมความเสี่ยง ควรมีการเฝ้าระวังและติดตามอย่างต่อเนื่องเพื่อไม่ให้ความเสี่ยงเพิ่มขึ้น หากมีความเสี่ยงเพิ่มขึ้นจะต้องมีการบริหารจัดการในทันที

๓.๕ เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ประจำปีของศูนย์เทคโนโลยีและการสื่อสาร มีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้นและไม่ก่อให้เกิดผลกระทบต่อการดำเนินงาน ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารควรมีการกำหนดแผนปฏิบัติการมีการกำหนดระยะเวลาเริ่มต้นและระยะเวลาที่ดำเนินการเสร็จสิ้น มีการติดตามผลการปฏิบัติงานตามแผนและรายงานผลการบริหารความเสี่ยงต่อผู้บริหารให้ครบถ้วนต่อไป

๔. <u>ข้อเสนอ</u>

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดลงนามในแบบรายงานสรุปสำหรับผู้บริหารในรายงานผลการสอบทานที่แนบมาพร้อมนี้ด้วยแล้ว

(นางสาวมีนรดา ค้าสม)
ผู้ตรวจสอบภายในกระทรวง

เห็นชอบ-ลงนามแล้ว

(นายอนุกูล ปีดแก้ว)
ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๒๐ ต.ค. ๒๕๖๖

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
ปีงบประมาณ พ.ศ. ๒๕๖๖

๑. ความเป็นมา

ตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๖ กำหนดให้กลุ่มตรวจสอบภายในสอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๒. วัตถุประสงค์ของการตรวจสอบ

๑. เพื่อสอบทานความเชื่อถือได้ และถูกต้องของข้อมูลของการจัดทำแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ว่าเป็นไปตามมาตรฐาน

๒. เพื่อประเมินความมีประสิทธิภาพ ประสิทธิผลของแผนการจัดการบริหารความเสี่ยงด้านสารสนเทศและการสื่อสารศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓. เพื่อประเมินว่ามีการปฏิบัติตามยุทธศาสตร์ นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๔. เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบฐานข้อมูล ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์

๕. เพื่อประเมินความเพียงพอของระบบควบคุมภายใน และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๖. เพื่อให้ความมั่นใจว่าการบริหารจัดการความเสี่ยง สามารถดำเนินการได้ตามแผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้อยู่ในระดับที่ยอมรับได้

๓. ขอบเขตการสอบทานแผนบริหารความเสี่ยง

๑. สอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปี ๒๕๖๖ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. ประเมินความเสี่ยงตามแผนการบริหารจัดการความเสี่ยงอาคารที่ทำการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เลขที่ ๑๐๓๔ ถนนกรุงเกษม แขวงคลองมหานาค เขตป้อมปราบศัตรูพ่าย กรุงเทพมหานคร

๔. ระยะเวลาของการสอบทาน

ระหว่างวันที่ ๑๕ - ๒๙ กันยายน ๒๕๖๖

๕. วิธีการประเมินผลการบริหารความเสี่ยง

๑. ศึกษากฎหมายและระเบียบที่เกี่ยวข้องกับแผนการบริหารจัดการความเสี่ยง

๒. ประเมินผลการบริหารจัดการความเสี่ยงที่ได้ดำเนินการว่าสามารถบรรลุเป้าหมายตามภารกิจหลัก

๓. สอบทานความเพียงพอ ความเชื่อถือได้ของการจัดทำแผนบริหารจัดการความเสี่ยงของกิจกรรมที่ประเมินในปีปัจจุบัน

๔. วิเคราะห์ทบทวนข้อมูล ผลการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงว่าสามารถทำให้ความเสี่ยงที่ยังคงเหลืออยู่นั้นลดลงหรืออยู่ในระดับที่ยอมรับได้

๕. รายงานผลการสอบทาน ความเพียงพอ ความเชื่อถือได้ของการจัดทำแผนบริหารจัดการความเสี่ยง

รายละเอียดวิธีการประเมินผลแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑. ทบทวนเอกสาร (Documentation review)

โดยการรวบรวมและตรวจสอบความเป็นปัจจุบัน ข้อบกพร่องที่สามารถนำไปสู่ความผิดพลาด หรือความไม่เหมาะสมในการควบคุมความมั่นคงปลอดภัยของสารสนเทศ ดังต่อไปนี้

๑) แนวนโยบายด้านความมั่นคงปลอดภัยของสารสนเทศ

๒) การออกแบบระบบเครือข่ายคอมพิวเตอร์

๓) ขั้นตอนการปฏิบัติงานในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์

๔) แผนบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศและระบบเครือข่ายคอมพิวเตอร์

๕) ข้อตกลงหรือสัญญาที่เกี่ยวข้องกับการบำรุงรักษา หรือการเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์

๖) แผนการตอบสนองต่อภัยคุกคามทางระบบเครือข่ายคอมพิวเตอร์ (Incident response Plan)

๒. การสัมภาษณ์ (Interview)

จัดทำข้อคำถามเพื่อสอบถามเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศที่เคยเกิดขึ้นในอดีตผลกระทบที่เคยได้รับ ความถี่ในการเกิดเหตุการณ์ ความสูญเสีย และข้อกังวลเกี่ยวกับความเสี่ยงของระบบและองค์ประกอบของระบบที่อาจเกิดขึ้นในอนาคต เพื่อใช้สัมภาษณ์ผู้ที่เกี่ยวข้อง ได้แก่

๑) เจ้าของระบบงาน (System owner)

๒) ผู้พัฒนาระบบ (System Developer)

๓) ผู้ดูแลระบบ (System custodian)

๔) ผู้ใช้งาน (User)

ผลการสอบทานแผนการจัดการความเสี่ยง

แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๖ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการดำเนินการอย่างต่อเนื่องจากปีงบประมาณที่ผ่านมา โดยที่แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. ๒๕๖๖ ได้นำข้อเสนอแนะจากกลุ่มตรวจสอบภายใน สป.พม. เป็นแนวทางในการดำเนินงานวิเคราะห์ ประเมินความเสี่ยง ทบทวนข้อมูลผลการดำเนินการ ความเพียงพอ ความเชื่อถือได้ของแผนฯ ดังกล่าวเพื่อลดความเสี่ยงในการปฏิบัติงานให้มากยิ่งขึ้น 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

จากการประเมินแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๖ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีปัจจัยความเสี่ยงทั้งสิ้น ๓๑ ปัจจัยเสี่ยง โดยพบว่า

๑. ตารางแสดง**การปรับเพิ่มค่าคะแนน**การประเมินความเสี่ยง ๘ ปัจจัยเสี่ยง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๑.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๑.๒	ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับไฟกระชากจากปลั๊กพ่วง	๑ (เดิม ๑)	๔ (เดิม ๓)	๔ (เดิม ๓)	ควบคุมความเสี่ยง	-ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS) / แบตเตอรี่สำรองไฟ
๒	ครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๒.๒	ขาดมาตรการรองรับในการจัดการฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	๒ (เดิม ๑)	๒ (เดิม ๓)	๔ (เดิม๓)	ควบคุมความเสี่ยง	- มีมาตรการบำรุงรักษาตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุปผลการปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูลและกู้คืนระบบ ในรายการครุภัณฑ์ที่มีความสำคัญ - ทดสอบการโจมตีตามมาตรการที่กำหนด
๓		๒.๓	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ในกรณีที่เกิดความผิดพลาด	๓ (เดิม๑)	๒ (เดิม ๓)	๖ (เดิม ๓)	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก ๖ เดือน โดยการเปลี่ยนแปลง ปรับปรุงเพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ ทุก ๖ เดือน
๔		๒.๕	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๒ (เดิม ๑)	๒ (เดิม ๓)	๔ (เดิม ๓)	ควบคุมความเสี่ยง	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และยืนยันตัวบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา - มีการปรับเพิ่มประสิทธิภาพการบริหารจัดการทุกปี

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง: โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
๕	**ด้านระบบสารสนเทศและฐานข้อมูล**	๓.๑	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) เช่น มีการเจาะระบบเว็บไซต์ของ สนง.พมจ.	๒ (เดิม ๑)	๓ (เดิม ๔)	๖ (เดิม ๔)	จัดการความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัสและ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศทุก ๖ เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - จัดทำการสำรองข้อมูลระบบฐานข้อมูล อย่างสม่ำเสมอ อย่างน้อยสัปดาห์ละ ๑ ครั้ง - จัดทำแผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. ให้สอดคล้องกับสถานการณ์ปัจจุบันอย่างเหมาะสม - การทดสอบการเจาะระบบสารสนเทศที่สำคัญ เพื่อหาช่องโหว่ อย่างน้อยปีละ ๑ ครั้ง - VA scan เพื่อค้นหาช่องโหว่ของระบบปฏิบัติการ ระบบแอปพลิเคชัน และระบบฐานข้อมูล - ปรับปรุง source code เพื่อปิดช่องโหว่ที่ตรวจพบ หมายเหตุ : VPN (Virtual Private Network) ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง: โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
๖	ด้านโปรแกรมคอมพิวเตอร์	๔.๑	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	๓ (เดิม ๑)	๒ (เดิม ๓)	๖ (เดิม ๓)	จัดการความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - จัดทำ และส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย
๗	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯไม่เพียงพอ	๕.๓	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ	๒ (เดิม ๒)	๓ (เดิม ๒)	๖ (เดิม ๔)	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง - มีการจัดทำคู่มือในการปฏิบัติงานเฉพาะด้าน สำหรับผู้ดูแลระบบ เช่น application admin , system admin
๘		๕.๔	ผู้ใช้งาน/users ไม่มีความรู้ความชำนาญและทักษะในการใช้งานระบบ	๒ (เดิม ๑)	๓ (เดิม ๓)	๖ (เดิม ๓)	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีระบบ Call Center/ help desk สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุง หรือตามความต้องการของ User - สร้างความตระหนักถึงประโยชน์ของการนำข้อมูลไปใช้ในการวางแผนและปฏิบัติงาน - กำหนดการใช้งานระบบเป็นตัวชี้วัดหน่วยงานในเชิงคุณภาพ

จะเห็นได้ว่ามีค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับความเสี่ยงที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ การปรับเพิ่มค่าคะแนนความเสี่ยง ๘ ปัจจัยเสี่ยง เป็นความเสี่ยงของความถี่ และโอกาสที่อาจจะเกิดเพิ่มขึ้น ควรหาแนวทางมาตรการ ควบคุม ป้องกัน แก้ไข เพื่อลดความถี่และโอกาสและผลกระทบลดลง

๑) การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพ อาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด

๒) ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)

๓) การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)

๔) บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีฯ ไม่เพียงพอ

๒. ตารางแสดง**การปรับลดค่าคะแนน**การประเมินความเสี่ยง ๔ ปัจจัยเสี่ยง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๑.	ด้านระบบสารสนเทศและฐานข้อมูล	๓.๕	เกิดช่องโหว่ของซอฟต์แวร์และไม่ได้รับการอัปเดต	๑ (เดิม ๒)	๔ (เดิม ๓)	๔ (เดิม ๖)	จัดการความเสี่ยง	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอและมีการกำหนดไว้ใน TOR ในการบำรุงรักษาระบบสารสนเทศ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้งานได้รับทราบอย่างต่อเนื่อง - ดำเนินการปรับปรุง version ของระบบปฏิบัติการและบริการของระบบสารสนเทศให้เป็นปัจจุบัน
๒.	ด้านโปรแกรมคอมพิวเตอร์	๔.๒	ขาดการป้องกันหรือตรวจจับ Malware	๑ (เดิม ๑)	๔ (เดิม ๕)	๔ (เดิม ๕)	ควบคุมความเสี่ยง	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ - จัดทำ VLAN เพื่อแบ่งเครือข่ายออกเป็นกลุ่มย่อย - ส่งเสริมให้บุคลากรมีการสำรองข้อมูลที่สำคัญในเครื่อง PC ของตนเองอย่างสม่ำเสมอ
๓	ด้านงบประมาณ	๖.๑	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด	๔ (เดิม ๒)	๑ (เดิม ๓)	๔ เดิม ๖)	จัดการความเสี่ยง	- ปรับโครงการโดยจัดลำดับความสำคัญใหม่ ลดขอบเขตงานลง - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ - บริหารจัดการงบประมาณภายในหน่วยงานให้มีประสิทธิภาพ

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง: โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
๔	ด้านการบริหารจัดการ	๗.๒	แผนเตรียมความพร้อมกรณีฉุกเฉินไม่ครอบคลุมกับสถานการณ์ที่เกิดขึ้น เช่น กรณีเกิดสถานการณ์ ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑ (เดิม ๑)	๓ (เดิม ๕)	๓ (เดิม ๕)	ควบคุมความเสี่ยง	- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และทบทวนแผนฯ อย่างน้อยปีละ ๑ ครั้ง - มอบหมายผู้รับผิดชอบ และดำเนินการตามแผนฯ อย่างเคร่งครัด

การปรับลดค่าคะแนนการประเมินความเสี่ยง ๔ ปัจจัยเสี่ยง จากตารางจะเห็นได้ว่าเมื่อมีการปรับค่าคะแนนความเสี่ยงลง เพิ่มแนวทางการควบคุมความเสี่ยง มีค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๓ ระดับความเสี่ยงต่ำ ในลำดับที่ ๔ และปัจจัยเสี่ยงในลำดับที่ ๑ ๒ และ ๓ มีค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้

๓. ตารางแสดงการเพิ่มใหม่ค่าคะแนนการประเมินความเสี่ยง ๑ ปัจจัยเสี่ยง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง: โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
๑.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๑.๕	ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะ ต่ออุปกรณ์ที่ติดตั้งภายในห้องไฟฟ้าสื่อสารตามชั้นต่าง ภายในอาคาร และพื้นที่สำนักงาน	๒	๒	๔	ควบคุมความเสี่ยง	- มีการฉีดยาป้องกันแมลงบริเวณภายในอาคารเป็นประจำ - ตรวจสอบและบำรุงรักษาอุปกรณ์อย่างต่อเนื่อง - จัดพื้นที่สำหรับรับประทานอาหารให้เป็นสัดส่วน

จะเห็นได้ว่า มีการเพิ่มปัจจัยความเสี่ยง ๑ ปัจจัยเสี่ยง จะเห็นได้ว่าค่าคะแนนการประเมินความเสี่ยงเท่ากับ ๔ ค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับความเสี่ยงค่อนข้างต่ำ ยังอยู่ในระดับที่ยอมรับได้ เป็นไปตามแนวทางที่กำหนด

สำหรับปัจจัยเสี่ยงอื่นที่มีค่าคะแนนการประเมินความเสี่ยงตามรายปัจจัยเสี่ยงคงเดิม จำนวน ๑๘ ปัจจัยเสี่ยง เป็นการคงค่าคะแนนในกิจกรรมที่ไม่สามารถลดค่าคะแนนลงได้ เนื่องจากเป็นความเสี่ยงจากการทำงานในลักษณะคงที่ จึงไม่ก่อให้เกิดปัจจัยเสี่ยงที่จำส่งผลกระทบต่อการดำเนินงานและในบางปัจจัยเสี่ยงมีการเพิ่มเติมหรือปรับเปลี่ยนแนวทางการควบคุม สรุปเป็นตารางได้ ดังนี้

๔. ตารางแสดงค่าคะแนนการประเมินความเสี่ยงคงที่ จำนวน ๑๘ ปัจจัยเสี่ยง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๑.	การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม	๑.๑	ไฟไหม้ห้องศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์	๑	๕	๕	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งาน และตรวจสอบระบบดับเพลิงอัตโนมัติ โดยการจ้างบริษัทดำเนินการบำรุงเนื่องจากความเชี่ยวชาญเฉพาะด้าน
๒		๑.๓	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	๑	๓	๓	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น และมีการตรวจสอบสภาพแวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ
๓		๑.๔	ไม่มีการกำหนดสิทธิ์และไม่ควบคุมการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	๑	๓	๓	ควบคุมความเสี่ยง	บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการ ในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง
๔	การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๒.๑	ขาดการทบทวน/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร ให้เป็นปัจจุบัน	๑	๓	๓	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์
๕		๒.๔	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	๑	๓	๓	ควบคุมความเสี่ยง	- ระบุข้อกำหนด/ข้อตกลง ระดับการให้บริการที่ชัดเจนกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบหรือ ผอ. ศทส. ทุกครั้งที่ระบบฯ ขัดข้องเพื่อให้แก้ปัญหาได้ทันท่วงที

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๖	การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๒.๖	ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์ เจาะหรือลักลอบ (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
๗		๓.๒	ไม่มีการดำเนินการตามแผนการสำรองและทดสอบกู้คืนข้อมูล	๑	๕	๕	ควบคุมความเสี่ยง	- จัดทำการสำรองข้อมูลแบบอัตโนมัติโดยจัดเก็บ Storage ทุกวัน เฉพาะส่วนที่เพิ่มในแต่ละวัน และจัดเก็บข้อมูลทั้งระบบแบบ Full Backup บน Storage สัปดาห์ละ ๑ ครั้ง - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติโดยจัดเก็บใน Hard Disk เป็นประจำทุกเดือน - มีการทดสอบการกู้คืนข้อมูลของทุกระบบงานอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการเตรียมความพร้อมหากเกิดสถานการณ์ฉุกเฉิน - มีการควบคุมกำกับการสำรองข้อมูลให้เป็นไปตามแผนพร้อมทั้งการตรวจสอบความสมบูรณ์ในการสำรองข้อมูลทุกครั้ง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
				โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)		
๘		๓.๓	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๕	๕	ควบคุมความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึงระบบเครือข่าย - ทบทวน/กำหนดสิทธิ์ VPN ในการเข้าถึงระบบเครือข่ายจากระยะไกล เช่น กำหนดช่วงเวลาในการเข้าใช้ VPN อย่างน้อยปีละ ๑ ครั้ง - มีการกำหนดเงื่อนไขการเข้าใช้งานที่ไม่ถูกต้อง เช่น จำกัดจำนวนครั้งของการผิดพลาดในการเข้าใช้งาน เป็นต้น - มีการติดตาม/ตรวจสอบ การเข้าใช้งานของผู้ใช้งานอย่างสม่ำเสมอ
๙		๓.๔	การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์	๑	๓	๓	ควบคุมความเสี่ยง	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์ และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตามทุกขั้นตอนของการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐาน และ TOR
๑๐	การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๓.๖	ขาดการบำรุงรักษาโปรแกรม หรือระบบงานอย่างต่อเนื่อง	๑	๕	๕	จัดการความเสี่ยง	- จัดทำแผนการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่องเพื่อปิดช่องโหว่โดยการอัปเดตเวอร์ชันใหม่ๆ อย่างสม่ำเสมอ ทำให้สามารถใช้งานระบบได้อย่างต่อเนื่องและในเวลาที่ต้องการได้ - จัดทำ TOR ในการจัดซื้อจัดจ้างการพัฒนาระบบให้ครอบคลุมถึงการอบรมให้ความรู้ในการแก้ไขปัญหา เมื่อระบบขัดข้อง พร้อมทั้งส่งคู่มือระบบการใช้งานและแก้ไขปัญหาให้กับผู้ดูแลระบบ

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง: โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
๑๑		๓.๗	การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	๑	๓	๓	ควบคุมความเสี่ยง	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม(Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - รวบรวมข้อผิดพลาดที่เกิดขึ้น และปรับปรุงระบบให้สามารถป้องกันการนำเข้าข้อมูลที่ผิดพลาดได้
๑๒		๓.๘	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	๑	๓	๓	ควบคุมความเสี่ยง	- ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ - กำหนดนโยบายในการนำเข้าข้อมูล - กำหนดตัวชี้วัด - กำหนดรายการข้อมูลที่สำคัญ - พัฒนาระบบให้ตรงตามความต้องการของผู้ใช้งาน - ประสานความร่วมมือกับผู้รับผิดชอบหลักในการบันทึกข้อมูล
๑๓		๓.๙	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	๑	๒	๒	ควบคุมความเสี่ยง	- มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลางกระทรวง พม. อย่างต่อเนื่อง - มีการติดตามการนำมาตรฐานข้อมูลกลางกระทรวง พม. ไปใช้อย่างสม่ำเสมอ - มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) - มีการดำเนินงานทบทวน/ปรับปรุงและเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลาง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
								กระทรวง พม. ที่ครอบคลุมภารกิจของกระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ
๑๔	การควบคุมครุภัณฑ์และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๓.๑๐	ไม่มีบัญชีการเข้าถึงระบบปฏิบัติการ (Operating System) และโปรแกรมประยุกต์ (Applications)	๑	๓	๓	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์ในการเข้าถึง เพื่อทำการจำกัดและควบคุมการเข้าถึง - ใช้งานโปรแกรมเพื่อป้องกันการละเมิดโดยการตรวจสอบสิทธิ์ - มีการทบทวนสิทธิ์เป็นประจำ โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ อย่างน้อยปีละ ๑ ครั้ง - ปฏิบัติตามข้อปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. อย่างเคร่งครัด
๑๕	ด้านบุคลากร	๕.๑	มีการใช้บัญชีผู้ใช้งาน (username) ร่วมกัน ในการเข้าถึงระบบสารสนเทศและยืนยันตัวตนอินเทอร์เน็ต	๑	๓	๓	ควบคุมความเสี่ยง	- ปฏิบัติตามข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม. โดยใช้แบบฟอร์มการขอใช้งานบัญชีผู้ใช้งาน เพื่อการจัดเก็บ Log ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ - ส่งเสริมให้ผู้ใช้งานตระหนักถึงโทษตาม พ.ร.บ.คอมพิวเตอร์ฯ และความเสียหายที่จะเกิดขึ้น - ทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศและอินเทอร์เน็ตอย่างน้อยปีละ ๑ ครั้ง

ลำดับที่	กิจกรรม	รหัสปัจจัยเสี่ยง	ปัจจัยเสี่ยง	ค่าคะแนนการประเมินความเสี่ยง โอกาสความถี่ (๑)	ผลกระทบความรุนแรง (๒)	ระดับคะแนน (๑)x(๒)	กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม
๑๖		๕.๒	การจ้างบุคคลภายนอกที่ขาดความรู้ความชำนาญ ความเชี่ยวชาญในการดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓	ควบคุมความเสี่ยง	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน - มีการจัดทำแผนงานขั้นตอนการทำงานที่ชัดเจน และควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้ - มีการติดตามเพื่อป้องกันการเกิดข้อผิดพลาดและแก้ไขปัญหาได้ทันที โดยมีการประชุมทุกสัปดาห์
๑๗		๕.๕	ผู้ใช้งาน (Users) ใช้คอมพิวเตอร์/เครือข่ายผิดวัตถุประสงค์	๑	๓	๓	ควบคุมความเสี่ยง	- มีนโยบายและแนวทางในการควบคุมการใช้คอมพิวเตอร์ ไม่ให้ใช้เครือข่ายผิดวัตถุประสงค์ - ควบคุมและบังคับใช้อย่างเคร่งครัด พร้อมทั้งกำหนดบทลงโทษ - จัดหาอุปกรณ์ตรวจสอบการเข้าถึงเครือข่ายและตรวจสอบระบบเครือข่ายอย่างสม่ำเสมอ
๑๘	**ด้านการบริหารจัดการ**	๗.๑	ความเสี่ยงจากการจัดซื้อจัดจ้าง - กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคาได้ - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา - ผู้รับจ้างไม่ปฏิบัติตามข้อกำหนด	๑	๓	๓	จัดการความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการ - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนด โดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสม เพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด

จากตารางจะเห็นได้ว่าปัจจัยเสี่ยงในลำดับที่ ๑ ๖ ๗ ๘ และ ๑๐ มีค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับความเสี่ยงอยู่ในระดับที่ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ซึ่งไม่ก่อให้เกิดปัจจัยเสี่ยงที่จะส่งผลกระทบต่อการดำเนินงานและในบางปัจจัยเสี่ยงมีการเพิ่มเติมหรือปรับเปลี่ยนแนวทางการควบคุมความเสี่ยง เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ ซึ่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสารควรดำเนินการตามแนวทางการควบคุมความเสี่ยงอย่างต่อเนื่อง

ข้อเสนอแนะ

เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๖ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้นและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.พม.ดำเนินการ ดังนี้

๑. การปรับเพิ่มค่าคะแนน ๘ ปัจจัยเสี่ยง โอกาสความถี่ที่เกิดเพิ่มขึ้น มีค่าคะแนนอยู่ในช่วงเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ และค่าคะแนนการประเมินความเสี่ยงที่มีค่าคะแนนอยู่ในระดับ ๖ เป็นความเสี่ยงที่จะต้องมีการจัดการความเสี่ยงและหาแนวทางมาตรการ ควบคุม ป้องกัน แก้ไข เพื่อลดโอกาสความถี่ลดลง จำนวน ๔ ปัจจัยเสี่ยง ได้แก่

๑) การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารในทุก ๆ ระดับผู้ใช้งานระบบ/ผู้ดูแลระบบขาดประสิทธิภาพกรณีที่ระดับความเสี่ยงเพิ่มขึ้นและต้องมีการควบคุมความเสี่ยงอาทิ การไม่สามารถตรวจสอบหรือระบุตัวตนผู้ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศได้ ในกรณีที่เกิดความผิดพลาด

กรณีที่ระดับความเสี่ยงเพิ่มขึ้นและแนวทางการจัดความเสี่ยง โดยการกำหนดสิทธิ์การเข้าถึงข้อมูล และมีการทบทวน การติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก ๖ เดือน และกรณีที่มีการเปลี่ยนแปลงโอน ย้าย ลาออก หรือเกษียณอายุ เห็นควรให้ทางศูนย์เทคโนโลยีและการสื่อสารควรประสานข้อมูลทางกองกลางเพื่อรีบดำเนินการทบทวนสิทธิ์ในทันที เพื่อป้องกันการใช้งานระบบโดยไม่ได้รับอนุญาต

๒) ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program) นอกจากที่มีแนวทางการควบคุมกำหนดแล้วควรมีการกำหนดและป้องกันการสูญหายของข้อมูล สิทธิ์ตัวผู้ใช้โปรแกรมเพื่อใช้ควบคุมการใช้งานและป้องกันการสูญหายของข้อมูล มีการกำหนดความสำคัญของระบบงานเพื่อกำหนดผู้ควบคุมการใช้งาน

๓) การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) การเข้าถึงข้อมูลโดยผู้ที่ไม่มีสิทธิ์ นอกจากมีแนวทางการควบคุมแล้ว และควรมีการจัดเก็บ log การเข้าถึงระบบงานและข้อมูล

๔.) ด้านบุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ นอกจากแนวทางควบคุมแล้ว ควรมีการจัดทำแผนพัฒนาบุคลากรด้านไอที

๒. การปรับลดค่าคะแนนการประเมินความเสี่ยง ๔ ปัจจัยเสี่ยง ความเสี่ยงที่ลดลงมีแนวทางการควบคุม การที่ความเสี่ยงลดลงจากเดิมต้องมีการกำหนดเกณฑ์การประเมินความเสี่ยงให้ครบถ้วนและระดับความเสี่ยงที่ยอมรับได้ และควรมีเครื่องมือที่ใช้ในการควบคุมที่ทำให้ความเสี่ยงลดลงอย่างมีนัยสำคัญจนทำให้เปลี่ยนเป็นระดับความเสี่ยงที่ยอมรับได้

๓. เพิ่มปัจจัยความเสี่ยงใหม่ ๑ ปัจจัยเสี่ยง การรักษาความปลอดภัยด้านกายภาพและสิ่งแวดล้อม ค่าคะแนนการประเมินความเสี่ยงเท่ากับ ๔ ค่าคะแนนการประเมินความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ซึ่งอยู่ในระดับความเสี่ยงค่อนข้างต่ำ ยังอยู่ในระดับที่ยอมรับได้ ตามแนวทางการควบคุมที่กำหนด

๔. กรณีที่ระดับความเสี่ยงเพิ่มขึ้นและต้องมีการควบคุมความเสี่ยง ควรมีการเฝ้าระวังและติดตามอย่างต่อเนื่องเพื่อไม่ให้ความเสี่ยงเพิ่มขึ้น หากมีความเสี่ยงเพิ่มขึ้นจะต้องมีการบริหารจัดการในทันที

๕. เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ประจำปีของศูนย์เทคโนโลยีและการสื่อสาร มีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้นและไม่ก่อให้เกิดผลกระทบต่อการดำเนินงาน ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารควรมีการกำหนดแผนปฏิบัติการ มีการกำหนดระยะเวลาเริ่มต้นและระยะเวลาที่ดำเนินการเสร็จสิ้น มีการติดตามผลการปฏิบัติงานตามแผนและรายงานผลการบริหารความเสี่ยงต่อผู้บริหารให้ครบถ้วนต่อไป

คำสั่งผู้บริหาร	ผู้สอบทานและรายงาน
ชื่อ	ลงชื่อ.....
(นายอนุกูล ปีดแก้ว)	(นางสาวมีนรดา ค้าสม)
ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์	ผู้ตรวจสอบภายในกระทรวง

ICTC MSDHS ศทส. WU.
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์