

ความเสี่ยง

ด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.





สารบัญ

เรื่อง	หน้า
บทที่ 1 : บทนำ	
1.1 หลักการและเหตุผล	1
1.2 วัตถุประสงค์การจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์	1
1.3 เป้าหมายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์	2
1.4 ขอบเขตการดำเนินงาน	2
1.5 ประโยชน์ที่คาดว่าจะได้รับ	2
บทที่ 2 : การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์	
2.1 ความรู้เกี่ยวกับการบริหารความเสี่ยง	3
2.2 สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและการสื่อสาร	6
2.3 กระบวนการบริหารความเสี่ยง	7
2.4 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.	11
2.5 ความเสี่ยงจากภัยคุกคามไซเบอร์	12
2.6 การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์	14
2.7 การตอบสนองความเสี่ยง	14
2.8 ปัจจัยเสี่ยง	15
2.9 การประเมินความเสียหาย	16
2.10 การติดตามและรายงานผล	16
2.11 ระบบรักษาความปลอดภัยบนเครือข่าย	16
บทที่ 3 : การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.	
3.1 แนวทางและขั้นตอนการบริหารความเสี่ยง	18
3.2 กระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.	19
3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.	20
3.4 ผลการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2567	21
3.5 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568	31



สารบัญ (ต่อ)

เรื่อง	หน้า
3.6 การประเมินแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568	37
3.7 การจัดทำแผนภูมิความเสี่ยง (Risk Map) ก่อนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยไซเบอร์	45
3.8 การจัดทำแผนภูมิความเสี่ยง (Risk Map) หลังการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยไซเบอร์	45
3.9 แผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568	47

บทที่ 4 : สรุปผลและข้อเสนอแนะ

4.1 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568	54
4.2 สรุปผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2568	59
4.3 ข้อเสนอแนะจากผลการสอบทานของกลุ่มตรวจสอบภายใน สป.พม.	62



บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (สป.พม.) ประจำปีงบประมาณ พ.ศ. 2568 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ โดยให้ความสำคัญในการบริหารจัดการความเสี่ยง เป็นเครื่องมือสำคัญตามหลักการกำกับดูแลกิจการที่ดีช่วยในการบริหารและการตัดสินใจ การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายต่อองค์กร การเปลี่ยนแปลง กระบวนการทำงานโดยการนำเทคโนโลยีสารสนเทศและการสื่อสาร เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การจัดการฐานข้อมูล การใช้เครื่องคอมพิวเตอร์และอุปกรณ์ การใช้เครือข่ายคอมพิวเตอร์และการสื่อสาร และการติดต่อสื่อสารผ่านระบบเครือข่าย ทั้งนี้ ภายใต้วิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศและการสื่อสารล้วนมีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการทำงานหรือเป้าหมายขององค์กร

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

1.2 วัตถุประสงค์การจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

- 1) เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ สป.พม. รวมถึงการถูกโจมตีจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น
- 2) เพื่อให้มีการปฏิบัติตามกฎระเบียบ หรือนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ ของ สป.พม. อย่างมีระบบ และต่อเนื่อง มีแผนงานที่สามารถแก้ไขสถานการณ์ได้ทัน่วงทีกรณีเกิดสถานการณ์ฉุกเฉิน เช่น แผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม. และแผนเตรียมความพร้อมกรณีฉุกเฉิน สป.พม. เป็นต้น
- 3) เพื่อให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการมอบหมายเจ้าหน้าที่ผู้รับผิดชอบในการปฏิบัติงานให้มีประสิทธิภาพตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ ของ สป.พม. ให้บรรลุเป้าหมาย เกิดผลการปฏิบัติงานและการป้องกันความเสียหายของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร



4) เพื่อเป็นแนวทางในการดำเนินงาน การกำกับดูแล การมอบหมาย การติดตามงาน การตรวจทานและประเมินความเสี่ยง ตลอดจนมีการเผยแพร่และประชาสัมพันธ์ผ่านช่องทางเว็บไซต์ ระบบ Intranet และช่องทางอื่น ๆ ของ สป.พม. เพื่อให้เกิดความเข้าใจระหว่างผู้ปฏิบัติและผู้บริหาร ในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ของ สป.พม.

1.3 เป้าหมายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

ศทส. สป.พม. มีแผนสำหรับดำเนินการเพื่อจัดการความเสี่ยง ดังนี้

- 1.3.1 มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.
- 1.3.2 มีแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- 1.3.3 มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.
- 1.3.4 มีแผนการสำรองและทดสอบกู้คืนข้อมูล สป.พม.
- 1.3.5 มีแผนการเตรียมความพร้อมกรณีฉุกเฉิน สป.พม.

1.4 ขอบเขตการดำเนินงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สป.พม. เรื่อง การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ และการตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ดำเนินการโดยคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. สป.พม. มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสารสนเทศ ระบบฐานข้อมูลและการจัดเก็บข้อมูล
2. สป.พม. มีแนวทางในการดูแล บำรุงรักษา ระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีเสถียรภาพและมีความพร้อมใช้งานอย่างต่อเนื่อง



บทที่ 2

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

2.1 ความรู้เกี่ยวกับการบริหารความเสี่ยง

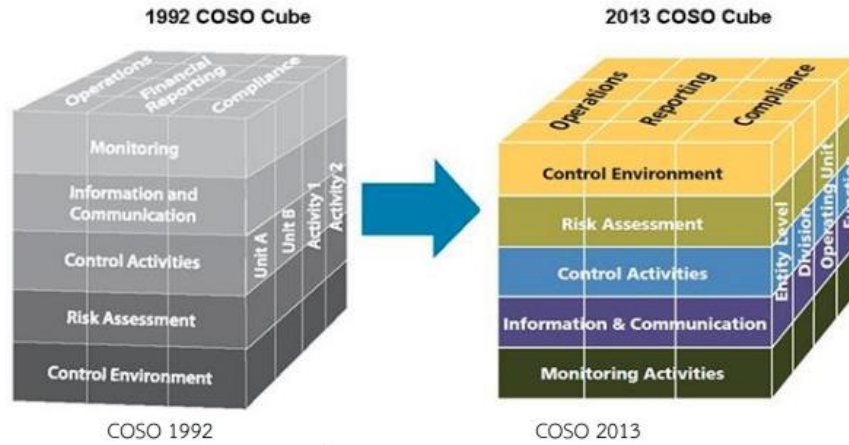
เป็นการรวบรวมข้อมูล และรายละเอียดที่เกี่ยวข้องกับการบริหารความเสี่ยงตามมาตรฐานของ COSO (The Committee of Sponsoring Organization of the Tread way Commission) กระบวนการบริหารความเสี่ยง รวมถึงการจัดทำรายงานด้านการบริหารความเสี่ยง ซึ่งแบ่งออกเป็น 2 ส่วน คือรายงานแผนบริหารความเสี่ยง และ รายงานผลประเมินระบบการควบคุมภายใน

การบริหารความเสี่ยงตามมาตรฐาน COSO ประวัติความเป็นมาของ COSO เริ่มจากเหตุการณ์วิกฤตทางการเมืองและเศรษฐกิจของสหรัฐอเมริกา ปี 1970 - 1977 สหรัฐอเมริกาได้ประกาศกฎหมายแนวปฏิบัติเกี่ยวกับความไม่สุจริตในการให้สินบนชาวต่างชาติ (the 1977 Foreign Corrupt Practices Act-FCPA) ซึ่งมีการกำหนดเรื่องการควบคุมภายในเป็นสาระสำคัญในประกาศดังกล่าว

- ปี 1985 (ตุลาคม) จัดตั้งองค์กรอิสระ คือ คณะกรรมการเพื่อบริหารงานการทุจริตแห่งชาติ (National Commission on Fraudulent Financial reporting หรือ Tread way)
- ปี 1987 คณะกรรมการเพื่อบริหารงานการทุจริตแห่งชาติได้รับการสนับสนุนจากคณะกรรมการวิชาชีพอิสระอื่นๆ จัดตั้ง The Committee of Sponsoring Organization of the Tread way Commission (COSO)
- ปี 1992 COSO เผยแพร่แนวคิดการควบคุมภายใน COSO Internal Control-integrated Framework กำหนดความหมายและกรอบโครงสร้างการควบคุมภายใน
- ปี 2004 COSO ได้พัฒนาแนวทางการบริหารความเสี่ยง ที่มีมาตรฐานสากลมากขึ้นเพื่อให้องค์กรสามารถใช้เป็นแนวปฏิบัติด้านการบริหารความเสี่ยง
- ปี 2013 COSO เริ่มประกาศให้ทราบถึงการปรับปรุง COSO 1992 ตั้งแต่ปลายปี 2010 และประกาศอย่างเป็นทางการในปี 2013 และใช้เวอร์ชันใหม่เป็นหลักตั้งแต่ 14 ธันวาคม 2014



กระบวนการควบคุมภายในระดับองค์กร



ที่มา : The Committee of Sponsoring Organization of the Tread way Commission (COSO)

การควบคุมภายใน COSO 2013 มีขั้นตอนที่สำคัญ ดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)
2. การประเมินความเสี่ยง (Risk Assessment)
3. กิจกรรมควบคุม (Control Activities)
4. ข้อมูลและการติดต่อสื่อสาร (Information and Communication)
5. การติดตาม (Monitoring)





องค์ประกอบของการบริหารความเสี่ยง ERM (Enterprise Risk Management)



องค์ประกอบของการบริหารความเสี่ยง ERM (Enterprise Risk Management) ประกอบด้วยองค์ประกอบ 8 ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment) สภาพแวดล้อมขององค์กร เป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการบริหารความเสี่ยงและเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางปฏิบัติงานของบุคลากร กระบวนการทำงาน ระบบสารสนเทศ เป็นต้น

2. การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม

3. การระบุความเสี่ยง (Risk Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอกองค์กร และเมื่อเกิดขึ้นแล้วส่งผลให้องค์กร ไม่บรรลุวัตถุประสงค์ หรือเป้าหมาย เช่น นโยบายการบริหารงาน บุคลากร การปฏิบัติงานการเงิน ระบบ สารสนเทศ ระเบียบข้อบังคับ เป็นต้น ทั้งนี้ เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้นๆ และเพื่อให้ ผู้บริหารพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้เป็นอย่างดี

4. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นการวัดระดับความรุนแรงของความเสี่ยง เพื่อพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)



5. การตอบสนองความเสี่ยง (Risk Response) เป็นการดำเนินการหลังจากที่องค์กรสามารถระบุความเสี่ยงขององค์กรและประเมินระดับของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการเพื่อลด โอกาสที่จะเกิดความเสี่ยงและลดระดับความรุนแรงของผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ด้วยวิธีจัดการความเสี่ยงที่เหมาะสมที่สุดและคุ้มค่ากับการลงทุน

6. กิจกรรมควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่างๆ เพื่อช่วยลด หรือควบคุมความเสี่ยง เพื่อสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้อง และทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ป้องกันและลดระดับความเสี่ยงให้อยู่ในระดับที่ องค์กรยอมรับได้

7. สารสนเทศและการสื่อสาร (Information and Communication) องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไป ตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

8. การติดตามประเมินผล (Monitoring) องค์กรจะต้องมีการติดตามผล เพื่อให้ทราบถึงผลการดำเนินงานว่าเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

2.2 สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและการสื่อสาร

สป.พม. มีครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) อุปกรณ์ป้องกันการโจรกรรมข้อมูลจากบุคคลภายนอก (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) เพื่อเฝ้าระวังไม่ให้เกิดการโจมตีเครือข่ายและอุปกรณ์ที่สำคัญ อีกทั้งยังมีการทำ DR Site หรือ Disaster Recovery Site สำรองข้อมูลในกรณีระบบหลักเกิดความเสียหาย



สำหรับระบบสารสนเทศของ สป.พม. ที่ให้บริการ ประกอบด้วย ระบบสมุดปกครอบครัวยุติธรรมอิเล็กทรอนิกส์ (MSO-Logbook) ระบบฐานข้อมูลกลางผู้รับสวัสดิการ พม. (DB Center) ระบบติดตามการให้บริการ พม. สถิติด้านสังคม (STAT INFO) สถิติพื้นฐานของการพัฒนามนุษย์ ระบบ Protect U ระบบการแจ้งเหตุด่วนเหตุร้ายแจ้งปัญหาสังคม และขอรับบริการ ระบบเยียวยาผู้ได้รับผลกระทบจากเหตุการณ์ชายแดนใต้ เป็นต้น

นอกจากนี้ยังมีระบบ Back office ที่สนับสนุนการปฏิบัติงานของบุคคลกร ประกอบด้วย ระบบทำเนียบหน่วยงาน (Directory) ระบบติดตามและประเมินผล Tracking and budgeting system ระบบแบบฟอร์มออนไลน์ (e-form) ระบบการขอใช้ทรัพยากร (E-reservation) ระบบเวลาปฏิบัติราชการด้วยลายนิ้วมือ ระบบอินทราเน็ต (Intranet) ระบบบัญชีเงินกองทุน (funds) ระบบงานพัฒนาระบบบริหาร เป็นต้น

2.3 กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุความเสี่ยง วิเคราะห์ ประเมินและจัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือองค์กร การบริหารจัดการความเสี่ยง รวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสมครอบคลุม 5 ขั้นตอน ดังนี้

1. การระบุความเสี่ยงหรือปัจจัยเสี่ยง เป็นกระบวนการที่คณะทำงานฯ และผู้ปฏิบัติงานที่เกี่ยวข้องร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องของโครงการหรือกิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายในและภายนอกองค์กร วิธีการระบุความเสี่ยง มีหลายวิธี เช่น

1. การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
2. การใช้ Checklist
3. การวิเคราะห์สถานการณ์จากการตั้งคำถาม What-if
4. การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

ในขั้นตอนนี้ มีการเก็บข้อมูลความเสี่ยงที่เกิดขึ้นในรูปแบบของความเสี่ยงของการเกิดความสูญเสียและความรุนแรงของความเสี่ยง รวมทั้งข้อมูลการดำเนินงานใดๆ เพื่อลดความเสี่ยงที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จและปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

2. การวิเคราะห์และประเมินความเสี่ยง การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมินและการจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

1. การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสียหาย (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) ซึ่งคณะทำงานฯ ต้องกำหนดเกณฑ์ขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่ก่อให้เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ ได้แก่ สูงมาก (รุนแรงมากที่สุด) สูง (ค่อนข้างรุนแรง) ปานกลาง น้อย และน้อยมาก ส่วนระดับของความเสี่ยงอาจกำหนดเป็น 4 ระดับ (สูง ค่อนข้างสูง ค่อนข้างต่ำ และต่ำ)



2. การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้น และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยง ซึ่งแต่ละความเสี่ยงก็จะมี ความรุนแรงต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงจะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น ดังตัวอย่างที่ยกมาประกอบนี้

เกณฑ์การประเมินผลกระทบ (ความน่าเชื่อถือ/ความพึงพอใจของผู้ใช้บริการ) ดังนี้

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

เกณฑ์การประเมินโอกาสของการประเมินความเสี่ยง ดังนี้

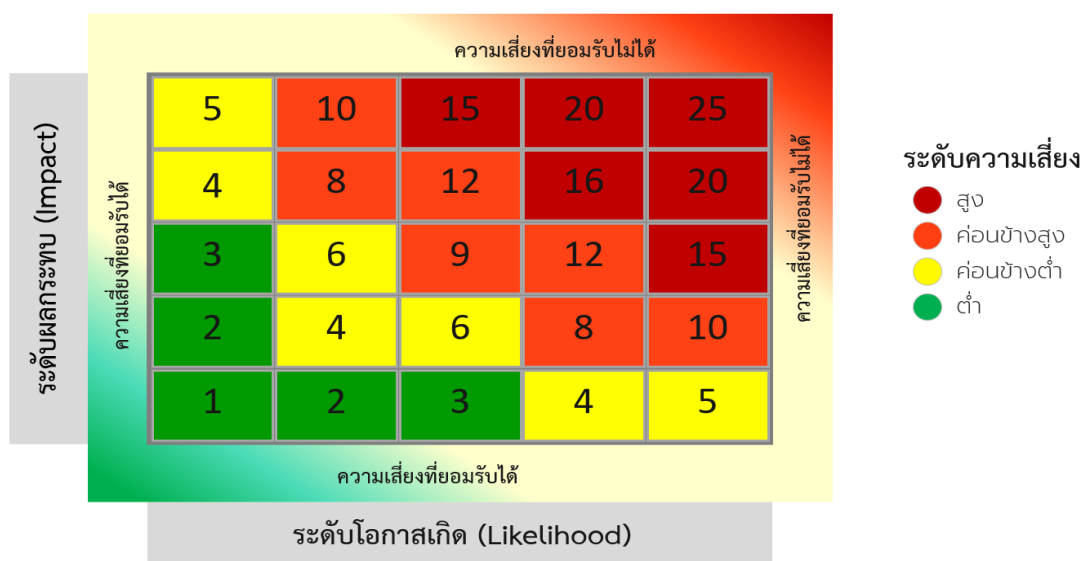
โอกาสที่จะเกิด	ความถี่ที่เกิดขึ้นของความเสี่ยง		ระดับคะแนน
	เชิงคุณภาพ	เชิงปริมาณ	
สูงมาก	มีโอกาสเกิดบ่อยมากเกือบทุกวัน	มากกว่า 1 ครั้งต่อเดือน	5
สูง	มีโอกาสเกิดค่อนข้างสูงหรือบ่อยๆ ทุกเดือน	ระหว่าง 1 - 6 เดือนต่อครั้ง	4
ปานกลาง	มีโอกาสในการเกิดบางครั้ง (ทุกปี)	ระหว่าง 6 - 12 เดือนต่อครั้ง	3
น้อย	อาจมีโอกาสดังกล่าว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



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 -



4. การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณา กำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ แล้วเลือกความเสี่ยงที่มีระดับสูงหรือค่อนข้างสูงมาจัดทำแผนบริหารจัดการความเสี่ยง



3. การกำหนดมาตรการจัดการความเสี่ยง มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้บรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ตามแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้นเพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ด้าน คือ

1. การควบคุมเพื่อป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น มีการแบ่งแยกหน้าที่ความรับผิดชอบและการมอบหมายการปฏิบัติงานโดยผู้บังคับบัญชา มีคำสั่งมอบหมายงานและระบุบุคคลอย่างชัดเจน

2. การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์การตรวจนับและการรายงานข้อบกพร่อง เป็นต้น

3. การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จ

4. การควบคุมเพื่อแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องหรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตตามวัตถุประสงค์

หลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงและค่อนข้างสูงมาประเมินมาตรการควบคุมเป็นอันดับแรก โดยใช้ขั้นตอนดังนี้

- 1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงหรือค่อนข้างสูงมากำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น
- 2) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่
- 3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

4. การติดตามและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยง การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ในการปฏิบัติเพื่อลดโอกาสความเสี่ยงหรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยงของโครงการหรือกิจกรรมควบคุมความเสี่ยงหรือมีแต่ไม่เพียงพอและนำมาวางแผนจัดการความเสี่ยง ซึ่งทางเลือกในการบริหารความเสี่ยงมีหลายวิธีสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการหลีกเลี่ยงความเสี่ยง การยอมรับความเสี่ยง การลดการควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการถ่ายโอนความเสี่ยง และเมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือกเพื่อการตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสม โดยพิจารณาจากประเด็นต่างๆ ดังนี้



1. พิจารณาย่อยรับความเสี่ยงหรือกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
2. เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่ได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่
3. กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.
4. ในรอบปีถัดไป ให้พิจารณาผลการบริหารความเสี่ยงในรอบปีก่อนที่จะดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยง ซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กรให้นำมาระบุการควบคุมในแผนบริหารจัดการความเสี่ยงด้วยการรายงานผลการวิเคราะห์ ประเมิน และบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังคงเหลืออยู่หรือไม่ ถ้ายังมีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไร เสนอต่อผู้บริหารเพื่อทราบและสั่งการ

5. การทบทวนการบริหารความเสี่ยงโดยรอบระยะเวลาในการทบทวนอย่างชัดเจน เป็นการทบทวน/ติดตามภายหลังจากได้ดำเนินการตามแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ปีละ 1 ครั้ง เพื่อให้มั่นใจว่าแผนบริหารจัดการความเสี่ยงฯ นั้นมีประสิทธิภาพ

2.4 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

ศทส. สป.พม. ได้วิเคราะห์ประเภทความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ตามแนวทางของ COSO แบ่งเป็น 8 ประเภท ดังนี้

1. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติและภัยที่มนุษย์สร้างขึ้น เช่น วัตถุภัย อุทกภัย อัคคีภัย ไฟผ่ากระแสน้ำฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและระบบสื่อสารที่มีประสิทธิภาพเพียงพอ

2. ความเสี่ยงด้านบุคลากร (Human Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงานการมอบหมายหน้าที่และสิทธิ์ของบุคลากรและคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกกลุ่ม/ฝ่าย อย่างละเอียดเพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และการสื่อสาร รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

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



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

5. ความเสี่ยงด้านระบบข้อมูล (Database Risk) หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสาร อันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทำให้เกิดความเสียหายขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้น การรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากมนุษย์ ภัยจากธรรมชาติหรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยี

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

7. ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และต่อการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

8. ความเสี่ยงด้านการบริหารจัดการ (Management Risk) หมายถึง ความเสี่ยงเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี

2.5 ความเสี่ยงจากภัยคุกคามไซเบอร์

ภัยคุกคามไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

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



1. อาชญากรรมคอมพิวเตอร์ ผู้ก่อการร้ายทางไซเบอร์ การจารกรรมทางไซเบอร์

2. Ransomware (แรนซัมแวร์) เป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่างๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรม และองค์กรต่างๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์โดยมีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ ด้วยการเข้ารหัสข้อมูลของเป้าหมาย ทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware

3. Phishing (ฟิชซิง) คือ การโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่างๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่น การส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาลบเลิกดำเนินการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีแล้วผู้ไม่หวังดีนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่นๆ ของเป้าหมาย เช่น ข้อมูลการเงิน ข้อมูลรหัสระบบต่างๆ ที่เป็นข้อมูลส่วนบุคคล

4. Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือ ซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยแบ่งออกเป็นหลายประเภท เช่น

1) Virus (ไวรัส) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศ โดยมุ่งเน้นในการโจมตีขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้

2) Worms (เวิร์ม) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศ ที่มีการเชื่อมต่อกับระบบเครือข่ายทั้งภายในและภายนอก โดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่าย จนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้

3) Trojan (โทรจัน) เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับ เปลี่ยนแปลง แก้ไข ข้อมูล ซึ่งอาจส่งผลกระทบต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศ หรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้

4) Spyware (สปายแวร์) คือ ซอฟต์แวร์ประสงค์ร้าย ที่ทำงานอย่างลับๆ บนคอมพิวเตอร์ และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล

5) Adware (แอดแวร์) คือ ซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหาให้กับระบบสารสนเทศได้ ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัย

5. Data leaks (ข้อมูลรั่วไหล) เกิดขึ้นเมื่อมีข้อมูลที่จะเสียก่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาชญากรผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้



6. ภัยธรรมชาติ ได้แก่ น้ำท่วม แผ่นดินไหว พายุ

7. สภาพแวดล้อม ได้แก่ ระบบไฟฟ้าขัดข้อง อุณหภูมิไม่เหมาะสม ความชื้นจากเครื่องปรับอากาศ โครงสร้างพื้นฐานถูกทำลาย

2.6 การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ หมายถึง การดำเนินการในการป้องกันภัยคุกคามไซเบอร์ โดยใช้มาตรการและกระบวนการบริหารความเสี่ยง เพื่อวิเคราะห์ภัยคุกคามไซเบอร์ ประเมินความเสี่ยงที่อาจเกิดขึ้น โดยการจัดหา จัดทำมาตรการ จัดหาวัสดุอุปกรณ์ เพื่อป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ หมายถึง วิธีการ มาตรการ หรือการดำเนินการใดๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งานของอุปกรณ์และข้อมูลภายในระบบสารสนเทศของสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

2.7 การตอบสนองความเสี่ยง

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

1. การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการหรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่า ผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่เกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับอาจนำมาซึ่งการเสียโอกาสของหน่วยงานได้

2. การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นไว้เอง โดยไม่ทำอะไรและยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหาย อยู่ในวิสัยที่หน่วยงานยอมรับได้หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่กำหนดให้แล้ว อาจจะบอก User/Password ของตน ให้ผู้ได้บังคับบัญชาทราบ และเมื่อผู้ได้บังคับบัญชาทราบ User/Password ของหัวหน้างานอาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายและหน่วยงานที่รับผิดชอบต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นแล้วจึงแก้ไขโดยการกำหนด User/Password ใหม่ให้กับหัวหน้างาน เป็นต้น



3. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงานหรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้ความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดหากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรจัดให้หมดไปหรือลดความรุนแรงของความเสียหายลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีการควบคุมความสูญเสีย มี 2 วิธี คือ

1) การป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียคือการหามาตรการหรือวิธีการใดๆ ในการป้องกันไม่ให้ความเสียหายเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคลหรือไวรัสคอมพิวเตอร์มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์และระบบเครือข่าย เป็นต้น

2) การควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความเสียหายขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องวัดอุณหภูมิความร้อนหรือสัญญาณเตือนภัยเพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความเสียหายของอุปกรณ์ภายในห้องคอมพิวเตอร์แม่ข่าย (Server Room) ให้ความเสียหายน้อยที่สุดหรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

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

2.8 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของ สป.พม. มีดังนี้

1. ปัจจัยภายนอก ได้แก่

- 1) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และภัยพิบัติอื่นๆ
- 2) การขโมยอุปกรณ์เครื่องแม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- 3) การชำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) จากการเคลื่อนย้าย หรืออื่นๆ
- 4) ระบบการสื่อสารของระบบเครือข่ายหลักเสียหาย/ขัดข้อง
- 5) ระบบกระแสไฟฟ้าขัดข้อง/ไฟดับ
- 6) ความเสี่ยงจากแมลงหรือสัตว์ประเภทกัดแทะ เช่น หนู แมลงสาบ เป็นต้น



2. ปัจจัยภายใน ได้แก่

- 1) ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- 2) การถูกไวรัสคอมพิวเตอร์ ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่างๆ
- 3) การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.9 การประเมินความเสียหาย

1. ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบ ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) เสียหาย และระบบฐานข้อมูลเสียหาย
2. ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วคราว ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของระบบเครือข่ายคอมพิวเตอร์ขัดข้อง กระแสไฟฟ้าขัดข้อง

2.10 การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการ หรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน ให้รายงานการเกิดปัญหาและผลการแก้ไข ให้ผู้ที่ได้รับมอบหมาย/ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ เจ้าหน้าที่ที่รับผิดชอบจะต้องมีคำสั่งแต่งตั้งจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร สำหรับรูปแบบรายงานใช้รายงานการตรวจรับงานที่ดำเนินการบำรุงรักษาระบบฯ ประจำเดือนทุกเดือน

2.11 ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์ของ สป.พม. ได้มีการพัฒนาและปรับปรุงประสิทธิภาพอย่างต่อเนื่องเพื่อให้งานผ่านระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ของ สป.พม. ตั้งอยู่ที่อาคารกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เลขที่ 1034 ถนนกรุงเกษม แขวงคลองมอหานะ เขตป้อมปราบศัตรูพ่าย กรุงเทพมหานคร มีการเชื่อมโยงเครือข่ายไปยังหน่วยงานภายในส่วนกลางของ สป.พม. และส่วนภูมิภาคสำนักงานพัฒนาสังคมและความมั่นคงของมนุษย์จังหวัด (พมจ.) ทุกจังหวัด

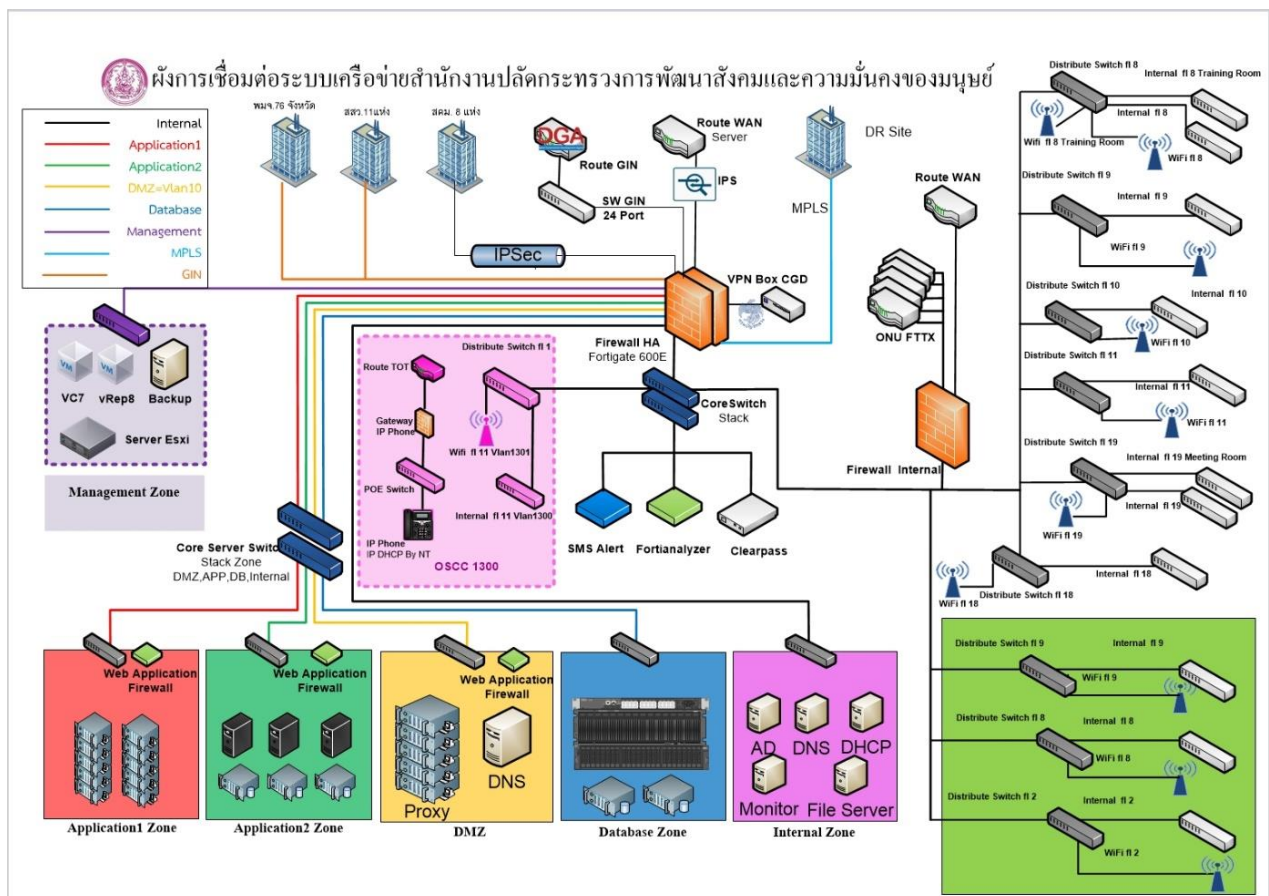


ระบบเครือข่ายคอมพิวเตอร์ของ สป.พม. มีการกำหนดนโยบายและมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศอย่างเป็นระบบ ทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์เพื่อป้องกันการโจมตีและการบุกรุกจากภายนอกเข้าสู่ระบบเครือข่าย ในส่วนของฮาร์ดแวร์ มีการใช้ระบบ Firewall เพื่อกำหนดนโยบายและกรองข้อมูล (Packet Filter) ที่ผ่านเข้ามาจากเครือข่ายภายนอก เช่น เครือข่ายของ สป.พม. เครือข่ายอินเทอร์เน็ต และเครือข่าย GIN โดยมุ่งป้องกันไม่ให้ข้อมูลหรือการเข้าถึงที่ไม่ได้รับอนุญาตส่งผลกระทบต่อระบบเครือข่ายส่วนกลางของ สป.พม.

นอกจากนี้ ยังมีมาตรการรักษาความปลอดภัยในระดับของเครื่องแม่ข่าย (Server Zone หรือ DemilitarizedZone: DMZ) ซึ่งทำหน้าที่ดูแลระบบแม่ข่ายที่สำคัญของ สป.พม. เช่น Web Server และ Mail Server ตลอดจนการติดตั้งโปรแกรมป้องกันไวรัสแบบ Client-Server สำหรับตรวจสอบและควบคุมความปลอดภัยของเครื่องคอมพิวเตอร์ทุกเครื่องในระบบเครือข่าย

มาตรการทั้งหมดนี้มีเป้าหมายเพื่อรักษาความมั่นคงปลอดภัยของข้อมูล ป้องกันความเสียหายที่อาจเกิดขึ้น และสนับสนุนการดำเนินงานของ สป.พม. ให้เป็นไปอย่างมีประสิทธิภาพและมั่นคง

ผังระบบเครือข่ายสำนักงานปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์





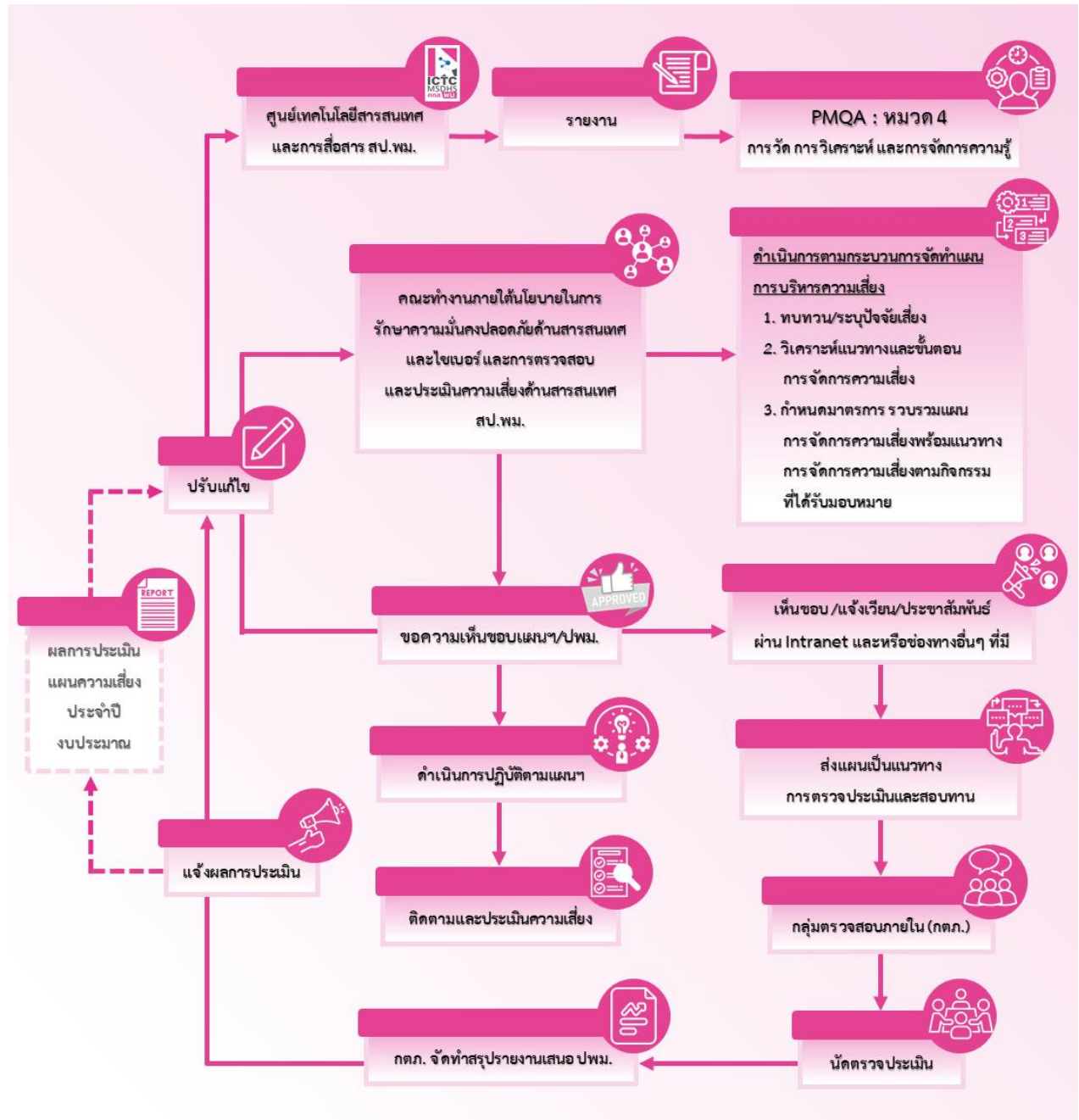
บทที่ 3

การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

สป.พม. ได้ตระหนักถึงความสำคัญของข้อมูลที่สามารถเกิดความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงได้มอบหมายให้ ศทส. จัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568 โดยกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. เริ่มต้นจากการรวบรวมกิจกรรม/ปัจจัยเสี่ยง ที่เกี่ยวข้องกับกระบวนการที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำการศึกษาข้อมูล ระดมความคิดเห็นกับเจ้าหน้าที่ผู้ปฏิบัติงานด้านกิจกรรมต่างๆ ดังนี้

3.1 แนวทางและขั้นตอนการบริหารความเสี่ยง





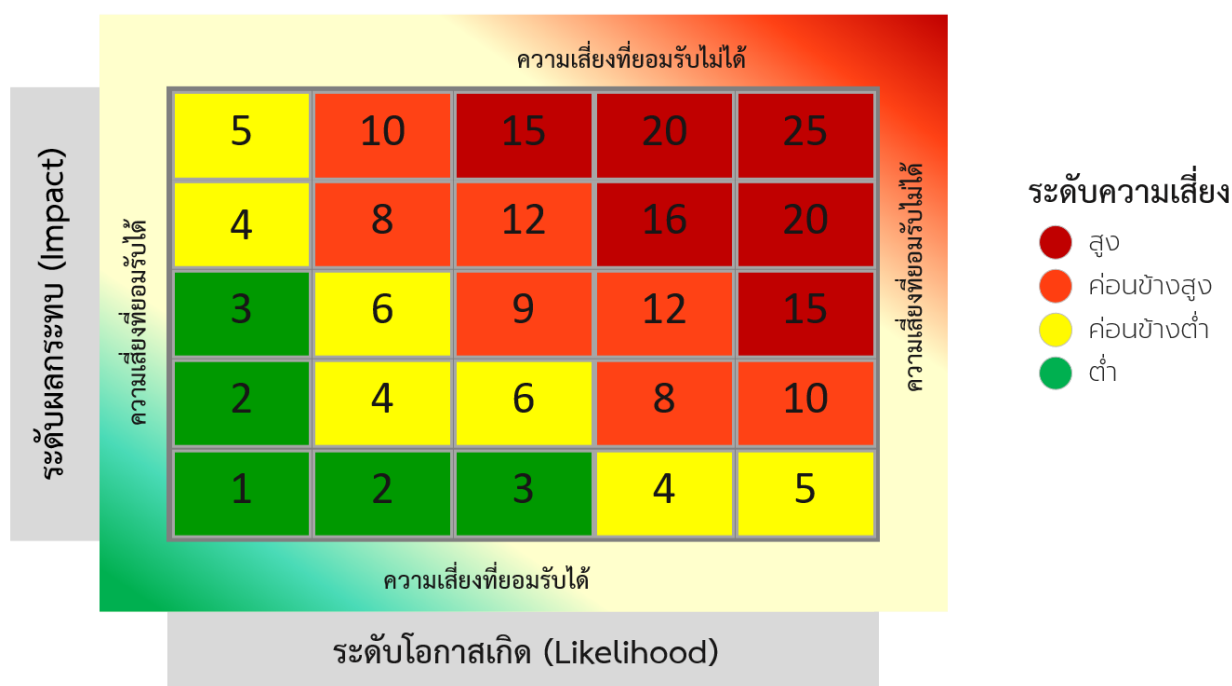


3.3 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์เป็นกระบวนการสำคัญที่ช่วยให้ ศทส. สป.พม. สามารถป้องกันและจัดการภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ หนึ่งในขั้นตอนหลักของกระบวนการ คือ การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่ ศทส. สป.พม. เผชิญอยู่ โดยมีการกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ รวมทั้งการประเมินความเป็นไปได้และผลกระทบ มีดังนี้

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 -





3.4 ผลการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สป.พม. ประจำปีงบประมาณ พ.ศ. 2567

ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
1. ด้านกายภาพและสิ่งแวดล้อม					
วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น					
1.1 ไฟไหม้ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	- ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งานและตรวจสอบระบบดับเพลิงอัตโนมัติเป็นการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้านแผนฉุกเฉินกรณีไฟไหม้	1	2	2
1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้ (การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดัน ไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภท ไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ)	- ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS)/แบตเตอรี่สำรองไฟเป็นประจำทุก 3 เดือน - มีแผนการบำรุงรักษาระบบไฟฟ้าของอาคารสถานที่ ปีละ 1 ครั้ง	1	2	2
1.3 การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น มีการตรวจสอบสภาพ แวดล้อมในห้องและระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ	1	3	3



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
1.4 มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต	- มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. - มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย	- บันทึกรายชื่อ/เวลา/เรื่องที่ดำเนินการในการเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท - ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน	1	3	3
2. ด้านบุคลากร					
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ					
2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนด ไม่ครบถ้วนในการบริหารจัดการสิทธิ์การเข้าถึงและการใช้งานระบบสารสนเทศ	มีความเสี่ยงที่อาจเกิดความเสียหายกับระบบสารสนเทศ ทำให้ระบบสารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูลรั่วไหล	- มีการบริหารจัดการการควบคุมและเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก - การมอบหมายหน้าที่ ความรับผิดชอบที่ชัดเจน - การกำกับติดตามการดำเนินงาน	1	3	3
2.2 บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงในตำแหน่งที่ว่าง	1	2	2
2.3 ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญและทักษะการใช้งานระบบ หรือเปลี่ยนผู้ปฏิบัติงานบ่อย	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนด ทำให้เกิดข้อขัดข้องไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้งานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งาน ทำให้ไม่มีการนำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบัน ขาดความน่าเชื่อถือ ข้อมูลไม่ถูกนำไปใช้งาน	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีช่องทางการแจ้งเหตุผ่านแอปพลิเคชัน LINE - มีระบบ Call Center สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุงตามความต้องการของ User	1	2	2



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
2.4 การจ้างบุคคล ภายนอกที่ขาดความ ตระหนัก ในการดูแล ข้อมูลที่สำคัญของ หน่วยงาน	- ข้อมูลของหน่วยงานเกิดการรั่วไหล อันเนื่องมาจากผู้รับจ้างประมาท เลินเล่อ ขาดความตระหนักในการดูแล ข้อมูลสำคัญระหว่างการบำรุงรักษา/ พัฒนาระบบ - หน่วยงานได้รับความเสียหายด้าน ภาพลักษณ์และชื่อเสียง	- มีการตรวจสอบ ติดตาม เพื่อป้องกัน การผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและ ตรวจรับงาน มีการทำข้อตกลงการห้าม เปิดเผยข้อมูล (NDA) และการใช้หรือ ประมวลผลข้อมูลส่วนบุคคล (DPA)	1	3	3
2.5 การจ้างบุคคล ภายนอกที่ขาดความรู้ ความชำนาญ ความ เชี่ยวชาญ ดูแลบำรุง รักษาระบบ/พัฒนา ระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไข ทำให้ต้องขยาย เวลาทำงานและไม่สามารถตรวจรับ งานได้ตามกำหนด ทำให้เกิดความ เสียหายแก่หน่วยงาน	- มีการตรวจสอบ ติดตาม เพื่อป้องกัน การผิดพลาด ทำให้เกิดการแก้ไข ปัญหาได้ทันที โดยมีการประชุมทุกๆ สัปดาห์ - มีการกำหนดคุณสมบัติของบุคลากร ภายนอก (Outsource) - มีการจัดทำแผนงาน ขั้นตอนการ ทำงานที่ชัดเจนและควบคุม ให้เป็นไป ตามแผนงานที่กำหนดไว้	1	2	2
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาด ของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ					
3.1 ไม่มีการควบคุม/ จัดทำบัญชี/ปรับปรุง บัญชีทรัพย์สินของ อุปกรณ์เทคโนโลยีและ การสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และ อุปกรณ์เครือข่ายสูญหาย	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบ พัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติ ครุภัณฑ์และอุปกรณ์ของ ศทส.	1	2	2
3.2 ขาดแผนรองรับ ระบบฮาร์ดแวร์ ภายใน ศูนย์ปฏิบัติการระบบ แม่ข่ายและเครือข่าย คอมพิวเตอร์ สป.พม.	ระบบข้อมูลเสียหาย/ถูกทำลายหรือ ระบบสารสนเทศไม่สามารถให้บริการ ต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้าน ฮาร์ดแวร์หรืออุปกรณ์ฮาร์ดแวร์ได้รับ ความเสียหายร้ายแรง	- มีแผนการบำรุงรักษา ตรวจสอบ และ ซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์ และอุปกรณ์เป็นประจำ - มีการประชุมติดตาม และสรุป ผล การปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูลและกู้คืนระบบ ในรายการครุภัณฑ์ที่มีความสำคัญ	1	3	3



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
3.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับผู้ใช้งานขาดประสิทธิภาพ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบบตัวต้นผู้ใช้งานไม่ได้ - หาผู้กระทำความผิดไม่ได้	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง/ปรับปรุง/เพิ่มเติม/แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ	2	2	4
3.4 ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อม ต่อกับผู้ให้บริการได้	เกิดความเสียหาย/ขัดข้อง ไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้	- ให้มีการระบุเกี่ยวกับระดับการให้บริการที่ชัดเจนในข้อกำหนด/ข้อตกลงกับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหากจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบหรือ ผอ. ศทส. ทุกครั้งที่ระบบขัดข้องเพื่อให้แก้ปัญหาได้ทัน่วงที	1	2	2
3.5 ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และยืนยันตัวตนบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา - มีการปรับปรุงประสิทธิภาพการบริหารจัดการทุกๆ ปี	2	1	2



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
3.6 ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์เจาะหรือ ลักลอบ (Hack) เข้าสู่ เครื่องคอมพิวเตอร์ แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตาม เพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการ อย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน - เข้าบริการศูนย์รับมือและตอบ สอนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการแจ้งเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์	2	3	6
3.7 ขาดการป้องกัน หรือตรวจจับไวรัส	- เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบเครือข่ายระบบ สารสนเทศและฐานข้อมูล	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ	2	2	4



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
4. ด้านโปรแกรมคอมพิวเตอร์					
วัตถุประสงค์ : ควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัปเดต เพื่อลดช่องโหว่ที่เกิดจาก Bug ของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์					
หมายเหตุ : Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้นๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้					
4.1 ละเมิดลิขสิทธิ์โปรแกรมมัลแวร์ (Utilities Program) (Utilities Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดว์ เรียกว่า ยๆ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์ เช่น ประสิทธิภาพการจัดไฟล์ป้องกันไวรัส บั๊อไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น)	- หน่วยงาน/บุคคล ต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุกคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศและการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำและส่งเสริมให้ใช้โปรแกรมมัลแวร์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย	2	1	2
5. ด้านระบบข้อมูล					
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูลต่างๆ ถูกทำลายจากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้					
5.1 ไม่มีการจัดทำบัญชีรายละเอียดของระบบสารสนเทศ และ ผู้เกี่ยวข้อง	- ไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างทันทั่วทั้งที่ - เมื่อระบบเสียหายไม่สามารถหาสาเหตุได้ - ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง	จัดทำ/ทบทวนรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง	1	2	2
5.2 ขาดการบริหารจัดการสิทธิ์ผู้ใช้งาน และการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบบตัวต้นผู้ใช้งานได้ไม่ได้ - หาผู้กระทำความผิดไม่ได้ - การถูกยึดครองระบบจากผู้ไม่หวังดี (Hacker)	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง/ปรับปรุง/เพิ่มเติม/แก้ไข	2	2	4



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
- การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี		- มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ - ระบุนิยามลักษณะทางเทคนิค ในการบริหารจัดการสิทธิ์ ผู้ใช้งานและการเข้าถึง เพื่อใช้งานระบบ ภายใต้ขอบเขตงานการพัฒนาระบบสารสนเทศ			
5.3 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ให้บริการทั่วไปไม่มีประสิทธิภาพ - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- 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 - ถูกโจมตีระบบทำให้ไม่สามารถให้บริการได้	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกล ในการเข้าถึง (VPN หรือ Virtual Private Network คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้) - การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งานทุก 6 เดือน	2	2	4



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
5.5 การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์ไม่มีความชัดเจน	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบที่มีการพัฒนาไว้อย่างหลากหลาย - สูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูง เกิดความไม่คุ้มค่า	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตามทุกขั้นตอนของการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐานและ TOR	2	3	6
5.6 ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลางกระทรวง พม. อย่างต่อเนื่อง - มีการติดตามการนำมาตรฐานข้อมูลกลางกระทรวง พม. ไปใช้อย่างสม่ำเสมอ - มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) - มีการดำเนินงานทบทวน/ปรับปรุงและเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลางกระทรวง พม. ที่ครอบคลุมภารกิจของกระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ	2	1	2
5.7 เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ติดตั้ง patch ของระบบ ปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ได้รับทราบอย่างต่อเนื่อง	2	2	4



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
5.8 การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	- มีการพัฒนาแพลตฟอร์มบริหารจัดการข้อมูลด้านสวัสดิการสังคม (Social Welfare Data Management Platform) เพื่อควบคุมคุณภาพข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล	2	2	4
5.9 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ	2	2	4
6. ด้านกลยุทธ์ วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการกำหนดนโยบาย กลยุทธ์ ที่ทำให้แผนการดำเนินงานไม่สามารถบรรลุวัตถุประสงค์องค์กร					
6.1 ทิศทาง/แนวทาง การพัฒนาด้านเทคโนโลยีสารสนเทศไม่ชัดเจน/ไม่สอดคล้องกับการกิจกรรมบูรณาการร่วมกัน	ไม่สามารถลดความซ้ำซ้อนของกระบวนการหรือระบบงานได้ ทำให้ขาดประสิทธิภาพในการดำเนินงานและการใช้งบประมาณไม่คุ้มค่า	- จัดทำ/ทบทวน สถาปัตยกรรมองค์กรของหน่วยงาน (Enterprise Architecture : EA) - นำสถาปัตยกรรมองค์กรของหน่วยงานมาใช้เป็นกรอบแนวทางในการพัฒนาระบบเทคโนโลยี สารสนเทศของหน่วยงาน	2	1	2
7. ด้านการเงิน (งบประมาณ) วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ/การเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลาเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลา					
7.1 การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนดทำให้ได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ขาดงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ	- จัดลำดับความสำคัญของโครงการที่จำเป็นต้องดำเนินการให้อยู่ในลำดับต้นๆ - จัดทำความเสี่ยงแนบไปกับโครงการและให้มีการถ่วงน้ำหนักของโครงการที่เป็นโครงการประเภทเดียวกัน - ชี้แจงผลกระทบหากไม่ได้ดำเนินโครงการและการยอมรับความเสี่ยง - ปรับลดขอบเขตงานลงตามงบประมาณที่ได้รับ - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ	3	1	3



ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจจะเกิดขึ้น	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
			โอกาส	ผลกระทบ	ระดับคะแนน
8. ด้านการบริหารจัดการ					
วัตถุประสงค์ : เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี					
8.1 กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคา - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา	การดำเนินโครงการเกิดความล่าช้า ทำให้ขาดประสิทธิภาพในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญ/ความเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด	2	2	4



3.5 ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568

ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ
1. ด้านกายภาพและสิ่งแวดล้อม วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น	1.1	ไฟไหม้ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูล ถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ฐานข้อมูล/ระบบสารสนเทศ
	1.2	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้ (การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหายและการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ฐานข้อมูล/ระบบสารสนเทศ
	1.3	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ฐานข้อมูล/ระบบสารสนเทศ
	1.4	- มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต - ประตูปิดไม่สนิท - อุปกรณ์ควบคุมการเข้าถึงเสีย - มีการใช้พื้นที่ทางเดินร่วมกับห้องปฏิบัติการคอมพิวเตอร์ (ห้องอบรม)	- มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. - มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย - เครื่องคอมพิวเตอร์ลูกข่าย - ฐานข้อมูล/ระบบสารสนเทศ



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ
2. ด้านบุคลากร วัตถุประสงค์ : เพื่อ ควบคุมความเสี่ยงที่เกิด จากดำเนินงานของ บุคลากรด้านเทคโนโลยี สารสนเทศ	2.1	ผู้ดูแลระบบปฏิบัติตามแนวทาง ที่กำหนดไม่ครบถ้วนในการ บริหารจัดการสิทธิ์การเข้าถึง และ การ ใช้ งาน ระบบ สารสนเทศ	มีความเสี่ยงที่อาจเกิดความเสียหาย กับระบบสารสนเทศ ทำให้ระบบ สารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูล รั่วไหล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.2	บุคลากรด้านไอที มีความรู้ ความเข้าใจด้านเทคโนโลยีไม่ เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบ บกพร่องและอาจเกิดความเสียหาย ทั้งระบบได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.3	ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญและทักษะการใช้ งานระบบหรือเปลี่ยน ผู้ปฏิบัติงานบ่อย	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนด ทำให้เกิด ข้อขัดข้องไม่สามารถแก้ไขปัญหา ด้วยตัวเองในเบื้องต้นได้ งานติดขัด - ความล่าช้าในการปฏิบัติงานเพิ่ม ภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งาน ทำให้ไม่มีการ นำเข้าข้อมูล/ข้อมูลไม่เป็นปัจจุบัน ขาดความน่าเชื่อถือ ข้อมูลไม่ถูก นำไปใช้งาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.4	การจ้างบุคคลภายนอกที่ขาด ความตระหนักในการดูแล ข้อมูลที่สำคัญของหน่วยงาน	- ข้อมูลของหน่วยงานเกิดการ รั่วไหล อันเนื่องมาจากผู้รับจ้าง ประมาทเลินเล่อ ขาดความตระหนัก ในการดูแลข้อมูลสำคัญระหว่าง การบำรุงรักษา/พัฒนาระบบ - หน่วยงานได้รับความเสียหาย ด้านภาพลักษณ์และชื่อเสียง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	2.5	การจ้างบุคคลภายนอกที่ขาด ความรู้ ความชำนาญ ความ เชี่ยวชาญ ดูแลบำรุงรักษา ระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตาม แผน เสียเวลาในการแก้ไข ทำให้ ต้องขยายเวลาทำงานและไม่สามารถ ตรวจรับงานได้ตามกำหนด ทำให้ เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ	3.1	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.2	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารและระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับผู้ใช้งานขาดประสิทธิภาพ	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบบตัวตนผู้ใช้งานไม่ได้ - หาผู้กระทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถระบุตัวตนผู้ใช้งานตัวจริงได้
	3.4	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	เกิดความเสียหาย/ขัดข้องไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถเข้าถึงระบบสารสนเทศจากภายนอกได้ - เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถเข้าถึงอินเทอร์เน็ตได้
	3.5	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.6	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลงทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง-ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	3.7	ขาดการป้องกันหรือตรวจจับไวรัส	เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบเครือข่ายระบบสารสนเทศและฐานข้อมูล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ
4. ด้านโปรแกรมคอมพิวเตอร์ วัตถุประสงค์ : ควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัปเดต เพื่อลดช่องโหว่ที่เกิดจาก Bug ของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบหรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์ <i>หมายเหตุ :</i> Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรมอันเนื่องมาจากคำสั่งในโปรแกรมนั้นๆเอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้	4.1	ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program) (Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดวส์ เรียกว่าง่าย ๆ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดวส์ เช่น ประสิทธิภาพการจัดไฟล์ป้องกันไวรัส ปับอัดไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น)	- หน่วยงาน/บุคคล ต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุกคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
5. ด้านระบบข้อมูล วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูลต่างๆ ถูกทำลาย จากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้	5.1	ไม่มีการจัดทำบัญชีรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง	- ไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที - เมื่อระบบเสียหายไม่สามารถหาสาเหตุได้ - ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.2	ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบบตัวต้นผู้ใช้งานได้ไม่ได้ - หาผู้กระทำความผิดไม่ได้ - การถูกยึดครองระบบจากผู้ไม่หวังดี (Hacker)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ
	5.3	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูลและการส่ง ข้อมูลคำสั่งเจตนาร้าย	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ให้บริการทั่วไปไม่มีประสิทธิภาพ - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.4	การรักษาความมั่นคงปลอดภัย ของผู้ปฏิบัติ งานจากระยะไกล ไม่ทั่วถึง	- อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.5	การกำหนดมาตรฐานในการ พัฒนาซอฟต์แวร์ไม่มีความ ชัดเจน	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบที่มีการพัฒนาไว้อย่างหลากหลาย - สูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูง เกิดความไม่คุ้มค่า	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.6	ไม่มีการนำมาตรฐานข้อมูลไปใช้ ในการพัฒนาและออกแบบ ระบบข้อมูลและฐานข้อมูลเพื่อ การแลกเปลี่ยนเชื่อมโยงข้อมูล	ไม่สามารถแลกเปลี่ยนเชื่อมโยง ข้อมูลระหว่างหน่วยงานได้อย่างมี ประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.7	เกิดช่องโหว่จากการพัฒนา โปรแกรมประยุกต์	ระบบสารสนเทศไม่ได้รับการปรับปรุง ให้มีความทันสมัยหรือความปลอดภัย ตามที่ผู้พัฒนาระบบได้กำหนด ทำให้ มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.8	การนำเข้าข้อมูลผิดพลาด ทั้งจาก ผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน
	5.9	การนำเข้าข้อมูลไม่ครบถ้วน และไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่อาจเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ
6. ด้านกลยุทธ์ วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการกำหนดนโยบาย กลยุทธ์ ที่ทำให้แผนการดำเนินงานไม่สามารถบรรลุวัตถุประสงค์องค์กร	6.1	ทิศทาง/แนวทางการพัฒนาด้านเทคโนโลยีสารสนเทศไม่ชัดเจน/ไม่สอดคล้องกับภารกิจขาดการบูรณาการร่วมกัน	ไม่สามารถลดความซ้ำซ้อนของกระบวนการหรือระบบงานได้ ทำให้ขาดประสิทธิภาพในการดำเนินงานและการใช้งบประมาณไม่คุ้มค่า	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน
7. ด้านการเงิน (งบประมาณ) วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ/การเบิกจ่าย 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. 2568

รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่จะเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ	ก่อน			กลยุทธ์ ที่ใช้จัดการ ความเสี่ยง	แนวทาง การควบคุม	หลัง		
				มีแนวทางการควบคุม	โอกาส	ผล กระทบ			ระดับ คะแนน	มีแนวทางการควบคุม	โอกาส
1. ด้านกายภาพและสิ่งแวดล้อม											
วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น											
1.1	ไฟไหม้ ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)	เกิดความเสียหายกับทรัพย์สิน ระบบเครือข่ายอุปกรณ์ และฐานข้อมูลถูกทำลายทั้งหมด การดำเนินงานหยุดชะงัก ระบบประมวลผลหยุดทั้งระบบ	-ผู้ใช้งานระบบผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย -เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	1	5	5	ควบคุมความเสี่ยง	ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งานและตรวจสอบระบบดับเพลิงอัตโนมัติ เป็นการจ้างบริษัทดำเนินการบำรุงรักษาเนื่องจากมีความเชี่ยวชาญเฉพาะด้าน - แผนฉุกเฉินกรณีไฟไหม้	1	2	2
1.2	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ทำให้ระบบเครือข่ายหลักและเครื่องแม่ข่ายไม่สามารถให้บริการได้ - ทำให้ระบบฐานข้อมูลเกิดความเสียหายได้ การเกิดกระแสไฟฟ้าขัดข้องหรือเกิดแรงดัน ไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่หรือเมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	-ผู้ใช้งานระบบผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย -เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	2	4	8	จัดการความเสี่ยง	- ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า (UPS)/แบตเตอรี่สำรองไฟ เป็นประจำทุก 3 เดือน - มีแผนการบำรุงรักษาระบบไฟฟ้าของอาคารสถานที่ ปีละ 1 ครั้ง	1	2	2
1.3	การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ผิดปกติ	เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	-ผู้ใช้งานระบบผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย -เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	1	4	4	ควบคุมความเสี่ยง	ติดตั้งระบบควบคุมอุณหภูมิ/ความชื้น มีการตรวจสอบสภาพแวดล้อมในห้อง และระบบควบคุมอุณหภูมิ/ความชื้นผ่านระบบควบคุมอย่างสม่ำเสมอ	1	3	3
1.4	มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต - ประสิทธิภาพไม่ดี - อุปกรณ์ควบคุมการเข้าถึงเสีย - มีการใช้พื้นที่ทางเดินร่วมกับห้องปฏิบัติการคอมพิวเตอร์ (ห้องอบรม)	มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย	-ผู้ใช้งานระบบผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย -เครื่องคอมพิวเตอร์ลูกข่าย - ระบบฐานข้อมูล/ระบบสารสนเทศ	2	4	8	จัดการความเสี่ยง	- บันทึกรายชื่อ/เวลา/เรื่องที่ทำเนิการ ในเช้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท - ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน - มีการใช้รหัสแบบ Two-Factor Authentication (2FA)	1	3	3



รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่จะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อน			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลัง		
				มีแนวทางการควบคุม	โอกาส	ผลกระทบ			มีแนวทางการควบคุม	โอกาส	ผลกระทบ
2. ด้านบุคลากร											
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ											
2.1	ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึงและการใช้งานระบบสารสนเทศ	มีความเสี่ยงที่อาจเกิดความเสียหายกับระบบสารสนเทศ ทำให้ระบบสารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูลรั่วไหล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	4	12	จัดการความเสี่ยง	มีการบริหารจัดการการควบคุมและเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก - การมอบหมายหน้าที่ความรับผิดชอบที่ชัดเจน - การกำกับติดตามการดำเนินงาน - ปรับปรุงระบบสารสนเทศให้มีความปลอดภัยมากขึ้น เช่น Session Time Out - พิจารณาใช้ดิจิทัล ID เพิ่มเติม เช่น THAID	1	3	3
2.2	บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ	เกิดความผิดพลาดในการใช้ระบบ มีผลทำให้การทำงานของระบบบกพร่องและอาจเกิดความเสียหายทั้งระบบได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- อบรม/ส่งเสริมสนับสนุนให้มีการสอบมาตรฐานวิชาชีพด้านไอที - มีการจ้างบุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญเฉพาะด้าน - มีการติดตามให้หน่วยงานที่รับผิดชอบสรรหาบุคลากรมาลงเฝ้าตำแหน่งที่ว่าง	1	2	2
2.3	ผู้ใช้งาน/users ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ หรือเปลี่ยนผู้ปฏิบัติงานบ่อย	- การใช้ระบบงานไม่เป็นไปตาม workflow ที่กำหนดทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ งานติดขัด - ความล่าช้าในการปฏิบัติงาน เพิ่มภาระให้กับผู้ดูแลระบบ - ไม่มีการใช้งานให้ทำให้ไม่มีการนำเข้าสู่ข้อมูล/ข้อมูลไม่เป็นปัจจุบันขาดความน่าเชื่อถือ ข้อมูลไม่ถูกนำไปใช้งาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- อบรมการใช้งานระบบงาน - จัดทำคู่มือสำหรับปฏิบัติงาน - มีช่องทางการแจ้งเหตุผ่านแอปพลิเคชัน LINE - มีระบบ Call Center สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ - จัดหลักสูตรรองรับงานที่มีการพัฒนาหรือมีการปรับปรุงหรือตามความต้องการของ User	1	2	2
2.4	การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	- ข้อมูลของหน่วยงานเกิดการรั่วไหล อันเนื่องมาจากผู้รับจ้างประมวลผลข้อมูลขาดความตระหนักในการดูแลข้อมูลสำคัญระหว่างการรักษา/พัฒนาระบบ - หน่วยงานได้รับความเสียหายด้านภาพลักษณ์และชื่อเสียง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	4	8	จัดการความเสี่ยง	- มีการตรวจสอบ ติดตามเพื่อป้องกันการผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน มีการทำข้อตกลงการห้ามเปิดเผยข้อมูล (NDA) และการใช้หรือประมวลผลข้อมูลส่วนบุคคล (DPA)	1	3	3



รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่จะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อน			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทาง การควบคุม	หลัง		
				มีแนวทางควบคุมโอกาส	ผลกระทบ	ระดับคะแนน			มีแนวทางควบคุมโอกาส	ผลกระทบ	ระดับคะแนน
2.5	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ เชี่ยวชาญ ดูแลบำรุงรักษาระบบ/พัฒนาระบบ	- มีข้อผิดพลาดและไม่เป็นไปตามแผน เสียเวลาในการแก้ไขทำให้ต้องขยายเวลาทำงาน และไม่สามารถตรวจรับงานได้ตามกำหนด ทำให้เกิดความเสียหายแก่หน่วยงาน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาดและให้เกิดการแก้ไขปัญหาได้ทันทีโดยมีการประชุมทุกๆ สัปดาห์ - มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) - มีการจัดทำแผนงาน ขั้นตอนการทำงานที่ชัดเจนและควบคุมให้เป็นไปตามแผนงานที่กำหนดไว้	1	2	2
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดของโหนดของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้งและไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ											
3.1	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	ครุภัณฑ์/อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายสูญหาย	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	1	3	3	ควบคุมความเสี่ยง	- จัดทำทะเบียนครุภัณฑ์ตามระเบียบพัสดุ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และอุปกรณ์ของ ศทส.	1	2	2
3.2	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.	ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรืออุปกรณ์ฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	1	5	5	ควบคุมความเสี่ยง	- มีแผนการบำรุงรักษาตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตามและสรุปผลการปฏิบัติงานทุกเดือน - จัดทำการสำรองข้อมูล และกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ	1	3	3
3.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกระดับผู้ใช้งานขาดประสิทธิภาพ	เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบบตัวต้นผู้ใช้งานได้ไม่ได้ - ทรัพยากรทำความผิดไม่ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถระบุตัวตนผู้ใช้งานตัวจริงได้	3	3	9	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือนโดยการเปลี่ยนแปลงปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ	2	2	4
3.4	ระบบเครือข่ายสื่อสารหลักสำหรับศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ไม่สามารถเชื่อมต่อกับผู้ให้บริการได้	เสียหาย/ขัดข้องไม่สามารถเข้าถึงบริการสารสนเทศจากระยะไกล (Remote) ได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบไม่สามารถเข้าถึงระบบสารสนเทศจากภายนอกได้ - เครื่องคอมพิวเตอร์แม่ข่าย ไม่สามารถเข้าถึงอินเทอร์เน็ตได้	1	5	5	ควบคุมความเสี่ยง	- ให้มีการระบุเกี่ยวกับระดับการให้บริการที่ชัดเจนในข้อกำหนด/ข้อตกลง กับผู้ให้บริการเครือข่าย - มีระบบตรวจสอบการเข้าถึงเครือข่ายสื่อสารหลัก - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแล - มีสัญญาการบำรุงรักษาและการแก้ไขปัญหาจากผู้ให้บริการเครือข่ายหลัก - มีข้อความเตือนผ่าน SMS ไปที่ผู้รับผิดชอบหรือ ผอ. ศทส. ทุกครั้งที่ระบบขัดข้อง เพื่อให้แก้ปัญหาได้ทันที	1	2	2



รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่จะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อน			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทาง การควบคุม	หลัง		
				มีแนวทาง โอกาส	การควบคุม ผลกระทบ	ระดับ คะแนน			มีแนวทาง โอกาส	การควบคุม ผลกระทบ	ระดับ คะแนน
3.5	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	- ไม่มีความมั่นคงปลอดภัยต่อการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและเครือข่ายคอมพิวเตอร์ของหน่วยงาน - เกิดการรบกวนการใช้งานภายในระบบเครือข่ายคอมพิวเตอร์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- ทำการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่ โดยมีระบบพิสูจน์และยืนยันตัวตนบุคคล - มีเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์พกพา - มีการปรับปรุงประสิทธิภาพการบริหารจัดการทุก ๆ ปี	2	1	2
3.6	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลายหรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ - ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง - ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	5	5	25	จัดการความเสี่ยง	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน - เช่าบริการศูนย์รับมือและตอบสนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการแจ้งเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์ - เข้าร่วมกับหน่วยงานภายนอกด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ สำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ในการเฝ้าระวังภัยทางไซเบอร์	2	3	6
3.7	ขาดการป้องกันหรือตรวจจับไวรัส	เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหายแก่ระบบเครือข่าย ระบบสารสนเทศและฐานข้อมูล	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ	2	2	4



รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหาย ที่จะเกิดขึ้น	ผลกระทบ/ ผู้ได้รับผลกระทบ	ก่อน มีแนวทางการควบคุม			กลยุทธ์ ที่ใช้จัดการ ความเสี่ยง	แนวทาง การควบคุม	หลัง		
				โอกาส	ผล กระทบ	ระดับ คะแนน			มีแนวทางการควบคุม	โอกาส	ผล กระทบ
4. ด้านโปรแกรมคอมพิวเตอร์											
วัตถุประสงค์ : ควบคุมความเสี่ยงที่เกิดจากการทำงานของระบบโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่อัปเดต เพื่อลดช่องโหว่ที่เกิดจาก Bug ของซอฟต์แวร์หรือถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบหรือจากการใช้ SW ที่ไม่มีลิขสิทธิ์											
หมายเหตุ : Bug คือ จุดบกพร่อง หมายถึง ปัญหาที่เกิดขึ้นกับโปรแกรม อันเนื่องมาจากคำสั่งในโปรแกรมนั้นๆ เอง ซึ่งในการทำงานของโปรแกรมไม่ถูกต้อง มีข้อผิดพลาดหรือไม่ราบรื่นเท่าที่ควร นอกนั้นอาจเป็นปัญหาเกี่ยวกับเครื่องก็ได้											
4.1	ละเมิดลิขสิทธิ์โปรแกรมมอรรถประโยชน์ (Utilities Program) (Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดว์ เรียกง่ายยว่า เป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์ เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บั๊บอัปเดตไฟล์สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น)	- หน่วยงาน/บุคคลต้องรับผิดชอบค่าปรับในคดีละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา - เกิดภัยคุกคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	2	6	ควบคุมความเสี่ยง	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติ ความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง จัดทำและส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ Open Source แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดซื้อลิขสิทธิ์ที่ถูกต้องตามกฎหมาย	2	1	2
5. ด้านระบบข้อมูล											
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูลต่างๆ ถูกทำลายจากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้											
5.1	ไม่มีการจัดทำบัญชีรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง	- ไม่สามารถตอบสนองต่อภัยคุกคามได้อย่างทันทั่วทั้ง - เมื่อระบบเสียหายไม่สามารถหาสาเหตุได้ - ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- จัดทำ/ทบทวนรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง - จัดทำบัญชีการวิเคราะห์ผลกระทบทางสารสนเทศ (BIA)	1	2	2
5.2	ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อล็อกอินผิดเพื่อป้องกันการโจมตี	- เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ - ระบบตัวต้นผู้ใช้งานได้ไม่ได้ - หาผู้กระทำความผิดไม่ได้ - การถูกยึดครองระบบจากผู้ไม่หวังดี (Hacker)	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลงปรับปรุงเพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ - ระบุคุณลักษณะทางเทคนิคในการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบ ภายใต้ขอบเขตงานการพัฒนาสารสนเทศ	2	2	4



รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่จะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อน			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทาง การควบคุม	หลัง		
				มีแนวทาง โอกาส	การควบคุม ผลกระทบ	ระดับ คะแนน			มีแนวทาง โอกาส	การควบคุม ผลกระทบ	ระดับ คะแนน
5.3	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลค่าส่งเจตนาร้าย	- การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ให้บริการทั่วไปไม่มีประสิทธิภาพ - ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน - ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	4	5	20	จัดการความเสี่ยง	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - สำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง - มีการตรวจสอบช่องโหว่และตรวจสอบระบบ อย่างน้อยปีละ 1 ครั้ง	2	3	6
5.4	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ถึง	- อาจถูกลักลอบขโมยข้อมูลหรือข้อมูลถูกทำลาย เกิดความสูญเสีย - ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ - ถูกโจมตีระบบ ทำให้ไม่สามารถให้บริการได้	- ผู้นำเข้าข้อมูล - ผู้ใช้งานระบบ/ข้อมูล - หน่วยงาน	4	3	12	จัดการความเสี่ยง	- มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง (VPN หรือ Virtual Private Network) คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้ - การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งาน ทุก 6 เดือน	2	2	4
5.5	การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์ไม่มีความชัดเจน	- เกิดความยุ่งยากซับซ้อนในการบำรุงรักษาระบบที่มีการพัฒนาอย่างหลากหลาย - สูญเสียงบประมาณในการดำเนินการบำรุงรักษาที่มีค่าใช้จ่ายสูง เกิดความไม่คุ้มค่า	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	2	3	6	ควบคุมความเสี่ยง	- จัดทำคู่มือมาตรฐานการพัฒนาซอฟต์แวร์ - ระบุมาตรฐานการพัฒนาซอฟต์แวร์ และคุณสมบัติผู้พัฒนาซอฟต์แวร์ในขั้นตอนการจัดทำ TOR - ควบคุม ติดตามทุกขั้นตอนของการพัฒนาซอฟต์แวร์ให้เป็นไปตามมาตรฐานและ TOR	2	1	2



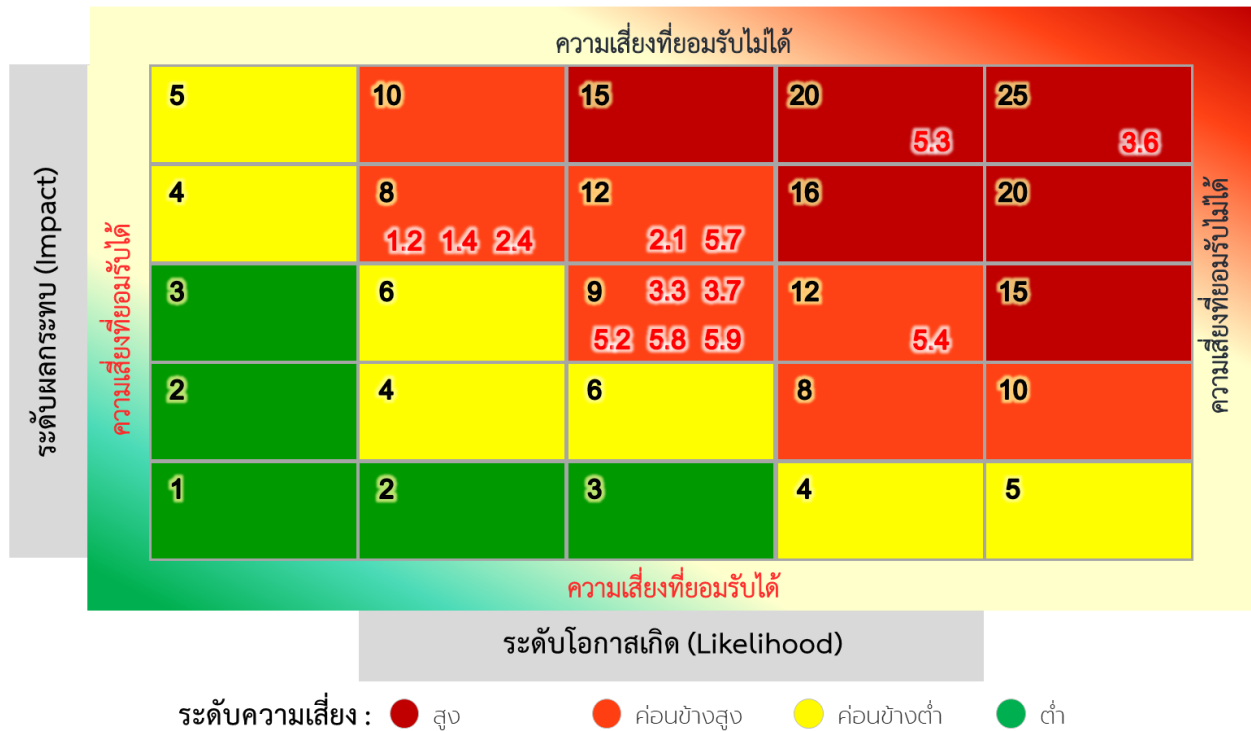
รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่จะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อนมีแนวทางการควบคุม			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทางการควบคุม	หลังมีแนวทางการควบคุม		
				โอกาส	ผลกระทบ	ระดับคะแนน			โอกาส	ผลกระทบ	ระดับคะแนน
5.6	ไม่มีการนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล	ไม่สามารถแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- มีการเผยแพร่ประชาสัมพันธ์และส่งเสริมการใช้งานมาตรฐานข้อมูลกลางกระทรวง พม. อย่างต่อเนื่อง - มีการติดตามการนำมาตรฐานข้อมูลกลาง กระทรวง พม. ไปใช้อย่างสม่ำเสมอ - มีการนำมาตรฐานข้อมูลไปใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลในเรื่องการรายงานการช่วยเหลือผู้ประสบปัญหาทางสังคม (เงินอุดหนุน) - มีการดำเนินงานทบทวน/ปรับปรุง และเพิ่มเติมชุดรายการมาตรฐานข้อมูลกลางกระทรวง พม. ที่ครอบคลุมภารกิจของกระทรวงและสอดคล้องกับสถานการณ์ปัจจุบันอย่างต่อเนื่องสม่ำเสมอทุกปี - มีการกำหนดให้นำมาตรฐานข้อมูลไปใช้เป็นหลักในการพัฒนาระบบสารสนเทศ	2	2	4
5.7	เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	ระบบสารสนเทศไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบได้กำหนด ทำให้มีความเสี่ยงจากการถูกบุกรุกโจมตีได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	4	3	12	จัดการความเสี่ยง	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ได้รับทราบอย่างต่อเนื่อง - พิจารณาจัดทำแผน/ปรับปรุงระบบ	1	3	3
5.8	การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และ ความผิดพลาดของระบบ (Bug)	- ข้อมูลไม่มีคุณภาพ - ไม่สามารถเชื่อมโยงข้อมูลได้ - ไม่สามารถออกรายงานได้	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- มีการควบคุมคุณภาพข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล - สร้างความตระหนักรู้ในการนำเข้าข้อมูล - มอบรางวัลเพื่อเป็นกำลังใจให้กับหน่วยงานที่มีการนำเข้าข้อมูลผิดพลาดน้อย	2	2	4
5.9	การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- ไม่มีข้อมูลในฐานข้อมูล - ไม่สามารถออกรายงานได้ถูกต้องและเป็นปัจจุบัน	- ผู้ใช้งานระบบ/ผู้ดูแลระบบ - หน่วยงาน	3	3	9	จัดการความเสี่ยง	- กำหนดตัวชี้วัดในการบันทึกข้อมูล - ออกประกาศเกี่ยวกับการนำเข้าข้อมูลสารสนเทศ - ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ	1	3	3



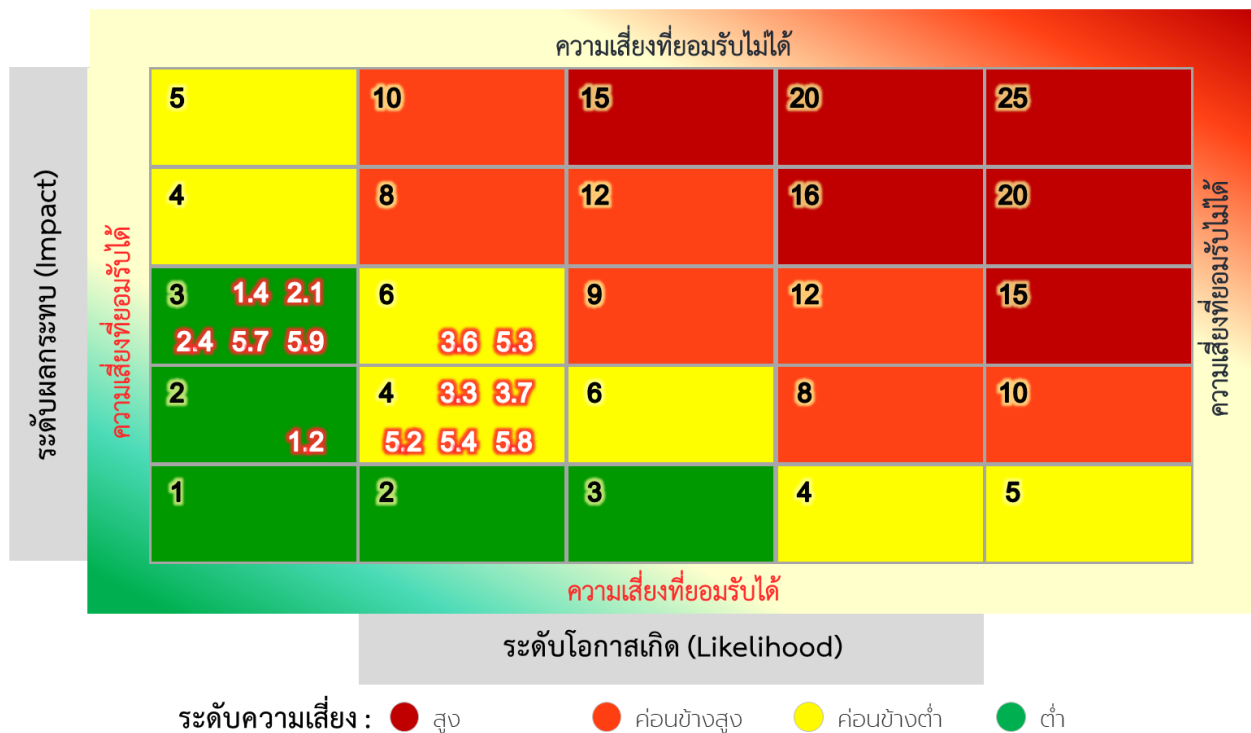
รหัส	ปัจจัยเสี่ยง	ลักษณะความเสียหายที่จะเกิดขึ้น	ผลกระทบ/ผู้ได้รับผลกระทบ	ก่อน			กลยุทธ์ที่ใช้จัดการความเสี่ยง	แนวทาง การควบคุม	หลัง		
				มีแนวทางการควบคุม	โอกาส	ผลกระทบ			มีแนวทางการควบคุม	โอกาส	ผลกระทบ
6. ด้านกลยุทธ์											
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการกำหนดนโยบาย กลยุทธ์ ที่ทำให้แผนการดำเนินงานไม่สามารถบรรลุวัตถุประสงค์											
6.1	ทิศทาง/แนวทางการพัฒนาด้านเทคโนโลยีสารสนเทศไม่ชัดเจน/ไม่สอดคล้องกับการขยายการบูรณาการร่วมกัน	ไม่สามารถลดความซ้ำซ้อนของกระบวนการหรือระบบงานได้ ทำให้ขาดประสิทธิภาพในการดำเนินงานและการใช้งบประมาณไม่คุ้มค่า	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน	3	2	6	ควบคุมความเสี่ยง	- จัดทำ/ทบทวนสถาปัตยกรรมองค์กรของหน่วยงาน (Enterprise Architecture : EA) - นำสถาปัตยกรรมองค์กรของหน่วยงานมาใช้เป็นกรอบแนวทางในการพัฒนาระบบเทคโนโลยีสารสนเทศของหน่วยงาน - ส่งเสริมและสนับสนุนให้บุคลากรทุกระดับเข้าใจและให้ความสำคัญในการจัดทำสถาปัตยกรรมองค์กรของหน่วยงาน - ทบทวน/ขับเคลื่อนการดำเนินงานตามแผนดิจิทัล พม.	2	1	2
7. ด้านการเงิน (งบประมาณ)											
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากการได้รับการสนับสนุนงบประมาณไม่เพียงพอ/การเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลาเบิกจ่าย งบประมาณไม่ทันตามกำหนดเวลา											
7.1	การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่างๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนัก แต่จะเป็นการปรับลดตามเปอร์เซ็นต์ที่หน่วยงานกำหนด ทำให้ได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ขาดงบประมาณในการบริหารจัดการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน	3	2	6	ควบคุมความเสี่ยง	- จัดลำดับความสำคัญของโครงการที่จำเป็นต้องดำเนินการให้อยู่ในลำดับต้นๆ - จัดทำความเสี่ยงแนบไปกับโครงการ และให้มีการถ่วงน้ำหนักของโครงการที่เป็นโครงการประเภทเดียวกัน - ชี้แจงผลกระทบหากไม่ได้ดำเนินโครงการ และการยอมรับความเสี่ยง - ปรับลดขอบเขตงานลงตามงบประมาณที่ได้รับ - ขอใช้เงินเหลือจ่ายสำหรับเพิ่มประสิทธิภาพ	3	1	3
8. ด้านการบริหารจัดการ											
วัตถุประสงค์ : เพื่อเป็นการควบคุมความเสี่ยงอันเนื่องมาจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี											
8.1	กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน - อนุมัติโครงการล่าช้า - ไม่สามารถประกาศผลผู้ชนะการประกวดราคา - สัญญาไม่ตรงตามร่างข้อกำหนด - ไม่มีผู้เข้าประกวดราคาได้ทันเวลา	การดำเนินโครงการเกิดความล่าช้า ทำให้ขาดประสิทธิภาพในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ	- หน่วยงาน - ผู้ใช้งานระบบ - เจ้าหน้าที่ผู้ปฏิบัติงาน	3	2	6	ควบคุมความเสี่ยง	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - ติดตามการอนุมัติโครงการให้เป็นไปตามแผนปฏิบัติการอย่างจริงจัง กรณีผู้บริหารอนุมัติโครงการล่าช้า ต้องขอวาระชี้แจงเหตุผลความจำเป็นและจัดลำดับความสำคัญเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนดโดยการประสานกับเจ้าหน้าที่พัสดุ ก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด	2	2	4



3.7 การจัดทำแผนภูมิความเสี่ยง (Risk Map) ก่อนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์



3.8 การจัดทำแผนภูมิความเสี่ยง (Risk Map) หลังการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์





ปีงบประมาณ พ.ศ. 2568 ศทส. ได้ทำการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ และได้จัดทำแผนบริหารจัดการความเสี่ยง กำหนดกิจกรรม เป้าหมายการดำเนินการ โดยเพิ่มมาตรการจัดการความเสี่ยง และควบคุมความเสี่ยงให้อยู่ในระดับคะแนนที่ยอมรับได้ ซึ่งผลจากการวิเคราะห์และประเมินความเสี่ยง สรุปได้ดังนี้

ความเสี่ยงที่มีคะแนนอยู่ในระดับค่อนข้างสูง 11 ปัจจัยเสี่ยง คือ

ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

รหัส 1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ ค่าคะแนนระดับ 8

รหัส 1.4 มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต ประตูปิดไม่สนิท อุปกรณ์ควบคุมการเข้าถึงเสีย มีการใช้พื้นที่ทางเดินร่วมกับห้องปฏิบัติการคอมพิวเตอร์ (ห้องอบรม) ค่าคะแนนระดับ 8

ความเสี่ยงด้านบุคลากร

รหัส 2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึงและใช้งานระบบสารสนเทศ ค่าคะแนนระดับ 12

รหัส 2.4 การจ้างบุคคลภายนอกที่ขาดความระมัดระวังในการดูแลข้อมูลที่สำคัญของหน่วยงาน 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 20

3.9 แผนปฏิบัติการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

ประจำปีงบประมาณ พ.ศ. 2568

ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2568												ผู้รับผิดชอบ	
		ค.ค.67	พ.ย.67	ธ.ค.67	ม.ค.68	ก.พ.68	มี.ค.68	เม.ย.68	พ.ค.68	มิ.ย.68	ก.ค.68	ส.ค.68	ก.ย.68		ติดตาม
1. ด้านกายภาพและสิ่งแวดล้อม															
วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคามทางธรรมชาติ สิ่งแวดล้อมและผลกระทบที่เกิดขึ้น															
1.2 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบความพร้อมใช้งานของระบบสำรองไฟฟ้า(UPS)/แบตเตอรี่สำรองไฟ เป็นประจำทุก 3 เดือน - มีแผนการบำรุงรักษาระบบไฟฟ้าของอาคารสถานที่ ปีละ 1 ครั้ง	✖	—	—	—	—	—	—	—	—	—	—	—	📍	ศทส.
1.4 มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. โดยไม่ได้รับอนุญาต	- บันทึกรายชื่อ/เวลา/เรื่องที่ทำเนิการ ในเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท	✖	—	—	—	—	—	—	—	—	—	—	—	📍	ศทส.
- ประตูปิดไม่สนิท	- ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน														
- อุปกรณ์ควบคุมการเข้าถึงเสีย	- มีการใช้รหัสแบบ Two-Factor Authentication (2FA)														
- มีการใช้พื้นที่ทางเดินร่วมกับห้องปฏิบัติการคอมพิวเตอร์ (ห้องอบรม)															



ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2568												ผู้รับผิดชอบ
		ต.ค.67	พ.ย.67	ธ.ค.67	ม.ค.68	ก.พ.68	มี.ค.68	เม.ย.68	พ.ค.68	มิ.ย.68	ก.ค.68	ส.ค.68	ก.ย.68	
2. ด้านบุคลากร														
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ														
2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนด ไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึงและการใช้งานระบบสารสนเทศ	มีการบริหารจัดการ การควบคุม และเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก - การมอบหมายหน้าที่ความรับผิดชอบที่ชัดเจน - การกำกับติดตามการดำเนินงาน - ปรับปรุงระบบสารสนเทศให้มีความปลอดภัยมากขึ้น เช่น Session Time Out - พิจารณาใช้ดิจิทัล ID เพิ่มเติม เช่น THAID													ศทส.
2.4 การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน มีการทำข้อตกลงการห้ามเปิดเผยข้อมูล (NDA) และการใช้หรือประมวลผลข้อมูลส่วนบุคคล (DPA)													ศทส.
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร														
วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้ง และไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ														
3.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบปฏิบัติการ (Operating System) ในทุกระดับ ผู้ใช้งานขาดประสิทธิภาพ	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลงปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ													ศทส.



ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2568												ผู้รับ ผิดชอบ
		ต.ค.67	พ.ย.67	ธ.ค.67	ม.ค.68	ก.พ.68	มี.ค.68	เม.ย.68	พ.ค.68	มิ.ย.68	ก.ค.68	ส.ค.68	ก.ย.68	
3.6 ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน - เข้าบริการศูนย์รับมือและตอบสนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการแจ้งเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์ - เข้าร่วมกับหน่วยงานภายนอกด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ สำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ในการเฝ้าระวังภัยทางไซเบอร์													ศทส.
3.7 ขาดการป้องกันหรือตรวจจับไวรัส	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ													ศทส.



ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2568												ผู้รับ ผิดชอบ
		ต.ค.67	พ.ย.67	ธ.ค.67	ม.ค.68	ก.พ.68	มี.ค.68	เม.ย.68	พ.ค.68	มิ.ย.68	ก.ค.68	ส.ค.68	ก.ย.68	
5. ด้านระบบข้อมูล														
วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศ ฐานข้อมูลต่างๆ ถูกทำลายจากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการ หรือออกรายงานได้														
5.2 ขาดการบริหารจัดการสิทธิ์ผู้ใช้งาน และการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลงปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ - ระบุคุณลักษณะทางเทคนิคในการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบ ภายใต้ขอบเขตงานการพัฒนาระบบสารสนเทศ													ศทส.
5.3 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบ หรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ - ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - สำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง													ศทส.



ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2568												ผู้รับ ผิดชอบ
		ต.ค.67	พ.ย.67	ธ.ค.67	ม.ค.68	ก.พ.68	มี.ค.68	เม.ย.68	พ.ค.68	มิ.ย.68	ก.ค.68	ส.ค.68	ก.ย.68	
	- มีการตรวจสอบช่องโหว่และตรวจสอบระบบ อย่างน้อยปีละ 1 ครั้ง													
5.4 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง (VPN หรือ Virtual Private Network คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ต และตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้) - การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งานทุก 6 เดือน													ศทส.
5.7 เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง - พิจารณาจัดทำแผน/ปรับปรุงระบบ													ศทส.
5.8 การนำเข้าข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	- มีการควบคุมคุณภาพข้อมูลให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล - สร้างความตระหนักรู้ในการนำเข้าข้อมูล - มอบรางวัลเพื่อเป็นกำลังใจให้กับหน่วยงานที่มีการนำเข้าข้อมูลผิดพลาดน้อย													ศทส.



ปัจจัยเสี่ยง	แนวทางการควบคุม	ปีงบประมาณ พ.ศ. 2568												ผู้รับ ผิดชอบ
		ต.ค.67	พ.ย.67	ธ.ค.67	ม.ค.68	ก.พ.68	มี.ค.68	เม.ย.68	พ.ค.68	มิ.ย.68	ก.ค.68	ส.ค.68	ก.ย.68	
5.9 การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	- กำหนดตัวชี้วัดในการบันทึกข้อมูล - ออกประกาศเกี่ยวกับการนำเข้าข้อมูลสารสนเทศ - ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ													ศทส.

หมายเหตุ : ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปี พ.ศ. 2568 จะเริ่มตั้งแต่ ตุลาคม 2567 – กันยายน 2568 (เป็นการควบคุมตามรอบปีงบประมาณประจำปี พ.ศ. 2568)



บทที่ 4

สรุปผลและข้อเสนอแนะ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์เป็นสิ่งจำเป็นอย่างยิ่งในองค์กรยุคดิจิทัล เนื่องจากระบบฐานข้อมูลมีบทบาทสำคัญในการดำเนินงาน ซึ่งเหตุผลหลักที่ต้องมีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ คือ

- 1. ปกป้องข้อมูลและทรัพย์สินขององค์กร** หากไม่มีมาตรการบริหารความเสี่ยงที่เหมาะสม อาจเกิดการรั่วไหลของข้อมูลสำคัญ หรือถูกโจมตีโดยภัยไซเบอร์
- 2. ลดผลกระทบจากภัยคุกคามไซเบอร์** การโจมตีแบบมัลแวร์ ฟิชชิง และแรนซัมแวร์ สามารถสร้างความเสียหายอย่างหนักต่อระบบข้อมูลและการดำเนินงานของหน่วยงาน การบริหารความเสี่ยงจะช่วยป้องกันและลดผลกระทบที่อาจเกิดขึ้นได้
- 3. เพิ่มความน่าเชื่อถือและความปลอดภัยของระบบไอที** หากหน่วยงานมีมาตรการจัดการความเสี่ยงที่ดี จะสามารถรับรองได้ว่าระบบไอทีมีความปลอดภัยและเชื่อถือได้
- 4. ปฏิบัติตามกฎหมายและข้อกำหนดด้านความปลอดภัย** หลายประเทศมีข้อบังคับด้านการคุ้มครองข้อมูล เช่น GDPR และ PDPA ซึ่งกำหนดให้องค์กรต้องมีมาตรการในการปกป้องข้อมูลส่วนบุคคล
- 5. ลดค่าใช้จ่ายจากความเสียหายและการฟื้นฟูระบบ** หากหน่วยงานถูกโจมตีทางไซเบอร์ ต้องเสียค่าใช้จ่ายในการกู้คืนข้อมูล การบริหารความเสี่ยงช่วยลดโอกาสเกิดเหตุการณ์เหล่านี้และลดต้นทุนในการแก้ไขปัญหา
- 6. รองรับการพัฒนาและเปลี่ยนแปลงเทคโนโลยี** เทคโนโลยีมีการเปลี่ยนแปลงอยู่ตลอดเวลา ภัยคุกคามทางไซเบอร์มีการพัฒนาอย่างต่อเนื่อง หากหน่วยงานมีระบบบริหารความเสี่ยงที่ดี ก็สามารถปรับตัวและป้องกันภัยคุกคามใหม่ๆ ได้อย่างมีประสิทธิภาพ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์เป็นเครื่องมือสำคัญในการสร้างความมั่นคงให้กับองค์กร หากไม่มีการบริหารความเสี่ยงหน่วยงานอาจต้องเผชิญกับภัยคุกคามที่ส่งผลเสียชื่อเสียงและองค์กร

แนวโน้มในอนาคตของภัยคุกคามไซเบอร์ องค์กรกำลังเผชิญกับความท้าทายที่ซับซ้อนและรุนแรงขึ้น เนื่องจากเทคโนโลยีมีการพัฒนาอย่างรวดเร็ว หน่วยงานต้องเตรียมรับมือ ดังนี้

- 1. การโจมตีแบบเรียกค่าไถ่ (Ransomware) ที่ซับซ้อนขึ้น** แฮกเกอร์จะใช้เทคนิคที่ซับซ้อนมากขึ้น เช่น การเข้ารหัสข้อมูลหลายชั้น และการโจมตีแบบกำหนดเป้าหมายเฉพาะองค์กร
- 2. การโจมตีห่วงโซ่อุปทาน (Supply Chain Attacks)** องค์กรต้องเผชิญกับการโจมตีที่มุ่งเป้าไปยังผู้ให้บริการซอฟต์แวร์หรือฮาร์ดแวร์ เพื่อเข้าถึงระบบขององค์กรโดยอ้อม
- 3. ภัยคุกคามที่ขับเคลื่อนด้วย AI (AI-Powered Attacks)** แฮกเกอร์เริ่มใช้ AI ในการสร้างอีเมลฟิชชิงที่แนบเนียนขึ้น และวิเคราะห์ช่องโหว่ของระบบอย่างรวดเร็ว
- 4. การโจมตีอุปกรณ์ IoT (Internet of Things)** อุปกรณ์ IoT ที่เชื่อมต่อกับเครือข่ายองค์กรจะเป็นเป้าหมายหลักของการโจมตี เนื่องจากมีช่องโหว่ด้านความปลอดภัย
- 5. ภัยคุกคามจากภายใน (Insider Threats)** บุคลากรภายในองค์กรอาจเป็นช่องทางให้เกิดการรั่วไหลของข้อมูล หรือถูกล่อลวงให้เปิดเผยข้อมูลสำคัญ



6. การโจมตีบนระบบคลาวด์ (Cloud Attacks) ระบบคลาวด์จะเป็นเป้าหมายหลักของการโจมตี โดยเฉพาะการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตและการโจมตีแบบ DDoS

7. การใช้ Deepfake และ Social Engineering การปลอมแปลงข้อมูลด้วยเทคโนโลยี Deepfake การหลอกลวงจะมีความแนบเนียนมากขึ้น ทำให้การตรวจจับทำได้ยาก องค์กรต้องเตรียมพร้อมรับมือกับภัยคุกคามไซเบอร์ที่มีความซับซ้อนมากขึ้น โดยการใช้มาตรการป้องกันที่ทันสมัย เช่น การใช้ระบบ AI สำหรับตรวจจับภัยคุกคาม การอบรมพนักงาน การใช้มาตรฐานความปลอดภัยที่เข้มงวด

การจัดการความเสี่ยง (Risk Management) กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสียหายมากที่สุด อันเนื่องมาจากความเสี่ยงที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งเมื่อมีการปรับเปลี่ยน โดยเทคโนโลยีสารสนเทศและการสื่อสาร เข้ามามีบทบาทสำคัญเป็นกลไกในการขับเคลื่อนการดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีการปรับเปลี่ยน โดยเทคโนโลยีสารสนเทศและการสื่อสารช่วยทำให้ความซับซ้อนของกระบวนการทำงานลดลง และสามารถให้บริการที่รวดเร็ว และการเข้าถึงบริการที่ง่ายขึ้นสะดวกขึ้น ซึ่งในแต่ละวันมีปริมาณข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกให้กับปฏิบัติงานของทุกหน่วยงานภายใน สป.พม.

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

การทบทวนและจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568 เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่ หรือความเสี่ยงที่ได้จัดการไปแล้ว แต่ยังควบคุมความเสี่ยงต่อ ประกอบการตัดสินใจว่าจะต้องจัดการความเสี่ยง ลดโอกาส/ความเสียหายที่จะเกิดขึ้น ให้อยู่ในระดับที่ยอมรับได้ จัดการความเสี่ยงจากความเสี่ยงสูง โดยจะต้องมีมาตรการ แนวทาง/กิจกรรมควบคุม เพื่อให้ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ตามสถานการณ์จริง

4.1 การวิเคราะห์ปัจจัยเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. ประจำปีงบประมาณ พ.ศ. 2568

การระบุความเสี่ยง (Risk Identification) เป็นการบ่งชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่ สป.พม. เผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ ในปีงบประมาณ พ.ศ. 2568 มีผลคะแนนที่ได้จัดการความเสี่ยง เพื่อควบคุมและจัดทำแผนความเสี่ยงให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยเมื่อมีการจัดการความเสี่ยงและควบคุมความเสี่ยงได้ ระดับความเสี่ยงจะมีค่าคะแนนที่ค่อนข้างต่ำ และ ต่ำ ที่สรุปได้ดังนี้



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับคะแนน	
1. ด้านกายภาพและสิ่งแวดล้อม วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยและป้องกัน ความเสี่ยงจากภัยคุกคามทางธรรมชาติ 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 - มีการใช้พื้นที่ทางเดินร่วมกับห้องปฏิบัติการคอมพิวเตอร์ (ห้องอบรม)	1	3	3	- บันทึกรายชื่อ/เวลา/เรื่องที่ทำดำเนินการในเข้าออกศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. ทุกครั้ง - มีสัญญาณแจ้งเตือนเมื่อประตูปิดไม่สนิท - ตรวจสอบอุปกรณ์การเข้าถึงเป็นประจำทุก 3 เดือน - มีการใช้รหัสแบบ Two-Factor Authentication (2FA)
2. ด้านบุคลากร วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากดำเนินงานของบุคลากรด้านเทคโนโลยีสารสนเทศ	2.1	ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์การเข้าถึง และการใช้งานระบบสารสนเทศ	1	3	3	มีการบริหารจัดการการควบคุมและเข้าถึงระบบ ดังนี้ - การใช้งานสารสนเทศ - ระบบเครือข่าย - ระบบปฏิบัติการ - โปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ - การเข้าถึงของหน่วยงานภายนอก - การกำกับติดตามการดำเนินงาน - ปรับปรุงระบบสารสนเทศให้มีความปลอดภัยมากขึ้น เช่น Session Time Out - พิจารณาใช้ดิจิทัล ID เพิ่มเติม เช่น THAID
	2.4	การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน	1	3	3	- มีการตรวจสอบ ติดตาม เพื่อป้องกันการผิดพลาดในการใช้ข้อมูล - มีข้อกำหนดการจ้างในการติดตามและตรวจรับงาน มีการทำข้อตกลงการห้ามเปิดเผยข้อมูล (NDA) และการใช้หรือประมวลผลข้อมูลส่วนบุคคล (DPA)



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับคะแนน	
3. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ : เพื่อป้องกันและแก้ไขข้อผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ไม่ว่าจะเกิดจากการทำงานผิดพลาดของอุปกรณ์ หรือการเคลื่อนย้ายอุปกรณ์ การติดตั้งและไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ	3.3	การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารและระบบปฏิบัติการ (Operating System) ในทุกๆ ระดับผู้ใช้งานขาดประสิทธิภาพ	2	2	4	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์ เป็นประจำทุก 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 - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อ Update อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ติดตามและรายงานผล ทุก 3 เดือน - เข้าบริการศูนย์รับมือและตอบสนองภัยคุกคามทางไซเบอร์ - ดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ - มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ - ดำเนินการแจ้งเจ้าหน้าที่ในการติดตามและเฝ้าระวังภัยทางไซเบอร์



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับคะแนน	
						- เข้าร่วมกับหน่วยงานภายนอกด้าน การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ สำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ในการเฝ้าระวังภัยทางไซเบอร์
	3.7	ขาดการป้องกันหรือตรวจจับไวรัส	2	2	4	- จัดหาและติดตั้งโปรแกรมป้องกันไวรัส - Update โปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ
5. ด้านระบบข้อมูล วัตถุประสงค์ : เพื่อควบคุมความเสี่ยงที่เกิดจากระบบสารสนเทศฐานข้อมูลต่างๆ ถูกทำลายจากผู้บุกรุกข้อมูล การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทั้งจากคน จากธรรมชาติ หรือเหตุการณ์ใดๆ ที่ทำให้เกิดความไม่มั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงจากการดำเนินงานที่ทำให้ระบบฐานข้อมูลไม่สามารถเชื่อมโยง บูรณาการหรือออกรายงานได้	5.2	ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย - การทบทวนสิทธิ์ผู้ใช้งาน - การบริหารจัดการรหัสผ่าน - การยุติการใช้บริการตามเวลาที่กำหนด (Session Time Out) - การหน่วงเวลาเมื่อล็อกอินผิดเพื่อป้องกันการโจมตี	2	2	4	- มีการกำหนดสิทธิ์การเข้าถึงงานระบบสารสนเทศตามระดับผู้ใช้งาน/ผู้ดูแลระบบ/admin - มีการทบทวนสิทธิ์เป็นประจำทุก 6 เดือน โดยการเปลี่ยนแปลง ปรับปรุง เพิ่มเติม แก้ไข - มีการติดตามและจัดทำรายงานผลการกำหนดสิทธิ์และทบทวนสิทธิ์ทุก 6 เดือน - พิจารณาใช้งาน 2FA หรือ MFA มาใช้งานร่วมกับการใช้รหัสผ่านในระบบที่สำคัญ - ระบุคุณลักษณะทางเทคนิคในการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบภายใต้ขอบเขตงานการพัฒนาระบบสารสนเทศ
	5.3	การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย	2	3	6	- ติดตั้งโปรแกรมป้องกันไวรัส และ patch ทุกครั้งที่เจ้าของผลิตภัณฑ์อัปเดต - ติดตั้ง patch ของระบบปฏิบัติการทุกสัปดาห์ - เปลี่ยนรหัสผ่านตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ทุก 6 เดือน - มีการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับคะแนน	
						- ผู้มีสิทธิ์เข้าถึงระบบต้องเข้าผ่านระบบภายใน หรือ VPN ตามข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - สำรองข้อมูลระบบฐานข้อมูลอย่างสม่ำเสมอ อย่างน้อยเดือนละ 1 ครั้ง - มีการตรวจสอบช่องโหว่และตรวจสอบระบบ อย่างน้อยปีละ 1 ครั้ง
	5.4	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	2	2	4	มีการทำ VPN สำหรับผู้ปฏิบัติงานในระยะไกลในการเข้าถึง (VPN หรือ Virtual Private Network คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัว VPN จะสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้และอินเทอร์เน็ต สามารถซ่อนกิจกรรมบนอินเทอร์เน็ตและตำแหน่งของผู้ใช้เพื่อหลีกเลี่ยงการติดตามได้) - การติดตามตรวจสอบการเข้าใช้งานระบบ VPN - การทบทวนสิทธิ์บัญชีผู้ใช้งาน ทุก 6 เดือน
	5.7	เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์	1	3	3	- ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - Update Software ระบบต่างๆอย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศและประชาสัมพันธ์ให้ผู้ใช้ได้รับทราบอย่างต่อเนื่อง - พิจารณาจัดทำแผน/ปรับปรุงระบบ
	5.8	การนำเข้าข้อมูลผิดพลาด ทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)	2	2	4	- มีการควบคุมคุณภาพข้อมูล ให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) - มีการปรับปรุงระบบให้สามารถตรวจสอบเงื่อนไขการนำเข้าข้อมูล - สร้างความตระหนักรู้ในการนำเข้าข้อมูล



ประเภทความเสี่ยง	รหัส	ปัจจัยเสี่ยง	หลังมีแนวทางการควบคุม			แนวทางการควบคุม
			โอกาส	ผลกระทบ	ระดับคะแนน	
						- มอบรางวัลเพื่อเป็นกำลังใจให้กับหน่วยงานที่มีการนำเข้าสู่ข้อมูลผิดพลาดน้อย
	5.9	การนำเข้าสู่ข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน	1	3	3	- กำหนดตัวชี้วัดในการบันทึกข้อมูล - ออกประกาศเกี่ยวกับการนำเข้าสู่ข้อมูลสารสนเทศ - ติดตามผลการบันทึกข้อมูลอย่างต่อเนื่องและรายงานให้ผู้บริหารทราบ

4.2 สรุปผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.

ประจำปีงบประมาณ พ.ศ. 2568

ปีงบประมาณ พ.ศ. 2568 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 มีการใช้พื้นที่ทางเดินร่วมกับห้องปฏิบัติการคอมพิวเตอร์ (ห้องอบรม) ซึ่งความเสียหายที่อาจเกิดขึ้น คือ มีการขโมยข้อมูลหรืออุปกรณ์ในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. มีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่าย ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 8 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

2) ความเสี่ยงด้านบุคลากร ปัจจัยเสี่ยง จำนวน 2 ปัจจัย คือ

รหัส 2.1 ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วน ในการบริหารจัดการสิทธิ์ การเข้าถึง และการใช้งานระบบสารสนเทศ ทำให้มีความเสี่ยงที่อาจเกิดความเสียหายกับระบบสารสนเทศ ทำให้ระบบสารสนเทศขาดความมั่นคงปลอดภัย ข้อมูลขาดความน่าเชื่อถือ ข้อมูลรั่วไหล ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 12 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม



รหัส 2.4 การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลที่สำคัญของหน่วยงาน ข้อมูลของหน่วยงานเกิดการรั่วไหล อันเนื่องมาจากผู้รับจ้างประมาทเลินเล่อ ขาดความตระหนักในการดูแลข้อมูล สำคัญระหว่างการบำรุงรักษา/พัฒนาระบบ หน่วยงานได้รับความเสียหายด้านภาพลักษณ์และชื่อเสียง ก่อนจัดการ ความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 8 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนน ให้อยู่ในระดับที่ 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร ปัจจัยเสี่ยง จำนวน 3 ปัจจัย คือ

รหัส 3.3 การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร และระบบ ปฏิบัติการ (Operating System) ในทุกๆ ระดับ ผู้ใช้งานขาดประสิทธิภาพ เกิดความผิดพลาดในการให้บริการระบบ สารสนเทศและการสื่อสารทั้งระบบ ระบบตัวตนผู้ใช้งานไม่ได้ หากผู้กระทำความผิดไม่ได้ ก่อนจัดการความเสี่ยงมีค่า คะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับ ที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยัง ระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.6 ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ข้อมูลถูกแก้ไขเปลี่ยนแปลงหรือถูกทำลาย การทำงานของระบบคอมพิวเตอร์ถูกแก้ไขเปลี่ยนแปลง ทำลาย หรืออาจกระทำการแก้ไขสิทธิ์ของบุคคลที่มีหน้าที่รับผิดชอบ ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ ทรัพยากรในระบบถูกนำไปใช้ทำให้ประสิทธิภาพของระบบลดลง ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 25 คือ สูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่า คะแนนให้อยู่ในระดับที่ 6 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความ เสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 3.7 ขาดการป้องกันหรือตรวจจับไวรัส เกิดไวรัสรบกวนการทำงานและก่อให้เกิดความเสียหาย แก่ระบบเครือข่าย ระบบสารสนเทศและฐานข้อมูล ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอ ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่า คะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

4) ความเสี่ยงด้านระบบข้อมูล ปัจจัยเสี่ยง จำนวน 6 ปัจจัย คือ

รหัส 5.2 ขาดการบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความ มั่นคงปลอดภัย การทบทวนสิทธิ์ผู้ใช้งาน การบริหารจัดการรหัสผ่าน การยุติการให้บริการตามเวลาที่กำหนด (Session Time Out) การหน่วงเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี เกิดความผิดพลาดในการให้บริการระบบ สารสนเทศและการสื่อสารทั้งระบบ ระบบตัวตนผู้ใช้งานได้ไม่ได้ หากผู้กระทำความผิดไม่ได้ การถูกยึดครองระบบจาก ผู้ไม่หวังดี (Hacker) ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 9 คือ ค่อนข้างสูง เมื่อได้รับการจัดการความ เสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 4 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการ



ควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.3 การโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย การให้บริการระบบสารสนเทศหยุดชะงัก ส่งผลต่อการให้บริการประชาชนและผู้ให้บริการทั่วไปไม่มีประสิทธิภาพ ข้อมูลสารสนเทศและการทำงานของระบบเสียหาย ส่งผลให้การประมวลผลไม่ถูกต้องครบถ้วน ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข ก่อนจัดการความเสี่ยงมีค่าคะแนนอยู่ในระดับที่ 20 คือ สูง เมื่อได้รับการจัดการความเสี่ยงแล้ว สามารถปรับลดค่าคะแนนให้อยู่ในระดับที่ 6 คือ ค่อนข้างต่ำ ซึ่งเป็นระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ หรือจัดการให้มีค่าคะแนนที่ต่ำลง จนสามารถควบคุมและยอมรับได้ต่อไป

รหัส 5.4 การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง อาจถูกลักลอบขโมยข้อมูล หรือข้อมูลถูกทำลาย เกิดความสูญเสีย ไม่มีผู้รับผิดชอบเนื่องจากไม่สามารถยืนยันตัวตนของผู้ใช้งานที่ทำให้เกิดความเสียหายต่อระบบได้ 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 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

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 3 คือ ต่ำ ซึ่งเป็นระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม



4.3 ข้อเสนอแนะจากผลการสอบทานของกลุ่มตรวจสอบภายใน สป.พม.

สรุปข้อเสนอแนะในปีงบประมาณ พ.ศ. 2567 ของกลุ่มตรวจสอบภายใน สป.พม. เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม. มีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้น และไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ พร้อมวางแผนแนวทางในการป้องกันภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้น สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ ศทส. สป.พม. ดำเนินการ ดังนี้

1. ปักจายเสี่ยงด้านการควบคุมการเข้าถึงด้านกายภาพและสิ่งแวดล้อม ในการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม. เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น ให้จัดทำป้ายเพื่อแสดงสัญลักษณ์ ดังนี้
 - 1.1 ห้ามบุคคลภายนอกเข้าไปในห้องแม่ข่ายโดยไม่มีกิจที่จำเป็น
 - 1.2 ห้ามสูบบุหรี่ และนำอาหารเครื่องดื่มเข้าไปในบริเวณห้องแม่ข่าย
 - 1.3 ห้ามนำสิ่งของที่ไม่เกี่ยวข้องเข้ามาในห้องแม่ข่าย
2. ปักจายเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล ความเสี่ยงอยู่ในระดับที่พอยอมรับได้ต้องมีกิจกรรมควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปอยู่ในระดับที่ยอมรับไม่ได้ ความเสี่ยงที่อาจเกิดขึ้น คือ การถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่คอมพิวเตอร์แม่ข่าย (Server) อาทิ
 - 2.1 ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ
 - 2.2 ตรวจสอบโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ
 - 2.3 ควรมีการกำหนดระยะเวลาให้ชัดเจนในการตรวจสอบการบุกรุกเครือข่ายและ Update ระบบอย่างสม่ำเสมอหรือมีการแจ้งเตือนจากหน่วยงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อความปลอดภัยและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
3. ปักจายเสี่ยงด้านระบบข้อมูล ความเสียหายที่อาจเกิดขึ้น คือ การโจมตีโดยบุคคลที่ไม่มีสิทธิ์หรือลักลอบเข้าสู่ระบบฐานข้อมูล การดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย การกำหนดสิทธิผู้ใช้งานและทบทวนสิทธิ์ ควรกำหนดระยะเวลาให้ชัดเจน เช่น อย่างน้อย 3 เดือน/ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งานในระบบ เพื่อป้องกันผู้ที่ไม่สิทธิเข้าถึงข้อมูล
4. ดำเนินการตามแนวทางการควบคุมความเสี่ยงของแต่ละปักจายเสี่ยง และติดตามการบริหารจัดการความเสี่ยงอย่างต่อเนื่อง



- ภาคผนวก -



ประกาศกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๗

โดยที่พระราชบัญญัติกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ ได้กำหนดให้ หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับ หน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำมีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐดำเนินการ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานในสังกัด เป็นไปในทิศทางเดียวกัน กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ จึงเห็นควรกำหนดแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ดังต่อไปนี้

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

ข้อ ๒ ประกาศนี้มีผลบังคับใช้ตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

หน่วยงาน หมายความว่า หน่วยงานในสังกัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับ ความมั่นคงปลอดภัย

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

ข้อ ๔ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงานของรัฐนั้นๆ

(๓) กำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

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

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

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

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

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

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

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

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในกรณีที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสม เพื่อป้องกันการไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในกรณีที่ไม่มีผู้ดูแล

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

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘ นโยบายการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

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

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

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

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

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

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

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

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

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

(๔) การใช้งานโปรแกรมรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย ที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

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

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

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

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

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๑ นโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๒ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อยดังนี้

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

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

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

และการสื่อสารของหน่วยงานเกิดความเสียหาย หรือเป็นอันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ตามแนวทางต่อไปนี้

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

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

(๓) ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานต้องจัดทำแนวปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวง

ข้อ ๑๕ หน่วยงานต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๓ พฤศจิกายน พ.ศ. ๒๕๕๗



(นายวิเชียร ขวาลิต)

ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 67
	เรื่องที่ 3 : การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0103

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์

วัตถุประสงค์

เพื่อเป็นแนวทางในการวางกรอบและกระบวนการบริหารและจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ของหน่วยงาน และต้องมีการตรวจสอบและปรับปรุงอย่างต่อเนื่อง เพื่อให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไปและภัยคุกคามใหม่ๆ ที่เกิดขึ้น

ผู้รับผิดชอบและผู้เกี่ยวข้อง

1. **หน่วยงานที่รับผิดชอบ** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
2. **คณะกรรมการ** หมายถึง คณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
3. **เจ้าหน้าที่/ผู้ดูแลระบบ** หมายถึง เจ้าหน้าที่ของ ศทส. ที่ได้รับมอบหมาย
4. **ผู้ใช้งาน** หมายถึง เจ้าหน้าที่ของ สป.พม. หรือบุคคลจากหน่วยงานภายนอก ที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สป.พม.

แนวปฏิบัติ

1. การดำเนินงาน

- 1.1 แต่งตั้งคณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนา ระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นประธาน
- 1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาศักยภาพและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ
- 1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน และเตรียมความพร้อมเพื่อรับการตรวจสอบและประเมิน ความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผนฯ
- 1.6 ทบทวน/ปรับปรุงแผนฯ ปีละ 1 ครั้ง

2. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์

2.1 การประเมินความเสี่ยง (Risk Assessment)

- 2.1.1 การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าว อาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากรหรือปัจจัยภายนอก

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 67
	เรื่องที่ 3 : การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0103

2.1.2 การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

2.1.3 การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานของหน่วยงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

2.2 ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการฯ ประกาศกำหนด

2.3 ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- คำอธิบายของความเสี่ยง (Description of the Risk)
- โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- การจัดการความเสี่ยง (Risk Treatment)
- เจ้าของความเสี่ยง (Risk Owner)
- สถานะของการจัดการความเสี่ยง (Status of the Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

2.4 การจัดการความเสี่ยง (Risk Treatment) ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสม สอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินงาน ให้สอดคล้องกับสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

2.5 การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

2.6 การรายงานความเสี่ยง (Risk Reporting) ต้องรายงานระดับความเสี่ยงและผลกระทบการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการกำกับและดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจ

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 67
	เรื่องที่ 3 : การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0103

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 67
	เรื่องที่ 4 : การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0104

การตรวจประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

วัตถุประสงค์

เพื่อให้หน่วยงานมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ที่อาจเกิดขึ้น ทำให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของหน่วยงาน โดยการตรวจสอบและประเมินความเสี่ยงนั้น จะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

ผู้รับผิดชอบและผู้เกี่ยวข้อง

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

แนวปฏิบัติ

1. การดำเนินงาน

- 1.1 แต่งตั้งคณะทำงานภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม. ประกอบด้วย กลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร กลุ่มการพัฒนาระบบสารสนเทศ และกลุ่มการวิเคราะห์ข้อมูล โดยมีผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นประธาน
- 1.2 ประชุมคณะทำงานฯ เพื่อจัดทำแผนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.3 นำเสนอร่างแผนฯ ต่อปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เพื่อขอความเห็นชอบ
- 1.4 มอบหมายเจ้าหน้าที่ดำเนินงานตามแผน และเตรียมความพร้อมเพื่อรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 1.5 กำกับ ติดตาม และประเมินผลการดำเนินงานตามแผนฯ
- 1.6 ทบทวน/ปรับปรุงแผนฯ ปีละ 1 ครั้ง

	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สป.พม.	
	ส่วนที่ 1 : การระบุ และเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง (Identify)	แก้ไขล่าสุด : ต.ค. 67
	เรื่องที่ 4 : การตรวจประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์	รหัสเอกสาร : IC-0104

2. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์

- 2.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. ปีละ 1 ครั้ง โดยดำเนินการให้สอดคล้องตามแผนในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 2.2 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. ให้ดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor)
- 2.3 กำหนดขอบเขตและขั้นตอนปฏิบัติสำหรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม.
- 2.4 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. ที่มีความสำคัญหรือเป็นข้อมูลส่วนบุคคล มีข้อจำกัด ดังนี้
 - 2.4.1 ผู้ตรวจสอบภายในหน่วยงานของรัฐ สามารถเข้าถึงข้อมูลที่ต้องตรวจสอบในลักษณะที่อ่านได้เพียงอย่างเดียว
 - 2.4.2 ในกรณีที่ผู้ตรวจสอบภายในหน่วยงานของรัฐจำเป็นต้องเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้ จะต้องดำเนินการด้วยวิธีการที่ปลอดภัย
 - 2.4.3 มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบภายในหน่วยงานของรัฐทำงานบนข้อมูลสำเนา
 - 2.4.4 มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ
 - 2.4.5 มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ
- 2.5 ผู้ตรวจสอบภายในหน่วยงานของรัฐ สรุปรายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและไซเบอร์ของ สป.พม. เสนอต่อ ปพม. และ ศทส. เพื่อรับทราบ
- 2.6 ทบทวน/ปรับปรุงการดำเนินงานตามที่ผู้ตรวจสอบภายในหน่วยงานของรัฐให้ข้อเสนอแนะต่อไป



คำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ที่ **๓๓๕** / ๒๕๖๘

เรื่อง แต่งตั้งคณะทำงานในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๕ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อเป็นกลไกในการขับเคลื่อนการทำงาน ให้เป็นไปด้วยความเรียบร้อย และบรรลุตามวัตถุประสงค์ จึงมีคำสั่งดังนี้

๑. ให้ยกเลิกคำสั่งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๒/๒๕๖๗ ลงวันที่ ๓๑ มกราคม พ.ศ. ๒๕๖๗ เรื่อง แต่งตั้งคณะทำงานภายใต้นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๒. แต่งตั้งคณะทำงานในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังต่อไปนี้

๒.๑ องค์ประกอบ

- | | | |
|-------|--|-----------|
| ๒.๑.๑ | นางสาวเสาวลักษณ์ วิจิตร | ประธาน |
| | ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร | |
| ๒.๑.๒ | นายพูนพัฒน์ ชันธาโรจน์ | รองประธาน |
| | ผู้อำนวยการกลุ่มการพัฒนาระบบเทคโนโลยีและการสื่อสาร | |
| ๒.๑.๓ | นางสาวทศวรรณ จันทร์อ่อน | คณะทำงาน |
| | ผู้อำนวยการกลุ่มการพัฒนาระบบสารสนเทศ | |

๒.๑.๔	นางสาวยุหนันท์ สมปาง ผู้อำนวยการกลุ่มการวิเคราะห์ข้อมูล	คณะทำงาน
๒.๑.๕	จำสืบเอกฤทธิเดช แสงแจ่ม นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๒.๑.๖	นายศรัณยู สวัสดิ์มงคล นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
๒.๑.๗	นายอัศราวุฒิ ตอโมกษ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒.๑.๘	นายพลสิทธิ มีไปล์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒.๑.๙	นายภูวดล เกตุดี นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
๒.๑.๑๐	นางสาวพิชญ์ชญาดา มีนาภา นักพัฒนาสังคมปฏิบัติการ	คณะทำงาน
๒.๑.๑๑	นางสาวกฤตพร ใจแน่น นักวิเคราะห์นโยบายและแผนปฏิบัติการ	คณะทำงาน
๒.๑.๑๒	นายปฏิพัทธ์ ก้อมมะณี เจ้าพนักงานพัฒนาสังคมปฏิบัติงาน	คณะทำงาน
๒.๑.๑๓	นางสาวสมอุษา วิไลพันธุ์ นักวิเคราะห์นโยบายและแผนชำนาญการ	คณะทำงาน และเลขานุการ
๒.๑.๑๔	นางสาวประทุมรัตน์ กลิ่นประทุม นักพัฒนาสังคม	คณะทำงาน และผู้ช่วยเลขานุการ

๒.๒ หน้าที่และอำนาจ

๒.๒.๑ จัดทำ/ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของ สป.พม. เพื่อเป็นกรอบในการดำเนินการสำหรับการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ การลดผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัย การคุ้มครองและควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศสำคัญ

๒.๒.๒ บริหารจัดการ เฝ้าระวัง และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมถึงการกู้คืน และฟื้นฟูระบบสารสนเทศเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัย

๒.๒.๓ ติดตาม ตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ของ สป.พม. รวมถึงรายงานผลการตรวจสอบและข้อเสนอแนะให้กับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ทราบ

๒.๒.๔ ปฏิบัติงานอื่นๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ตามคำสั่งของผู้บริหารหรือหน่วยงานที่รับผิดชอบ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๖ มีนาคม พ.ศ. ๒๕๖๘



(นางสาวเสาวลักษณ์ วิจิตร)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



บันทึกข้อความ

ปพม.
รับที่ 12365
วันที่ 10 ต.ค. ๖๕
เวลา

ส่วนราชการ กลุ่มตรวจสอบภายใน สำนักงานปลัดกระทรวงฯ โทร. ๐ ๒๒๐๒ ๙๐๖๑

ที่ พม ๐๒๒๓/๑๐๒๖

วันที่ ๑๐ ตุลาคม ๒๕๖๗

เรื่อง รายงานผลการสอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์

สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

เรียน ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๑. เรื่องเดิม

๑.๑ ตามหนังสือ ที่ พม ๐๒๑๐/ว ๖๒๐ ลงวันที่ ๕ มิถุนายน ๒๕๖๗ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ได้ส่งร่างแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป. พม. ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

๑.๒ ตามหนังสือ พม ๐๒๒๓/๗๖๕ กลุ่มตรวจสอบภายใน แจ้งการเข้าสอบทานแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแผนการตรวจสอบ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ เพื่อดำเนินการสอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร นั้น

๒. ข้อเท็จจริง

กลุ่มตรวจสอบภายใน ได้สอบทานแผนบริหารจัดการความเสี่ยงและประเมินความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ โดยใช้กระดานทำการสอบทานความเสี่ยงด้านเทคโนโลยีและภัยไซเบอร์ เป็นเครื่องมือในการสอบทาน และทำการวิเคราะห์ ประเมินความเสี่ยง ทบทวนข้อมูลผลการดำเนินงาน ความเพียงพอ ความเชื่อถือได้ของแผนบริหารจัดการความเสี่ยงฯ จากการสอบทาน ปีงบประมาณ พ.ศ. ๒๕๖๗ ซึ่งมีประเด็นในการสอบทาน จำนวน ๑๓ ประเด็น ๙๖ ข้อ และปัจจัยเสี่ยงทั้งสิ้น ๒๘ ปัจจัยเสี่ยง โดยมีข้อตรวจพบ ดังนี้

๑. ปัจจัยเสี่ยงด้านการควบคุมการเข้าถึงทางกายภาพ ไม่มีการติดป้ายแจ้งเตือน เพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้นในห้องแม่ข่าย ดังนี้

๑.๑ ห้ามบุคคลภายนอกเข้าไปในห้องแม่ข่ายโดยไม่มีกิจที่จำเป็น

๑.๒ ห้ามสูบบุหรี่ และนำอาหารเครื่องดื่มเข้าไปในบริเวณห้องแม่ข่าย

๑.๓ ห้ามนำสิ่งของที่ไมเกี่ยวข้องเข้ามาในห้องแม่ข่าย

๒. ปัจจัยเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล ลักษณะความเสี่ยงอยู่ในระดับที่พออนุมัติได้ แต่ต้องมีกิจกรรมควบคุมเพื่อมิให้ความเสี่ยงเคลื่อนย้ายไปอยู่ในระดับที่ยอมรับไม่ได้ ความเสี่ยงที่อาจจะเกิดขึ้นคือการถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่คอมพิวเตอร์แม่ข่าย (Server) มีการดำเนินการอย่างสม่ำเสมอ ไม่มีการกำหนดระยะเวลาในการดำเนินการที่ชัดเจน อาทิ

๒.๑ ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS Firewall)

อย่างสม่ำเสมอ

๒.๒ บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตาม เพื่อ Update

อย่างสม่ำเสมอ

๒.๓ ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ

๒.๔ ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ

๓. ปัจจัย ...

๓. ปัจจัยเสี่ยงด้านระบบข้อมูล ลักษณะความเสี่ยงอยู่ในระดับที่พอยอมรับได้แต่ต้องมีกิจกรรมควบคุมเพื่อมิให้ความเสี่ยงเคลื่อนย้ายไปอยู่ในระดับที่ยอมรับไม่ได้ ความเสี่ยงที่อาจเกิดขึ้น คือ การโจมตีโดยบุคคลที่ไม่มีสิทธิ์ระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database) การดักจับข้อมูล และการส่งข้อมูลคำสั่งเจตนาร้าย การควบคุมการกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ผู้ใช้งานสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่มียสิทธิ์เข้าถึงข้อมูล การกำหนดสิทธิ์ผู้ใช้งานและทบทวนสิทธิ์ ควรกำหนดระยะเวลาให้ชัดเจน เช่น อย่างน้อย ๓ เดือนครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งานในระบบ

๔. ดำเนินการตามแนวทางการควบคุมความเสี่ยงของแต่ละปัจจัยเสี่ยงและติดตามการบริหาร ความเสี่ยงอย่างต่อเนื่องเพื่อป้องกันมิให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้

๓. ข้อพิจารณา

เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ของสำนักงาน ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๗ ของศูนย์เทคโนโลยีและการสื่อสาร มีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุน การดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการตามรายงานผลการสอบทานฯ ที่แนบมาพร้อมนี้

๔. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดลงนามในแบบรายงานสรุปสำหรับผู้บริหาร ในรายงานผลการสอบทานที่แนบมาพร้อมนี้ด้วยแล้ว



(นางสาวมินรดา คำสม)

ผู้ตรวจสอบภายในกระทรวง

เห็นชอบ-ลงนามแล้ว



(นายอนุกุล ปิตแก้ว)

ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๓๐ ต.ค. ๒๕๖๗

รายงานสรุปสำหรับผู้บริหาร
การสอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
ปีงบประมาณ พ.ศ. ๒๕๖๗

๑.ความเป็นมา

ตามแผนการตรวจสอบภายใน ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ กำหนดให้กลุ่มตรวจสอบภายใน สอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๒. วัตถุประสงค์ของการตรวจสอบ

๑. เพื่อสอบทานความเชื่อถือได้ และถูกต้องของข้อมูลของการจัดทำแผนบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ว่าเป็นไปตามมาตรฐาน

๒. เพื่อประเมินความมีประสิทธิภาพ ประสิทธิผลของแผนการบริหารจัดการความเสี่ยง ด้านสารสนเทศและการสื่อสาร

๓. เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบฐานข้อมูล ระบบเทคโนโลยี สารสนเทศและระบบเครือข่ายคอมพิวเตอร์

๔. เพื่อประเมินความเพียงพอของระบบการควบคุมภายใน และการบริหารจัดการความเสี่ยง ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๕. เพื่อให้ความมั่นใจว่าการบริหารจัดการความเสี่ยง สามารถดำเนินการได้ตามแผนการบริหาร จัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้อยู่ในระดับที่ยอมรับได้

๓. ขอบเขตการสอบทานแผนบริหารความเสี่ยง

สอบทานแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สำนักงาน ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ประจำปี ๒๕๖๗ ของศูนย์เทคโนโลยีสารสนเทศ และสื่อสาร

๔. ระยะเวลาของการสอบทาน

ระหว่างวันที่ ๒๘ สิงหาคม-๒๗ กันยายน ๒๕๖๗

๕. วิธีการประเมินผลการบริหารความเสี่ยง

๑. ศึกษากฎหมายและระเบียบที่เกี่ยวข้องกับแผนการบริหารจัดการความเสี่ยง

๒. สอบทานความเพียงพอ ความเชื่อถือได้ของการจัดทำแผนบริหารจัดการความเสี่ยงของ กิจกรรมที่ประเมินในปัจจุบัน โดยจัดทำกระดาษทำการสอบทานความเสี่ยงด้านเทคโนโลยีและภัยไซเบอร์ สป.พม. ประกอบด้วยประเด็นในสอบทาน จำนวน ๑๓ ประเด็น ๙๖ ข้อ โดยมีประเด็นในการตรวจสอบ ดังนี้

ประเด็นการตรวจสอบที่ ๑ การจัดทำนโยบายความมั่นคงปลอดภัยเป็นไปตามกฎหมายและ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จำนวน ๕ ข้อ

ประเด็นการตรวจสอบที่ ๒ การควบคุมการเข้าถึงของผู้ใช้งานระบบสารสนเทศและเครือข่าย รวมทั้งระบบปฏิบัติการ เป็นไปตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จำนวน ๑๔ ข้อ

ประเด็นการตรวจสอบที่ ๓ การควบคุมการเข้าถึงทางกายภาพ ตรวจสอบในห้องแม่ข่าย จำนวน ๒๕ ข้อ

ประเด็น ...

ประเด็นการตรวจสอบที่ ๔ หน่วยงานมีการดำเนินงานควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ จำนวน ๒ ข้อ

ประเด็นการตรวจสอบที่ ๕ หน่วยงานต้องมีการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินตามที่กฎหมายหรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จำนวน ๑๑ ข้อ

ประเด็นการตรวจสอบที่ ๖ มีการประเมินขีดสมรรถนะของระบบสารสนเทศให้มีความพร้อมใช้งานจำนวน ๕ ข้อ

ประเด็นการตรวจสอบที่ ๗ การดำเนินงานควบคุมและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม จำนวน ๓ ข้อ

ประเด็นการตรวจสอบที่ ๘ การพัฒนาระบบสารสนเทศมีคุณภาพและเหมาะสมต่อการใช้งานรวมทั้งพัฒนาต่อยอดได้ในอนาคต จำนวน ๑๖ ข้อ

ประเด็นการตรวจสอบที่ ๙ เผยแพร่ตาม พรบ. ข้อมูลข่าวสาร พ.ศ. ๒๕๔๐ กำหนด จำนวน ๒ ข้อ

ประเด็นการตรวจสอบที่ ๑๐ การตรวจสอบการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ จำนวน ๔ ข้อ

ประเด็นการตรวจสอบที่ ๑๑ การเข้ารหัสมาตรฐานความปลอดภัย จำนวน ๑ ข้อ

ประเด็นการตรวจสอบที่ ๑๒ การรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน ๖ ข้อ

ประเด็นการตรวจสอบที่ ๑๓ การดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จำนวน ๒ ข้อ

โดยการสอบถามเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศที่เคยเกิดขึ้นในอดีตผลกระทบที่เคยได้รับ ความถี่ในการเกิดเหตุการณ์ ความสูญเสีย และข้อกังวลเกี่ยวกับความเสี่ยงของระบบและองค์ประกอบของระบบที่อาจเกิดขึ้นในอนาคต เพื่อใช้สัมภาษณ์ผู้ที่เกี่ยวข้อง ได้แก่

๑) ผู้ดูแลระบบ (System custodian)

๒) ผู้ใช้งาน (User)

๓. วิเคราะห์บทวนข้อมูล ผลการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงว่าสามารถทำให้ความเสี่ยงที่ยังคงเหลืออยู่นั้นลดลงหรืออยู่ในระดับที่ยอมรับได้

๔. รายงานผลการสอบทาน ความเพียงพอ ความเชื่อถือได้ของการจัดทำแผนบริหารจัดการความเสี่ยง

ผลการสอบทานแผนการจัดการความเสี่ยง

๑. การสอบทานความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๓ จำนวน ๑๓ ประเด็นการตรวจสอบ ๙๖ ข้อ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ประเมินความเสี่ยงตามที่กลุ่มตรวจสอบภายในได้จัดทำเป็นเครื่องมือในการสอบทาน โดยศูนย์เทคโนโลยีฯ ได้แนบหลักฐานประกอบการสอบทาน ใช้เป็นหลักฐานในการตรวจสอบ ครบถ้วนตามประเด็นการตรวจสอบ ยกเว้น ประเด็นที่ ๓ การควบคุมการเข้าถึงทางกายภาพตรวจสอบในห้องแม่ข่าย

ข้อ ๒๘ ห้ามบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น ไม่มีป้ายห้ามบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น

ข้อ ๒๙ ห้ามสูบบุหรี่ และนำอาหารเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง ไม่มีป้ายห้ามสูบบุหรี่และนำอาหาร เครื่องดื่มเข้าไปในบริเวณห้องเครื่อง

ข้อ ๓๐ ห้ามนำสิ่งของที่ไม่เกี่ยวข้องเข้ามาในห้องแม่ข่าย มีการนำสิ่งของที่ไม่เกี่ยวข้องเข้ามาในห้องแม่ข่าย

๒. แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สำนักงานปลัดกระทรวง
การพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๗ ตามเกณฑ์การประเมิน ดังนี้

คะแนน	ระดับ ความเสี่ยง	คำอธิบาย
๑๕ - ๒๕	สูง	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
๘ - ๑๔	ค่อนข้างสูง	ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
๔ - ๗	ค่อนข้างต่ำ	ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับ ที่ยอมรับไม่ได้
๑ - ๓	ต่ำ	ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องการจัดการเพิ่มเติม

จากการประเมินแผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สป.พม.
พ.ศ. ๒๕๖๗ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีปัจจัยความเสี่ยงทั้งสิ้น ๒๘ ปัจจัยเสี่ยง ตามระดับ
ความเสี่ยง พบว่า

๑. ด้านกายภาพและสิ่งแวดล้อม มี ๔ ปัจจัยความเสี่ยง มีแนวทางการควบคุมความเสี่ยง
ที่อาจจะเกิดขึ้น ให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑-๓ ระดับความเสี่ยงต่ำ
ซึ่งอยู่ในระดับยอมรับได้ คือ

๑.๑ ไฟไหม้ห้องศูนย์ข้อมูลกลางสารสนเทศ (Data Center)

๑.๒ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๑.๓ การควบคุมอุณหภูมิ/ความชื้นภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่าย
คอมพิวเตอร์ สป.พม. ผิดปกติ

๑.๔ มีการเข้าถึงศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป. พม. โดยไม่ได้
รับอนุญาต ไม่ทราบด้านกายภาพและสิ่งแวดล้อม อาจปิดประตูไม่สนิท ทำให้อุณหภูมิ/ความชื้นภายใน
ห้องปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ผิดปกติ อุปกรณ์อิเล็กทรอนิกส์เกิดความเสียหาย

๒. ด้านบุคลากร มี ๕ ปัจจัยความเสี่ยง มีแนวทางการควบคุมความเสี่ยงที่อาจจะเกิดขึ้นทำให้
ความเสี่ยงลดลง ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑ - ๓ ระดับความเสี่ยงต่ำ อยู่ในระดับที่ยอมรับได้ คือ

๒.๑ ผู้ดูแลระบบปฏิบัติตามแนวทางที่กำหนดไม่ครบถ้วนในการบริหารจัดการสิทธิ์
การเข้าถึงและใช้งานระบบสารสนเทศ

๒.๒ บุคลากรด้านไอทีมีความรู้ความเข้าใจด้านเทคโนโลยีไม่เพียงพอ

๒.๓ ผู้ใช้งาน/user ไม่มีความรู้ ความชำนาญและทักษะการใช้งานระบบหรือเปลี่ยนผู้ปฏิบัติงานบ่อย

๒.๔ การจ้างบุคคลภายนอกที่ขาดความตระหนักในการดูแลข้อมูลสำคัญของหน่วยงาน

๒.๕ การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญ ดูแลบำรุงรักษาระบบ/
พัฒนาระบบ

๓. ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร มี ๗ ปัจจัยความเสี่ยง มีแนวทางการควบคุม
ความเสี่ยงที่อาจจะเกิดขึ้นทำให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยง ๒ ระดับ ดังนี้

๓.๑ ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑ - ๓ ระดับความเสี่ยงต่ำ อยู่ในระดับ
ที่ยอมรับได้ จำนวน ๔ ปัจจัยเสี่ยง คือ

๑) มีการ ...

- ๑) มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่าย
- ๒) แผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สป.พม.
- ๓) ระบบเครือข่ายสื่อสารหลักสำคัญศูนย์ปฏิบัติการระดับแม่ข่ายและเครือข่าย สป.พม. ไม่สามารถเชื่อมต่อกับผู้ใช้บริการได้

๔) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓.๒ ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ระดับความเสี่ยงค่อนข้างต่ำ จำนวน ๓ ปัจจัยเสี่ยง คือ

๑) การบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารและระบบปฏิบัติการ (Operating System) ในทุก ๆ ระดับผู้ใช้งานขาดประสิทธิภาพ

๒) ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่คอมพิวเตอร์แม่ข่าย (Server)

๓) การป้องกันหรือตรวจจับไวรัส

๔. ด้านโปรแกรมคอมพิวเตอร์ มี ๑ ปัจจัยความเสี่ยง มีแนวทางควบคุมความเสี่ยงที่อาจจะเกิดขึ้นทำให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑-๓ ระดับความเสี่ยงต่ำ อยู่ในระดับที่ยอมรับได้ คือ ละเมิดลิขสิทธิ์โปรแกรมมัลแวร์ (Utilities Program) (Utility Program คือ โปรแกรมที่ติดมาพร้อมระบบปฏิบัติการวินโดวส์ ว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดวส์ เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ สำรองข้อมูล ยกเลิกการติดตั้ง เป็นต้น)

๕. ด้านระบบข้อมูล มี ๔ ปัจจัยความเสี่ยง มีแนวทางควบคุมความเสี่ยงที่อาจจะเกิดขึ้น ทำให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยง ๒ ระดับ

๕.๑ ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑ - ๓ ระดับความเสี่ยงต่ำ อยู่ในระดับที่ยอมรับได้ จำนวน ๓ ปัจจัยเสี่ยง

๑) การจัดทำบัญชีรายละเอียดของระบบสารสนเทศและผู้เกี่ยวข้อง

๒) การกำหนดมาตรฐานในการพัฒนาซอฟต์แวร์ไม่มีความชัดเจน

๓) การนำมาตรฐานข้อมูลไปใช้ในการพัฒนาและออกแบบระบบข้อมูลและฐานข้อมูลเพื่อการแลกเปลี่ยนเชื่อมโยงข้อมูล

๕.๒ ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ระดับความเสี่ยงค่อนข้างต่ำ จำนวน ๖ ปัจจัยเสี่ยง

๑) การบริหารจัดการสิทธิ์ผู้ใช้งานและการเข้าถึงเพื่อใช้งานระบบสารสนเทศที่มีความมั่นคงปลอดภัย เช่น การทบทวนสิทธิ์ผู้ใช้งาน การบริหารจัดการผ่าน การยุติการให้บริการตามเวลาที่กำหนด (Session Time Out) การทบทวนเวลาเมื่อมีการล็อกอินผิด เพื่อป้องกันการโจมตี

๒) การโจมตีโดยบุคคลที่ไม่มีสิทธิ์ระบบหรือลักลอบเข้าสู่ระบบฐานข้อมูลการดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย

๓) การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง

๔) เกิดช่องโหว่จากการพัฒนาโปรแกรมประยุกต์

๕) การนำข้อมูลผิดพลาดทั้งจากผู้นำเข้าข้อมูล (Human Error) และความผิดพลาดของระบบ (Bug)

๖) การนำเข้าข้อมูลไม่ครบถ้วนและไม่เป็นปัจจุบัน

๖. ด้านกลยุทธ์ มี ๑ ปัจจัยความเสี่ยง มีแนวทางควบคุมความเสี่ยงที่อาจจะเกิดขึ้น ทำให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑-๓ ระดับความเสี่ยงต่ำ ซึ่งอยู่ในระดับที่ยอมรับได้ คือ ทิศทาง/แนวทางการพัฒนาด้านเทคโนโลยีสารสนเทศไม่ชัดเจน/ไม่สอดคล้องกับภารกิจ ขาดการบูรณาการร่วมกัน

๗. ด้านการเงิน (งบประมาณ) มี ๑ ปัจจัยความเสี่ยง มีแนวทางควบคุมความเสี่ยงที่อาจเกิดขึ้นทำให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑-๓ ระดับความเสี่ยงต่ำ ซึ่งอยู่ในระดับที่ยอมรับได้ คือ การปรับลดวงเงินงบประมาณที่ขอจัดสรรสำหรับการดำเนินโครงการต่าง ๆ ไม่มีการวิเคราะห์ความจำเป็นและความต้องการแบบถ่วงน้ำหนักแต่จะเป็นการปรับลด ตามเปอร์เซ็นต์ที่หน่วยงานกำหนด

๘. ด้านบริหารจัดการ ๑ ปัจจัยความเสี่ยง มีแนวทางควบคุมความเสี่ยงที่อาจเกิดขึ้นทำให้ความเสี่ยงลดลง ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑-๓ ระดับความเสี่ยงต่ำ ซึ่งอยู่ในระดับที่ยอมรับได้ คือ กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน เช่น การอนุมัติโครงการล่าช้า ไม่มีผู้เข้าประกวดราคา ไม่สามารถประกาศผล ผู้ชนะการประกวดราคา การจัดทำสัญญาไม่ตรงตามร่างข้อกำหนดการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ได้มีการกำหนดแนวทางมาตรการ ควบคุม ป้องกัน แก้ไข ซึ่งมีผลทำให้ลดโอกาสเกิดความเสี่ยงและค่าคะแนนความเสี่ยง ดังนี้

๑. ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๑ - ๓ ระดับความเสี่ยงต่ำ ซึ่งอยู่ในระดับที่ยอมรับได้ จำนวน ๑๔ ปัจจัยเสี่ยง

๒. ค่าคะแนนความเสี่ยงอยู่ในช่วงคะแนนเท่ากับ ๔ - ๗ ระดับความเสี่ยงค่อนข้างต่ำ จำนวน ๔ ปัจจัยเสี่ยง หากวิเคราะห์ปัจจัยที่มีค่าคะแนนที่สุด มีค่าคะแนนที่ ๖ คะแนน มี ๒ ปัจจัยความเสี่ยง ดังนี้

๒.๑ ปัจจัยเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร ลักษณะความเสี่ยงที่อาจเกิดขึ้น คือการถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่คอมพิวเตอร์แม่ข่าย (Server)

๒.๒ ปัจจัยเสี่ยงด้านระบบข้อมูล ลักษณะความเสี่ยงที่อาจเกิดขึ้น คือการโจมตีโดยบุคคลที่ไม่มีสิทธิ์ระบบหรือลักลอบเข้าสู่ระบบฐานข้อมูลการดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย

ข้อเสนอแนะ

เพื่อให้แผนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ พ.ศ. ๒๕๖๗ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้นและไม่ก่อให้เกิดผลกระทบต่อการดำเนินการตามแผนฯ ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยไซเบอร์ พร้อมวางแผนแนวทางในการป้องกันภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้น สามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด จึงเห็นควรให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.ม.ดำเนินการ ดังนี้

๑. ปัจจัยเสี่ยงด้านการควบคุมการเข้าถึงทางกายภาพ เพื่อป้องกันความมั่นคงปลอดภัย ความเสี่ยงที่อาจเกิดขึ้น ให้จัดทำป้ายเพื่อแสดงสัญลักษณ์ ดังนี้

๑.๑ ห้ามบุคคลภายนอกเข้าไปในห้องแม่ข่ายโดยไม่มีกิจที่จำเป็น

๑.๒ ห้ามสูบบุหรี่ และนำอาหารเครื่องดื่มเข้าไปในบริเวณห้องแม่ข่าย

๑.๓ ห้ามนำสิ่งของที่ไม่เกี่ยวข้องเข้ามาในห้องแม่ข่าย

๒. ปัจจัยเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล ลักษณะความเสี่ยงอยู่ในระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อมิให้ความเสี่ยงเคลื่อนย้ายไปอยู่ในระดับที่ยอมรับไม่ได้ ความเสี่ยงที่อาจเกิดขึ้น คือการถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะหรือลักลอบ (Hack) เข้าสู่คอมพิวเตอร์แม่ข่าย (Server) อาทิ

๒.๑ ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ

๒.๒ บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตาม เพื่อ Update อย่างสม่ำเสมอ

๒.๓ ติดตั้งโปรแกรมป้องกันไวรัส และ patch อย่างสม่ำเสมอ

๒.๔ ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ

ควรมีการบริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและการติดตามเพื่อ Update โดยกำหนดระยะเวลาให้ชัดเจน หรือมีการแจ้งเตือนจากหน่วยงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อความปลอดภัยและสามารถแก้ไขสถานการณ์ได้อย่างทันที่

๓. ปัจจัยเสี่ยงด้านระบบข้อมูล ลักษณะความเสี่ยงอยู่ในระดับที่ยอมรับได้แต่ต้องมีกิจกรรมควบคุม เพื่อมิให้ความเสี่ยงเคลื่อนย้ายไปอยู่ในระดับที่ยอมรับไม่ได้ ความเสียหายที่อาจเกิดขึ้น คือการโจมตี โดยบุคคลที่ไม่มีสิทธิ์ระบบหรือลักลอบเข้าสู่ระบบฐานข้อมูลการดักจับข้อมูลและการส่งข้อมูลคำสั่งเจตนาร้าย การกำหนดสิทธิผู้ใช้งานและทบทวนสิทธิ ควรกำหนดระยะเวลาให้ชัดเจน เช่น อย่างน้อย ๓ เดือน/ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงผู้ใช้งานในระบบ เพื่อป้องกันผู้ที่ไม่มีสิทธิเข้าถึงข้อมูล

๔. ดำเนินการตามแนวทางการควบคุมความเสี่ยงของแต่ละปัจจัยเสี่ยงและติดตามการบริหารความเสี่ยงอย่างต่อเนื่องเพื่อป้องกันมิให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้

คำสั่งผู้บริหาร

ผู้สอบทานและรายงาน



ชื่อ

(นายอนุกุล ปัดแก้ว)

ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์



ลงชื่อ.....

(นางสาวมินรดา คำสม)

ผู้ตรวจสอบภายในกระทรวง



MANAGEMENT