แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ประจำปีงบประมาณ 2567
กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

วันที่จัดทำเอกสาร : 27 ตุลาคม 2566

รับรองโดย: .....

(นายนิพนธ์ กิจเกตุก้อง)

ตำแหน่ง: ผู้เชี่ยวชาญด้านบริหารความเสี่ยง

วันที่รับรอง: 31 ตุลาคม 2566

สารบัญ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญรูป

หน้า

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ประจำปีงบประมาณ 2567

กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน (พพ.) ได้นำเทคโนโลยีสารสนเทศเข้ามาใช้ในการปฏิบัติงานหลายด้าน ดังนั้น พพ. จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อหาวิธีการป้องกันปัญหาที่จะเกิดขึ้น อันส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของ พพ. อีกทั้งเป็นการนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุดและลดโอกาสความเสียหายที่จะเกิดขึ้น

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารมีวัตถุประสงค์เพื่อใช้เป็นแนวทางในการตรวจสอบ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ พพ. ด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงเกิดขึ้นจริงและ พพ. สามารถนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในการดำเนินการได้

1. สรุปผลการดำเนินการแผนบริการความเสี่ยง ปี 2566

แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ 2566 มีความเสี่ยง 9 ประเภท ซึ่งมีแนวทางการควบคุมความเสี่ยง 26 มาตรการ โดยมีการดำเนินงานดังต่อไปนี้

ศทส. ได้ปฏิบัติตามแนวทางการควบคุมความเสี่ยงทั้งสิ้น 24 มาตรการ และมีจำนวน 2 มาตรการ ที่ยังไม่สามารถดำเนินการได้ภายในปีงบประมาณ 2566 ได้แก่

1) ไม่สามารถดำเนินการติดสติ๊กเกอร์การละเมิดลิขสิทธิ์ เนื่องจากบริษัทที่จัดหาคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ยังไม่ส่งมอบครุภัณฑ์ เจ้าหน้าที่ของ ศทส. จึงไม่สามารถดำเนินการในขั้นตอนดังกล่าวได้
2) ไม่สามารถดำเนินการติดตั้งอุปกรณ์การแจ้งเตือน กรณีไฟดับ เนื่องจากนำงบประมาณไปใช้สำหรับงานหรือโครงการที่เร่งด่วนก่อน และจะทำการวางแผนเพื่อจัดหาอุปกรณ์ดังกล่าวในแผนของปีถัดไป

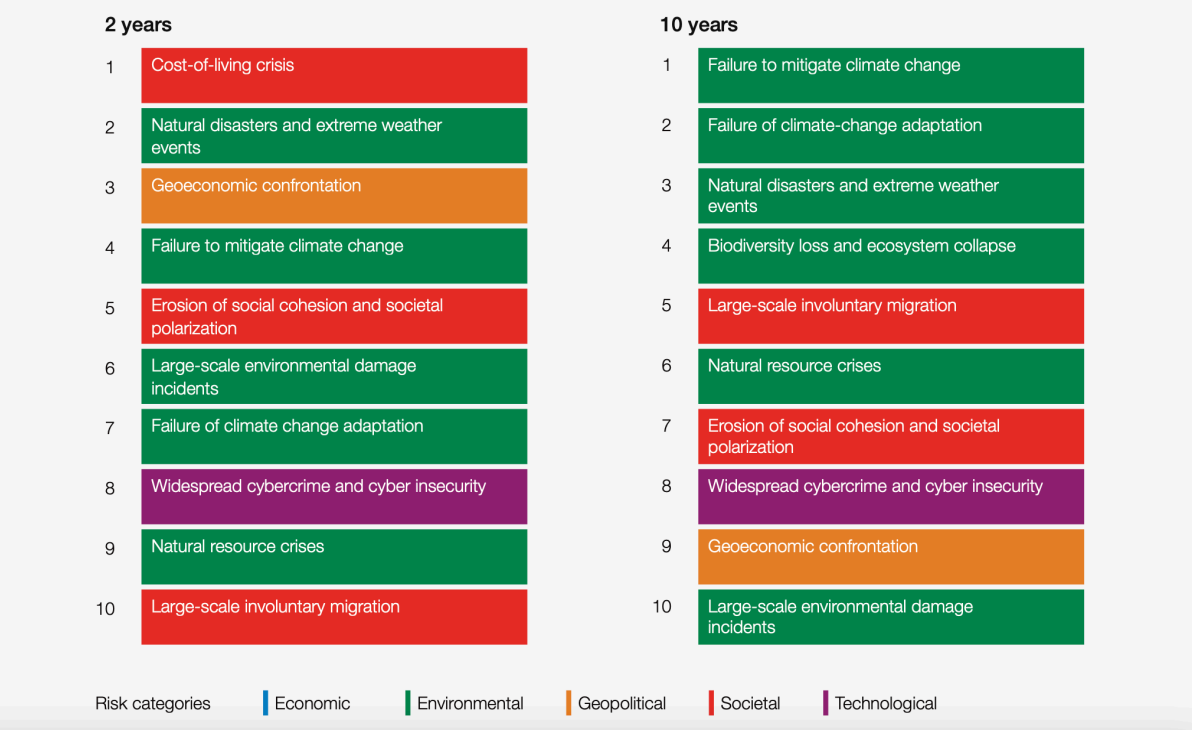
จากผลการดำเนินการในปีงบประมาณ 2566 พบว่า ศทส. ได้ดำเนินการตามแผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารคิดเป็น 92.3 เปอร์เซ็นต์ของแนวทางการควบคุมความเสี่ยงทั้งหมด แม้ว่าความเสี่ยงหรือภัยคุกคามที่เกิดขึ้นภายใน พพ. ในปีงบประมาณที่ผ่านมายังไม่ส่งผลกระทบต่อการทำงานของบุคลากรภายในองค์กร แต่คณะทำงานฯ ควรติดตามและผลักดันให้สามารถดำเนินการได้ครบถ้วนตามแผนปฏิบัติการที่กำหนด เพื่อลดช่วยความเสี่ยงที่อาจก่อให้เกิดความเสียหายในอนาคต

2. การทบทวนบริบทความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ 2567 ของ พพ. คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารได้ศึกษาบริบทที่เกี่ยวข้องกับความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับสากล เพื่อพิจารณาถึงทิศทางและแนวโน้มด้านความเสี่ยง และการป้องกัน เนื่องจากการประเมินความเสี่ยง ประจำปีงบประมาณ 2567 เป็นการประมาณการล่วงหน้า ซึ่งจำเป็นต้องพิจารณาทั้งภายในและภายนอกองค์กร เพื่อวางแผนป้องกันความเสี่ยงให้รอบด้าน

2.1 The Global Risks Report 2023 18th Edition

สภาเศรษฐกิจโลก (World Economic Forum : WEF) ได้ประเมินโอกาสของการเผชิญกับภัยคุกคามที่สำคัญและผลกระทบที่เกิดขึ้นจากภัยคุกคามในระดับสากลที่จัดในอยู่ในความเสี่ยงที่ควรเฝ้าระวัง มีรายละเอียดดังนี้



รูปที่ 1 The Global Risks Horizon 2023[1]

[1] แหล่งที่มา: The Global Risks **Report 2023**

จากรูปที่ 1 พิจารณาความเสี่ยงพบว่า ในปี พ.ศ. 2565 - พ.ศ. 2567 มีความเสี่ยงที่สามารถกลายเป็นภัยคุกคามร้ายแรงคือ Widespread cybercrime and cyber insecurity

Widespread cybercrime คือ การขยายเป็นวงกว้างของอาชญากรรมทางไซเบอร์ ซึ่งสามารถเกิดจากการโจมตีทางไซเบอร์หลายชนิดด้วยกัน เช่น DDoS Attack, Man-in-the-middle attack, Malware เป็นต้น โดยสิ่งเหล่านี้สามารถสร้างความเสียหายแก่ความปลอดภัยของข้อมูลภายในองค์กรได้

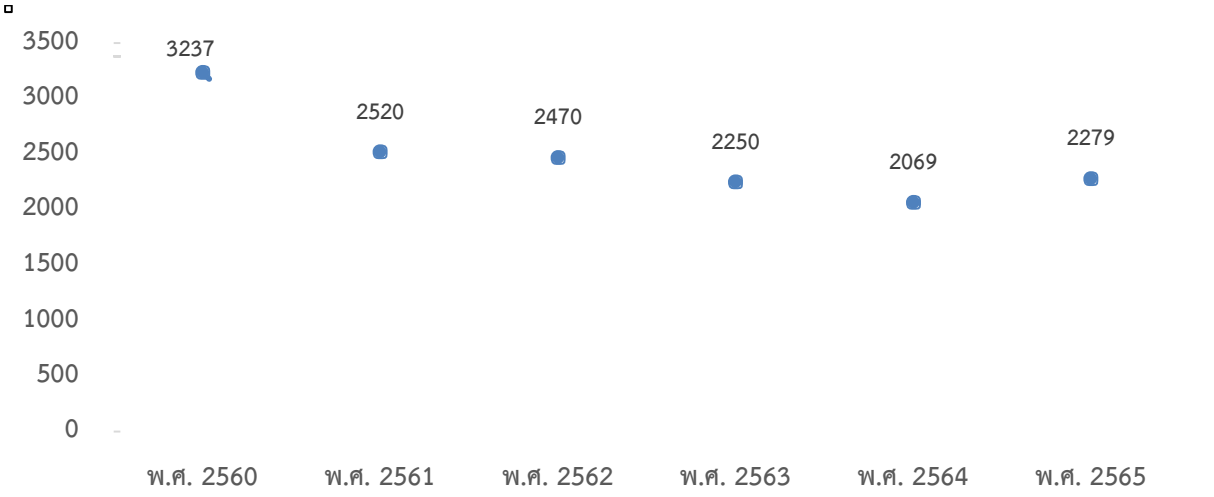
และ Cyber insecurity คือ ความไม่มั่นคงปลอดภัยทางไซเบอร์ หรือการขาดความมั่นคงปลอดภัยไซเบอร์ โดยที่ระบบสารสนเทศไม่มีความมั่นคงปลอดภัย จึงส่งผลให้ระบบนั้นไม่สามารถตั้งรับหรือทนต่อการโจมตีจากผู้ไม่ประสงค์ดี และเกิดความล้มเหลวในการทำงานของระบบสารสนเทศในภายหลังได้ง่าย

ดังนั้น พพ. ควรต้องทบทวนประเด็นความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ โดยทบทวนแผนความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อรับมือสถานการณ์ฉุกเฉินที่เกิดขึ้น เพื่อป้องกันหรือลดความเสี่ยงที่ส่งผลกระทบเป็นวงกว้าง และก่อให้เกิดความเสียหายอย่างร้ายแรงต่อ พพ. หากระบบรักษาความปลอดภัย และ/หรือ IT Infrastructure ของกรมฯ มีช่องโหว่หรือไม่สามารถใช้งานได้ ซึ่งส่งผลกระทบต่อปฏิบัติงานของบุคลากรภายใน พพ. และความน่าเชื่อถือขององค์กร

2.2 ภัยคุกคามไซเบอร์ของประเทศไทย

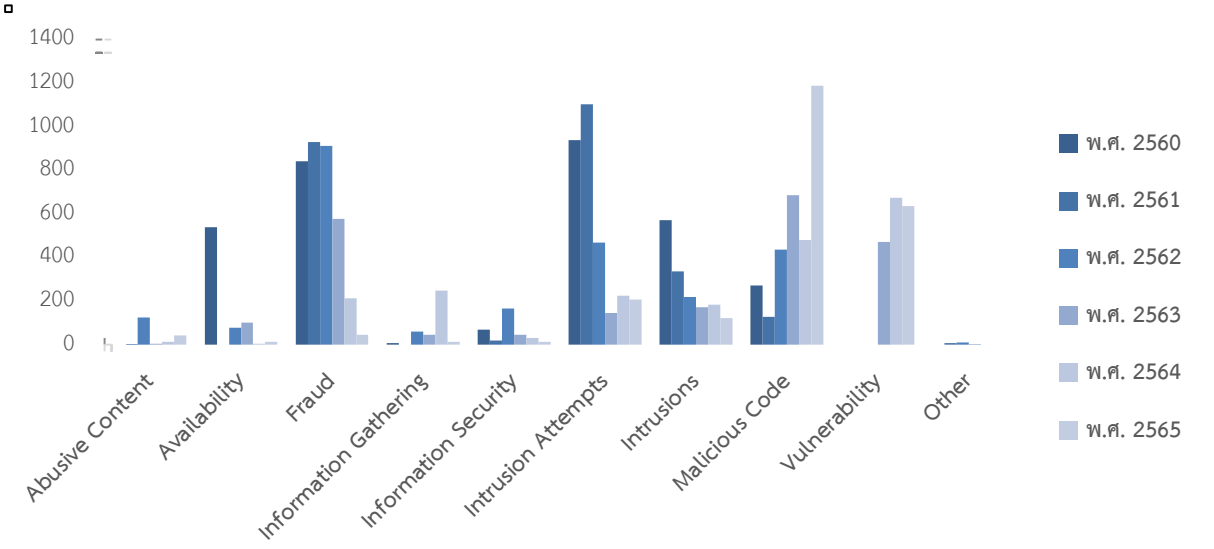
ภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 คือ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ดังนั้น การป้องกันภัยคุกคามทางไซเบอร์ จึงต้องมีมาตรการดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามต่าง ๆ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team : ThaiCERT) หรือไทยเซิร์ต ซึ่งมีภารกิจหลักในการจัดการ ให้คำแนะนำ และเผยแพร่เกี่ยวกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ได้เก็บข้อมูลภัยคุกตามตั้งแต่ พ.ศ. 2560 – 2565 พบว่า ปี 2560 – 2564 มีแนวโน้มภัยคุกคามลดลง แต่ในปี 2565 กลับมีจำนวนภัยคุกคามเพิ่มขึ้น (แสดงดังรูปที่ 2) และจากข้อมูลสถิติตามรูปที่ 3 ปรากฏว่า ประเภทของภัยคุกคามยังไม่เปลี่ยนไปมากหากเทียบกับภัยคุกคามในปีที่ผ่านมา ประกอบกับข้อมูลสถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์ ตั้งแต่วันที่ 1 ต.ค. 2565 – 4 ส.ค. 2566 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จะเห็นได้ว่า หน่วยงานของรัฐด้านอื่น ๆ (หน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ) ถูกโจมตีมากเป็นอันดับ 2 แสดงดังรูปที่ 4



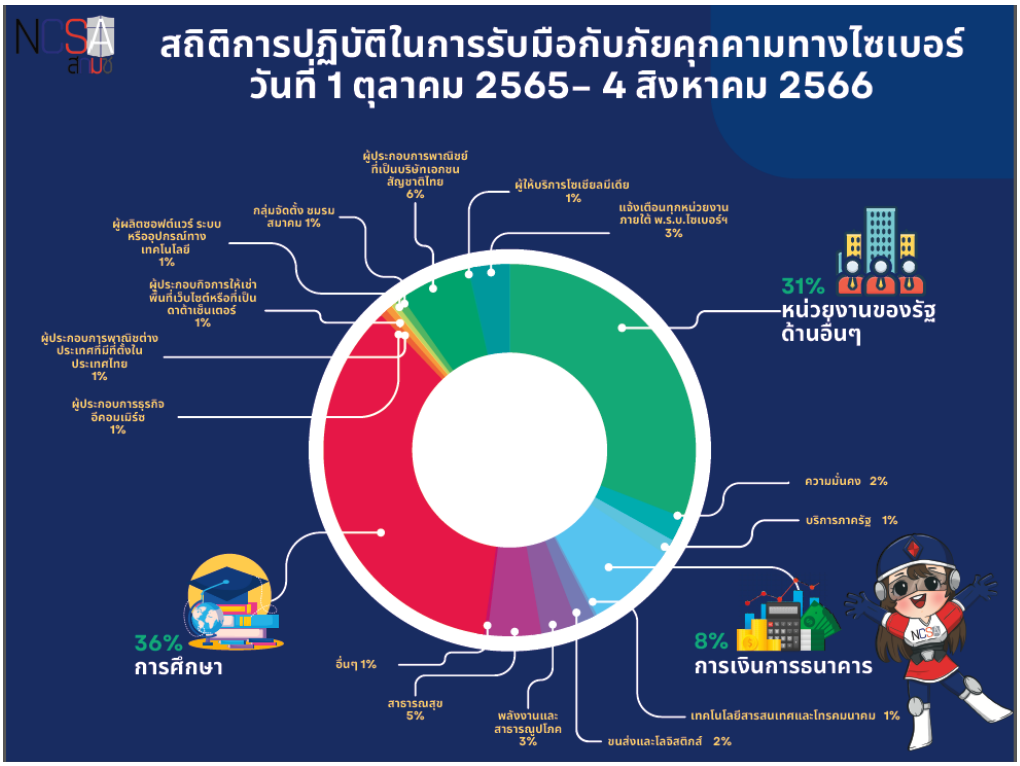
รูปที่ 2 แสดงจำนวนภัยคุกคาม พ.ศ. 2560 – 2565

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย 2565



รูปที่ 3 แสดงจำนวนภัยคุกคามแยกตามประเภท พ.ศ. 2560 – 2565

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย 2565



รูปที่ 4 สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์ ตั้งแต่วันที่ 1 ต.ค. 2565 – 4 ส.ค. 2566
ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

จากที่กล่าวมาแล้วข้างต้น พพ. ควรให้ความสำคัญด้านความมั่นคงปลอดภัยไซเบอร์เป็นหลัก เนื่องจากหากเกิดความเสียหายจะส่งผลกระทบเป็นวงกว้าง อาจทำให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูล หรือระบบต่าง ๆ ภายในหน่วยงาน ซึ่งส่งผลกระทบต่อปฏิบัติงานของบุคลากร และความน่าเชื่อถือขององค์กร

3. ความหมายของการบริหารความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่จะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้ สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลางและต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาส ที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง แบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือการยอมรับ การลด การควบคุม การยกเลิกและการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยงและทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมเพื่อการชี้แนะและการควบคุมเพื่อการแก้ไข

ทรัพย์สิน (Asset) หมายถึง ทรัพย์สินต่าง ๆ ขององค์กรแบ่งเป็น 5 หมวด ได้แก่ หมวดข้อมูล หมวดบุคลากร หมวดฮาร์ดแวร์ หมวดซอฟต์แวร์ และหมวดบริการ งบประมาณที่ใช้ในการลงทุนของโครงการ งบประมาณที่ใช้ในการดำเนินงาน เงินที่ใช้เป็นค่าจ้างต่าง ๆ ในการดำเนินกิจกรรม ตามภารกิจขององค์กร

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organizations of the Treadway Commission) มีดังนี้

1) การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2) การระบุความเสี่ยงต่าง ๆ (Event Identification)
3) การประเมินความเสี่ยง (Risk Assessment)
4) กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5) กิจกรรมการบริหารความเสี่ยง (Control Activities)
6) ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7) การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

ทั้งนี้ ในการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พพ. ได้มีผู้เชี่ยวชาญด้านการตรวจประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารจากภายนอกเป็นผู้ตรวจและรับรองผลการประเมิน โดยมีการทดสอบช่องโหว่การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารด้วยเครื่องมือการทดสอบที่เหมาะสมร่วมด้วย

4. วัตถุประสงค์

1) เพื่อให้การจัดการภายใต้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พพ. มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ พพ. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

3) เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

4) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

5. ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พพ.

6. คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ตารางที่ 1 แสดงรายชื่อคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับ	ตำแหน่ง/ชื่อ-สกุล	ตำแหน่ง	ความรับผิดชอบ
1.	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ผทส.	ประธานคณะทำงาน
2.	หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ	หทส.	คณะทำงาน
3.	หัวหน้ากลุ่มพัฒนาระบบสารสนเทศ	หพส.	คณะทำงาน
4.	หัวหน้ากลุ่มสถิติและข้อมูลพลังงาน	หสข.	คณะทำงาน
5.	หัวหน้ากลุ่มบริการสารสนเทศและภูมิสารสนเทศ	หบภ.	คณะทำงาน
6.	หัวหน้ากลุ่มองค์ความรู้พลังงานทดแทนและอนุรักษ์พลังงาน	หอร.	คณะทำงาน
7.	หัวหน้าฝ่ายบริหารงานทั่วไป	หบท.	คณะทำงาน
8.	นางสาวอรอนงค์ ผ่องแผ้ว	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ	คณะทำงาน
9.	นางสาวนัยนา บุญนาค	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	คณะทำงาน
10.	นางเพชรสุดา สิทธิพล	นักวิเคราะห์นโยบายและแผนชำนาญการ	คณะทำงาน
11.	นายชยุตม์รัฐ สายประดิษฐ์	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงาน
12.	นายกฤศ คชสุวรรณ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงาน
13.	นายจักรกฤต นิยมทัศน์	นักวิเคราะห์นโยบายและแผน	คณะทำงาน
14.	นายอนวัช ศรีสังข์	นักวิชาการคอมพิวเตอร์ชำนาญการ	คณะทำงานและเลขานุการ
15.	นางสาวณัฏฐณิชา ยงภูมิพุทธา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	คณะทำงานและผู้ช่วยเลขานุการ
16.	นายวันชัย กาสา	เจ้าพนักงานคอมพิวเตอร์	คณะทำงานและผู้ช่วยเลขานุการ

7. การประเมินความเสี่ยง (Risk Assessment)

การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของ พพ. สามารถแยกประเภทความเสี่ยงเป็น 5 ประเภท ดังนี้

1) ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่เกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น
2) ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่เกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยที่ผู้ใช้เข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือใช้ข้อมูลต่าง ๆ ของ พพ. เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
3) ความเสี่ยงจากการเกิดอัคคีภัย เป็นความเสี่ยงที่เกิดจากอัคคีภัยก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ
4) ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่ส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ
5) ความเสี่ยงจากปัจจัยภายนอก เป็นความเสี่ยงที่เกิดจากการให้บริการของหน่วยงานภายนอก พพ. ซึ่ง พพ. จำเป็นต้องใช้บริการดังกล่าว รวมทั้ง อยู่นอกเหนือการบริหารจัดการหรือการควบคุม พพ. ไม่สามารถป้องกันการหยุดหรือระงับการให้บริการได้ ซึ่ง พพ. จะต้องวางแผนการในลดผลกระทบจากความเสียหายที่จะเกิดขึ้นจากการไม่ได้รับบริการดังกล่าว

ทั้งนี้ ลักษณะรายละเอียดของความเสี่ยง (Description of Risk) แสดงดังตารางที่ 2

ตารางที่ 2 รายละเอียดของความเสี่ยง (Description of Risk)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
1. ความเสี่ยงจากสภาพแวดล้อม ความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	RIT01	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ความเสี่ยงจากประสิทธิภาพและความน่าเชื่อถือของระบบลดลงและทำให้เครื่องหยุดการทำงาน	▪ ระบบเครื่องปรับอากาศขัดข้อง	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ
2. ความเสี่ยงจากการเกิดอัคคีภัย	RIT02	ความเสี่ยงจากอัคคีภัย	การเกิดไฟไหม้อาคาร ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วนหรือได้รับความเสียหายทั้งหมด	▪ ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ▪ อุปกรณ์หรือเครื่องใช้ไฟฟ้าเก่า เช่น สายไฟ	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ อุปกรณ์เครือข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
3. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี และ/หรือ การถูกโจมตีโดยไวรัส (Virus) หรือ มัลแวร์ (Malware)	RIT03	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์ หรือระบบฐานข้อมูล	▪ Hacker/ Cracker ▪ การโจมตีการให้บริการ (denial of services/ DOS) ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย ▪ ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ▪ ไวรัส/ เวิร์ม	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ
4. ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT04	ความเสี่ยงด้านเทคนิค	พพ. ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับ - ส่งข้อมูลต่าง ๆ ได้	▪ ความล้มเหลวทางเทคนิค ▪ การดำเนินการของหน่วยงานภายนอก เช่น การไฟฟ้านครหลวง หรือผู้ให้บริการอินเตอร์เน็ตที่มีผลกระทบต่อระบบเครือข่ายของ พพ.	▪ ระบบเครือข่ายสื่อสาร ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
5. ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT05	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของ พพ. ส่งผลให้ พพ. ถูกฟ้องร้องได้	พพ. ถูกฟ้องร้องการละเมิดลิขสิทธิ์	▪ เครื่องคอมพิวเตอร์ ▪ อธิบดี พพ. ▪ ผู้ดูแลระบบ
6. ความเสี่ยงในการปรับปรุงบำรุงรักษาและจัดหาระบบงานสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ไม่เพียงพอ	RIT06	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงด้านระบบงานไม่สามารถสนับสนุนการทำงานปัจจุบันได้	▪ ความล้มเหลวทางเทคนิค ▪ การโจมตีการให้บริการ (denial of services/ DOS) ▪ การดักจับข้อมูล	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ เครื่องคอมพิวเตอร์ ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ดูแลระบบ
7. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT07	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดีหรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของ พพ.	▪ Hacker/ Cracker ▪ การโจมตีการให้บริการ (denial of services/ DOS) ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย ▪ ไวรัส/ เวิร์ม/ Ransomware	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ เครื่องคอมพิวเตอร์ ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
7. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ (ต่อ)					▪ ระบบเครือข่าย ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ
8. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	RIT08	ความเสี่ยงจากปัจจัยภายนอก	การเกิดกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย หรือทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดโดยไม่สมบูรณ์ (วันหยุดราชการ) ทำให้ข้อมูลสารสนเทศเกิดการสูญหาย และการให้บริการไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	▪ แหล่งกำเนิดไฟฟ้าขัดข้อง	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ เครื่องคอมพิวเตอร์ ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ระบบเครือข่าย ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
9. ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนาและส่งมอบให้กับ พพ.	RIT09	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การจัดซื้อ/ จัดจ้างพัฒนาระบบงานโดยหน่วยงานอื่น และไม่ผ่านการพิจารณาข้อกำหนดจากเจ้าหน้าที่เทคนิค ส่งผลต่อความเสี่ยงการบำรุงรักษาระบบในภายหลังที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยของสารสนเทศที่นำมาติดตั้งที่ส่วนของ ศทส.	▪ Hacker/ Cracker ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย ▪ ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ▪ ไวรัส/ เวิร์ม	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ
10. ความเสี่ยงจากการไม่ปฏิบัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	RIT10	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ระบบงานสารสนเทศไม่ได้รับการปรับปรุงให้มีความปลอดภัยและทันสมัยสอดรับกับพระราชบัญญัติฉบับนี้	▪ Hacker/ Cracker ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย	▪ ระบบฐานข้อมูล ▪ บุคลากรทั้งภายในและภายนอก พพ. ▪ ผู้ดูแลระบบ

8. การประมาณความเสี่ยง (Risk Estimation)

การประมาณความเสี่ยงเป็นการพิจารณาปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงใด และผลที่ตามมามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง (ดังตารางที่ 3) ระดับความรุนแรงของผลกระทบและระดับความเสี่ยง (ดังตารางที่ 4) ซึ่ง พพ. ใช้เกณฑ์ดังนี้

ตารางที่ 3 แสดงระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	> 4 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก/ไม่เกิด	1 ครั้ง/ปี

ในส่วนการประเมินระดับความรุนแรงของผลกระทบของความเสี่ยง ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินที่เกิดขึ้น มีแนวทางการประเมินดังนี้

1) ผลกระทบด้านการเงิน เป็นผลกระทบหรือความเสียหายที่เกิดจากความเสี่ยงและสามารถประเมินค่าเป็นตัวเงินได้ ได้แก่
   - ผลกระทบจากค่าความเสียหายในด้านต่าง ๆ ต่อทรัพย์สิน
   - ผลกระทบจากการลงทุน/ การร่วมลงทุน
   - ผลกระทบค่าใช้จ่ายการลงทุน
   - ผลกระทบต่อการเบิกจ่ายงบประมาณ

2) ผลกระทบต่อการดำเนินพันธกิจและความสามารถการเป็นผู้นำด้าน ICT มาใช้ประโยชน์และเกิดประสิทธิภาพสูงสุดหรือการบรรลุพันธกิจและวิสัยทัศน์ขององค์กร เป็นผลกระทบที่มีความเสียหายกับการดำเนินงานขององค์กรในภาพโดยรวม รวมถึงความสามารถในการเป็นผู้นำทางด้านสารสนเทศขององค์กร ได้แก่

- ผลกระทบจากปัจจัยภายนอก นโยบายรัฐบาล และกฎหมาย
- ผลกระทบจากการสูญเสียแนวร่วมกับผู้มีส่วนเกี่ยวข้อง Stakeholder
- ผลกระทบจากการสูญเสียความเชื่อมั่นและภาพลักษณ์ขององค์กรในการติดต่องาน
- ผลกระทบต่อระบบเทคโนโลยีสารสนเทศ
- ผลกระทบจากการดำเนินงานตามแผนงาน/ โครงการ

3) ผลกระทบด้านชื่อเสียงขององค์กร เป็นความเสียหายต่อชื่อเสียง ไม่ว่าจะเป็นผลจากการดำเนินงานทั้งทางตรงและทางอ้อม ที่ส่งผลต่อภาพพจน์และความเชื่อถือขององค์กร เช่น มีการเผยแพร่ข่าวในสื่อสิ่งพิมพ์ เป็นต้น

จากแนวทางการประเมินผลกระทบข้างต้น เมื่อพิจารณาร่วมกับกรอบการดำเนินงานของ พพ. ซึ่งเป็นองค์กรภาครัฐที่ไม่ได้มุ่งเน้นในด้านการแข่งขันทางธุรกิจ ดังนั้นในแนวทางการประเมินผลกระทบจึงได้เลือกใช้การวิเคราะห์ผลกระทบด้านการเงินหรือผลกระทบต่อระบบเทคโนโลยีสารสนเทศในการจัดระดับความรุนแรงของผลกระทบของความเสี่ยง (แสดงดังตารางที่ 4) ดังนี้

ตารางที่ 4 แสดงระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	> 10 ล้านบาท หรือเกิดความสูญเสียต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
4	สูง	> 5 แสนบาท – 10 ล้านบาท หรือเกิดปัญหากับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	> 2.5 แสนบาท – 5 แสนบาท หรือระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	> 1 แสนบาท – 2.5 แสนบาท หรือเกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก/ไม่เกิด	ไม่เกิน 100,000 บาท หรือเกิดเหตุร้ายที่ไม่มีความสำคัญ

ทั้งนี้ จากการประมาณความเสี่ยงข้างต้น สามารถแสดงรายละเอียดข้อมูลแสดงดังตารางที่ 5

ตารางที่ 5 การประมาณความเสี่ยง (Risk Estimation)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ	โอกาสเกิด/ ความถี่	ความรุนแรง
1. ความเสี่ยงจากสภาพแวดล้อมความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	RIT01	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	ความเสี่ยงจากประสิทธิภาพและความน่าเชื่อถือของระบบลดลง และทำให้เครื่องหยุดการทำงานได้	▪ ระบบเครื่องปรับอากาศขัดข้อง	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ	4	5
2. ความเสี่ยงจากการเกิดอัคคีภัย	RIT02	ความเสี่ยงจากอัคคีภัย	การเกิดไฟไหม้อาคารไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์ และระบบเครือข่ายหลักได้รับความเสียหายบางส่วนหรือได้รับความเสียหายทั้งหมด	▪ ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ▪ อุปกรณ์หรือเครื่องใช้ไฟฟ้าเก่า เช่น สายไฟ	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ อุปกรณ์เครือข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ	1	5

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ	โอกาสเกิด/ ความถี่	ความรุนแรง
3. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี และ/หรือการถูกโจมตี โดยไวรัส (Virus) หรือมัลแวร์ (Malware)	RIT03	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัส หรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	▪ Hacker/ Cracker ▪ การโจมตีการให้บริการ (denial of services/ DOS) ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย ▪ ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ▪ ไวรัส/ เวิร์ม	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ	5	4
4. ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT04	ความเสี่ยงด้านเทคนิค	พพ. ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับส่งข้อมูลต่าง ๆ ได้	▪ ความล้มเหลวทางเทคนิค ▪ การดำเนินการของหน่วยงานภายนอก เช่น การไฟฟ้านครหลวง หรือผู้ให้บริการอินเตอร์เน็ตที่มีผลกระทบต่อระบบเครือข่ายของ พพ.	▪ ระบบเครือข่ายสื่อสาร ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ▪ ผู้ดูแลระบบ	1	5

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ	โอกาสเกิด/ ความถี่	ความรุนแรง
5. ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT05	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของ พพ. ส่งผลให้ พพ. ถูกฟ้องร้องได้	▪ พพ. ถูกฟ้องร้องการละเมิดลิขสิทธิ์	▪ เครื่องคอมพิวเตอร์ ▪ อธิบดี พพ. ▪ ผู้ดูแลระบบ	1	4
6. ความเสี่ยงในการปรับปรุง บำรุงรักษาและจัดหาระบบงานสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ไม่เพียงพอ	RIT06	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงด้านระบบงานไม่สามารถสนับสนุนการทำงานปัจจุบันได้	▪ ความล้มเหลวทางเทคนิค ▪ การโจมตีการให้บริการ (denial of services/ DOS) ▪ การดักจับข้อมูล	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ เครื่องคอมพิวเตอร์ ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ดูแลระบบ	5	3

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ	โอกาสเกิด/ ความถี่	ความรุนแรง
7. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT07	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของ พพ. ส่งผลให้ พพ. ถูกฟ้องร้องได้	▪ พพ. ถูกฟ้องร้องการละเมิดลิขสิทธิ์	▪ เครื่องคอมพิวเตอร์ ▪ อธิบดี พพ. ▪ ผู้ดูแลระบบ	1	4
8. ความเสี่ยงในการปรับปรุง บำรุงรักษาและจัดหาระบบงานสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ไม่เพียงพอ	RIT08	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	การเกิดกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย หรือทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดโดยไม่สมบูรณ์ (วันหยุดราชการ) ทำให้ข้อมูลสารสนเทศเกิดการสูญหาย และการให้บริการไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	▪ แหล่งกำเนิดไฟฟ้าขัดข้อง	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ เครื่องคอมพิวเตอร์ ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ระบบเครือข่าย ▪ ผู้ใช้งาน ผู้ดูแลระบบ	2	5

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/ สิ่งคุกคาม	ผลกระทบ/ ผู้ได้รับผลกระทบ	โอกาสเกิด/ ความถี่	ความรุนแรง
9. ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนาและส่งมอบให้กับ พพ.	RIT09	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	การจัดซื้อ/ จัดจ้างพัฒนาระบบงาน โดยหน่วยงานอื่นและไม่ผ่านการพิจารณาข้อกำหนดจากเจ้าหน้าที่เทคนิค ส่งผลต่อความเสี่ยงการบำรุงรักษาระบบในภายหลังที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยของสารสนเทศ ที่นำมาติดตั้งที่ส่วนของ ศทส.	▪ Hacker/ Cracker ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย ▪ ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม ▪ ไวรัส/ เวิร์ม	▪ เครื่องคอมพิวเตอร์แม่ข่าย ▪ ระบบฐานข้อมูล ▪ ระบบงานสารสนเทศ ▪ ผู้ใช้งาน ผู้ดูแลระบบ	2	5
10. ความเสี่ยงจากการไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	RIT10	ความเสี่ยงด้านเทคนิค/ ความเสี่ยงจากผู้ปฏิบัติงาน	ระบบงานสารสนเทศไม่ได้รับการปรับปรุงให้มีความปลอดภัยและทันสมัยสอดรับกับพระราชบัญญัติฉบับนี้	▪ Hacker/ Cracker ▪ การดักจับข้อมูล ▪ คำสั่งเจตนาร้าย	▪ ระบบฐานข้อมูล ▪ บุคลากรทั้งภายในและภายนอก พพ. ▪ ผู้ดูแลระบบ	2	5

9. การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยงจะพิจารณาจากปัจจัยในขั้นตอนการประมาณความเสี่ยง คือ โอกาสที่ภัยคุกคาม จะเกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ ซึ่งการประเมินค่าความเสี่ยงต้องทำการวัดระดับความเสี่ยงเพื่อใช้ในการกำหนดกลยุทธ์การจัดการความเสี่ยงต่อไป

การวัดระดับความเสี่ยงเป็นการนำข้อมูลจากการประมาณความเสี่ยง (แสดงดังตารางที่ 5) มาพิจารณาประกอบกับตารางที่ 6 – 7 จึงได้การประเมินค่าความเสี่ยง (แสดงดังตารางที่ 8) ซึ่งมีรายละเอียดดังนี้

ตารางที่ 6 แสดงระดับคะแนนความเสี่ยง ระดับความเสี่ยง และกลยุทธ์ที่ใช้ในการจัดการความเสี่ยง

ระดับคะแนนความ	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 - 8	ต่ำ	ยอมรับความเสี่ยง	ขาว
9 - 12	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
13 - 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ส้ม
21 - 25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

9.1 แผนภูมิความเสี่ยง (Risk Map)

ตารางที่ 7 การวัดระดับความเสี่ยง

มาก

ผลกระทบ		
	ความเสี่ยงปานกลาง ▪ ผลกระทบรุนแรงมาก ▪ โอกาสเกิดน้อย	ความเสี่ยงสูง ▪ ผลกระทบรุนแรงมาก ▪ โอกาสเกิดมาก
	ความเสี่ยงต่ำ ▪ ผลกระทบน้อย ▪ โอกาสเกิดน้อย	ความเสี่ยงปานกลาง ▪ ผลกระทบน้อย ▪ โอกาสเกิดมาก

น้อย - **โอกาสที่จะเกิด** → มาก

9.2 การประเมินค่าความเสี่ยงที่เกิดขึ้น

ตารางที่ 8 การประเมินค่าความเสี่ยงที่เกิดขึ้น

ผลกระทบ/ความรุนแรง					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

โอกาสที่จะเกิด/ความถี่

สีแดง	ความเสี่ยงสูงมาก
สีส้ม	ความเสี่ยงสูง
สีเหลือง	ความเสี่ยงปานกลาง
สีขาว	ความเสี่ยงต่ำ (สามารถยอมรับได้)

ทั้งนี้ สามารถสรุปผลการประเมินค่าความเสี่ยงได้จากตารางที่ 9 และสามารถแสดงแผนภูมิความเสี่ยงด้านสารสนเทศ (Risk Map) แสดงดังตารางที่ 10

ตารางที่ 9 สรุปผลการประเมินค่าความเสี่ยง (Risk Evaluation)

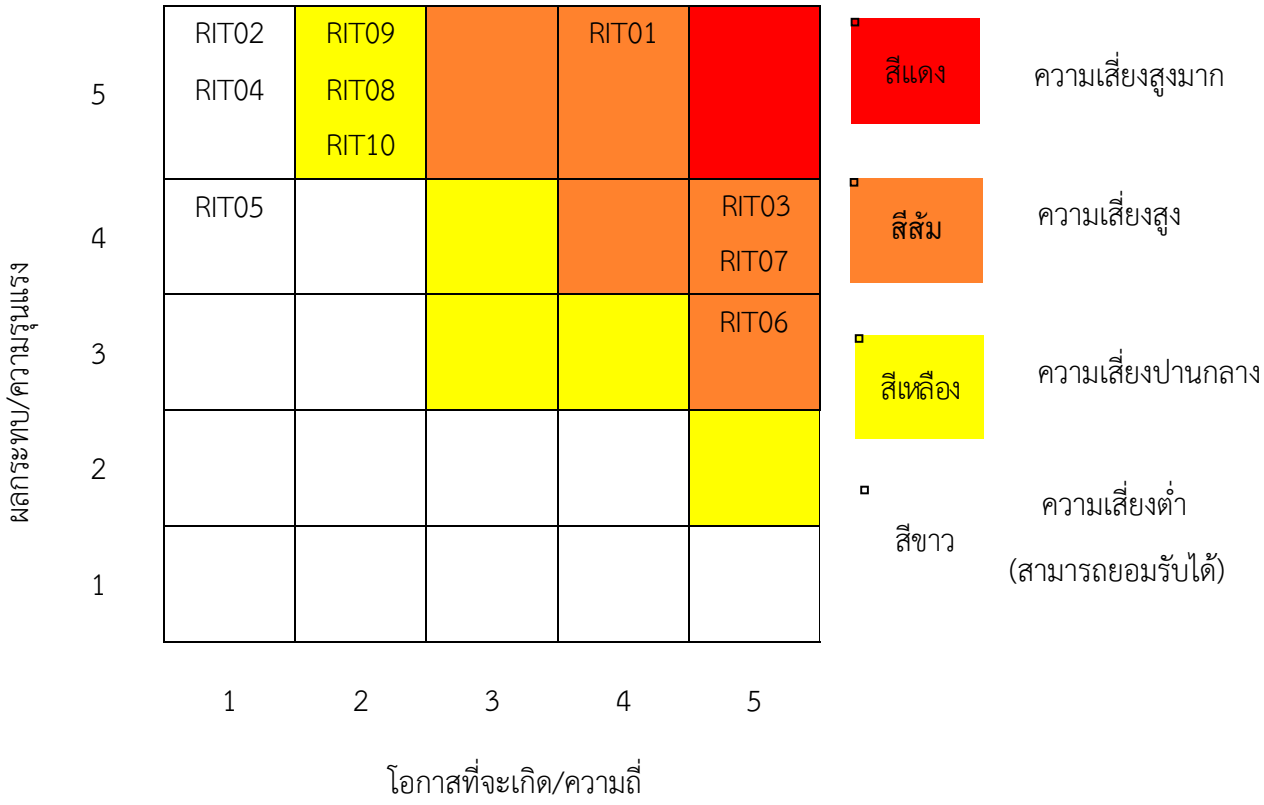
ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสที่จะเกิด/ความถี่	ความรุนแรง	ระดับคะแนน
1. ความเสี่ยงจากสภาพแวดล้อมความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	RIT01	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ความเสี่ยงจากประสิทธิภาพและความน่าเชื่อถือของระบบลดลง และทำให้เครื่องหยุดการทำงานได้	4	5	20
2. ความเสี่ยงจากการเกิดอัคคีภัย	RIT02	ความเสี่ยงจากอัคคีภัย	การเกิดไฟไหม้อาคารไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือได้รับความเสียหายทั้งหมด	1	5	5
3. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี และ/หรือการถูกโจมตี โดยไวรัส (Virus) หรือมัลแวร์ (Malware)	RIT03	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	5	4	20

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสที่จะเกิด/ความถี่	ความรุนแรง	ระดับคะแนน
4. ความเสี่ยงจากการเชื่อมต่อเครือข่าย อินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT04	ความเสี่ยงด้านเทคนิค	พพ. ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับส่งข้อมูลต่าง ๆ ได้	1	5	5
5. ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT05	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของ พพ. ส่งผลให้ พพ. ถูกฟ้องร้องได้	1	4	4
6. ความเสี่ยงในการปรับปรุง บำรุงรักษา และจัดหาระบบงานสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ไม่เพียงพอ	RIT06	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงด้านระบบงานไม่สามารถสนับสนุนการทำงานปัจจุบันได้	5	3	15
7. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT07	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดีหรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของ พพ.	5	4	20

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสที่จะเกิด/ความถี่	ความรุนแรง	ระดับคะแนน
8. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	RIT08	ความเสี่ยงจากปัจจัยภายนอก	การเกิดกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย หรือทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิด โดยไม่สมบูรณ์ (วันหยุดราชการ) ทำให้ข้อมูลสารสนเทศเกิดการสูญหาย และการให้บริการไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	2	5	10
9. ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนาและส่งมอบให้กับ พพ.	RIT09	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การจัดซื้อ/จัดจ้างพัฒนาระบบงาน โดยหน่วยงานอื่นและไม่ผ่านการพิจารณาข้อกำหนดจากเจ้าหน้าที่เทคนิค ส่งผลต่อความเสี่ยงการบำรุงรักษาระบบในภายหลัง ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยของสารสนเทศที่นำมาติดตั้งที่ส่วนของ ศทส.	2	5	10
10. ความเสี่ยงจากการไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	RIT10	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ระบบงานสารสนเทศไม่ได้รับการปรับปรุงให้มีความปลอดภัยและทันสมัยสอดรับกับพระราชบัญญัติฉบับนี้	2	5	10

9.3 แผนภูมิความเสี่ยงด้านสารสนเทศ (Risk Map)

ตารางที่ 10 แสดงการประเมินค่าความเสี่ยงที่เกิดขึ้น



10. ผลการวิเคราะห์ความเสี่ยง (Risk Analysis)

จากผลการประเมินความเสี่ยงสามารถจัดลำดับความสำคัญของความเสี่ยงด้านสารสนเทศในการบริหารจัดการได้อย่างมีประสิทธิภาพ แสดงดังตารางที่ 11

ตารางที่ 11 ผลการวิเคราะห์ความเสี่ยง (Risk Analysis)

ลำดับ	ความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
1	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี และ/หรือการถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์ (Malware)	RIT03	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การเปลี่ยนแปลงแก้ไขข้อมูลบนเว็บไซต์หรือระบบฐานข้อมูล	20
2	ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	RIT07	ความเสี่ยงจากผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดีหรือถูกดักจับข้อมูลสำคัญ หรือการส่งข้อมูลคำสั่งเจตนาร้าย หรือการติดไวรัสหรือเวิร์ม ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของ พพ.	20
3	ความเสี่ยงจากสภาพแวดล้อม ความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	RIT01	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ความเสี่ยงจากประสิทธิภาพและความน่าเชื่อถือของระบบลดลง และทำให้เครื่องหยุดการทำงานได้	20

ลำดับ	ความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
4	ความเสี่ยงในการปรับปรุงบำรุงรักษา และจัดหาระบบงานสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ไม่เพียงพอ	RIT06	ความเสี่ยงด้านการบริหารจัดการ	ระบบงานสารสนเทศและระบบคอมพิวเตอร์ไม่ได้รับการปรับปรุงให้มีความทันสมัยหรือความปลอดภัยตามที่ผู้พัฒนาระบบหรือบริษัทผู้ผลิตได้กำหนดทำให้มีความเสี่ยงด้านระบบงานไม่สามารถสนับสนุนการทำงานปัจจุบันได้	15
5	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	RIT08	ความเสี่ยงจากปัจจัยภายนอก	การเกิดกระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์ได้รับความเสียหาย หรือทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิด โดยไม่สมบูรณ์ ทำให้ข้อมูลสารสนเทศเกิดการสูญหาย และการให้บริการไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	10
6	ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนา และส่งมอบให้กับ พพ.	RIT09	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	การจัดซื้อ/จัดจ้างพัฒนาระบบงานโดยหน่วยงานอื่นและไม่ผ่านการพิจารณาข้อกำหนดจากเจ้าหน้าที่เทคนิค ส่งผลต่อความเสี่ยงการบำรุงรักษาระบบภายในภายหลังที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยของสารสนเทศที่นำมาติดตั้งที่ส่วนของ ศทส.	10
7	ความเสี่ยงจากการไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	RIT10	ความเสี่ยงด้านเทคนิค/ความเสี่ยงจากผู้ปฏิบัติงาน	ระบบงานสารสนเทศไม่ได้รับการปรับปรุงให้มีความปลอดภัยและทันสมัยสอดรับกับพระราชบัญญัติฉบับนี้	10
8	ความเสี่ยงจากการเกิดอัคคีภัย	RIT02	ความเสี่ยงจากอัคคีภัย	การเกิดไฟไหม้อาคารไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับ	5

ลำดับ	ความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
				ความเสียหายบางส่วน หรือได้รับความเสียหายทั้งหมด	
9	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	RIT04	ความเสี่ยงด้านเทคนิค	พพ. ไม่สามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตในการรับ-ส่งข้อมูลต่าง ๆ ได้	5
10	ความเสี่ยงจากการละเมิดลิขสิทธิ์	RIT05	ความเสี่ยงจากผู้ปฏิบัติงาน	การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ถูกต้องตามกฎหมายบนเครื่องคอมพิวเตอร์ของ พพ. ส่งผลให้ พพ. ถูกฟ้องร้องได้	4

หมายเหตุ : เรียงตามชื่อความเสี่ยงที่มีค่าระดับความเสี่ยงมากไปหาค่าระดับความเสี่ยงน้อยสุด

11. การจัดการความเสี่ยง (Risk Management)

สำนักงาน กพร. กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาพิจารณาดำเนินการบริหารจัดการความเสี่ยงก่อน โดยความเสี่ยงที่มีระดับความเสี่ยงมากกว่า 16 ขึ้นไปถือเป็นความเสี่ยงสูงมาก ดังนั้น คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารได้วิเคราะห์ระดับความเสี่ยง โดยพิจารณาร่วมกับบริบทความเสี่ยงและแนวโน้มการโจมตีด้านระบบสารสนเทศข้างต้น เห็นว่า พพ. ควรมีการป้องกันความเสี่ยงที่รัดกุมและมีความปลอดภัยสูงกว่าที่ กพร. กำหนด เนื่องจากระบบสารสนเทศของ พพ. เป็นเป้าโจมตีจากผู้ไม่หวังดี คณะทำงานฯ จึงสรุปว่าเกณฑ์การพิจารณาระดับความเสี่ยงที่ต้องนำมาดำเนินการบริหารจัดการความเสี่ยงคือ ความเสี่ยงที่มีระดับความเสี่ยงระดับต่ำ (ตั้งแต่ระดับ 1 – 8) ถึงความเสี่ยงสูงมาก (ตั้งแต่ระดับ 9 ขึ้นไป) ซึ่งสอดคล้องกับข้อกำหนดของ กพร. การดำเนินการบริหารจัดการความเสี่ยงแสดงดังตารางที่ 12

ตารางที่ 12 การจัดการความเสี่ยง (Risk Management)

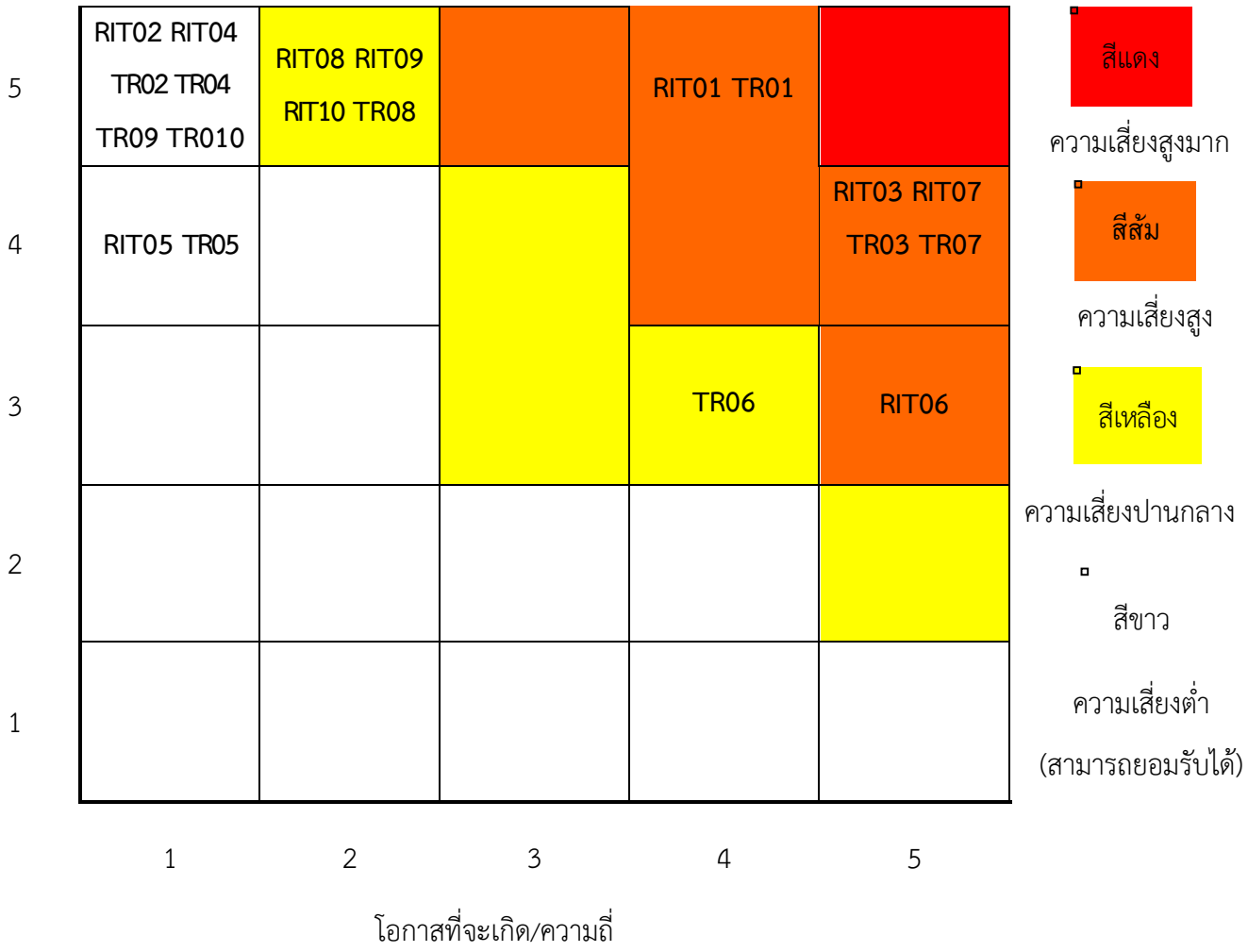
รหัส	ความเสี่ยง	ค่าระดับความเสี่ยง	ค่าระดับความเสี่ยงคงเหลือ	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
TR03	ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี และ/หรือการถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์ (Malware)	20	5 x 4 = 20	ป้องกันความเสี่ยง (มีมาตรการติดตาม)	1) ทดสอบความปลอดภัยของระบบ เช่น SQL Injection, การเจาะระบบ (Penetration Testing) เป็นต้น 2) จัดหา ติดตั้ง และตรวจสอบ Anti-Virus และ update patch บนเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายเพิ่มเติม 3) เพิ่มความถี่ในการสำรองข้อมูล และ/หรือสำรองข้อมูลไว้ที่อื่นเพิ่มเติม 4) บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย การตรวจสอบ Policy และ Log ของระบบ เพื่อป้องกันการบุกรุกผ่านเครือข่าย และติดตามอย่างสม่ำเสมอ

รหัส	ความเสี่ยง	ค่าระดับความเสี่ยง	ค่าระดับความเสี่ยงคงเหลือ	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
TR03 (ต่อ)	ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี และ/หรือการถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์ (Malware)				5) บันทึกความผิดปกติที่เกิดกับระบบเทคโนโลยีสารสนเทศที่ ศทส. รับผิดชอบ พร้อมทั้งวิธีแก้ไข
TR07	ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	20	4 x 4 = 16	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	1) เผยแพร่ความรู้เกี่ยวกับความมั่นคงปลอดภัยภายในกรมตามช่องทางต่าง ๆ 2) ศึกษามาตรฐานความมั่นคงปลอดภัยของกรม เช่น ISO27001 (ความมั่นคงปลอดภัยของสารสนเทศ) หรือ ISO27701 (มาตรฐานการจัดการข้อมูลส่วนบุคคล)
TR01	ความเสี่ยงจากสภาพแวดล้อมความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	20	4 x 5 = 20	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	จัดทำแผนการบำรุงรักษาเครื่องปรับอากาศในห้องควบคุมและห้องสำรองไฟฟ้า
TR06	ความเสี่ยงในการปรับปรุงบำรุงรักษา และจัดหาระบบงานสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ไม่เพียงพอ	15	4 x 3 = 12	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1) จัดหางบประมาณในส่วนการพัฒนาระบบเพิ่มเติม นอกจากการบำรุงรักษา 2) ปฏิบัติตามแนวทางประกาศ การจัดหา และจัดสรรครุภัณฑ์คอมพิวเตอร์ 3) บริหารจัดการปรับปรุงกระบวนการในการขอซื้อ การยืมครุภัณฑ์คอมพิวเตอร์
TR08	ความเสี่ยงจากกระแสไฟฟ้า	10	2 x 5 = 10	ยอมรับความเสี่ยง	1) เจ้าหน้าที่ตรวจสอบความพร้อมของระบบสำรองไฟฟ้าทุก 3

รหัส	ความเสี่ยง	ค่าระดับความเสี่ยง	ค่าระดับความเสี่ยงคงเหลือ	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
	ขัดข้อง				เดือน 2) วางแผนจัดหาอุปกรณ์การแจ้งเตือน กรณีไฟดับ
TR09	ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนา และส่งมอบให้กับ พพ.	10	1 x 5 = 5	ยอมรับความเสี่ยง	1) ศึกษาแนวทางมาตรฐานการพัฒนาระบบ สำหรับไปใช้ในการจัดทำ ข้อกำหนดการจ้าง (TOR) พัฒนาระบบสารสนเทศ โดยกำหนดให้ ผู้รับจ้างเพิ่ม E-R Diagram Data Dictionary และขั้นตอนการบำรุงรักษา (ก่อนร่าง TOR) และหาได้รับงบให้เก็บ TOR และ Breakdown 2) คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ พิจารณาการจัดหาระบบคอมพิวเตอร์ของกรม
TR10	ความเสี่ยงจากการไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	10	1 x 5 = 5	ยอมรับความเสี่ยง	1) ทบทวนระบบงานที่จัดเก็บข้อมูลส่วนบุคคลในกรม 2) อบรมให้เจ้าหน้าที่มีความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 3) ศึกษาเครื่องมือที่นำมาใช้ควบคุมข้อมูลส่วนบุคคล

รหัส	ความเสี่ยง	ค่าระดับความเสี่ยง	ค่าระดับความเสี่ยงคงเหลือ	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง
TR02	ความเสี่ยงจากการเกิดอัคคีภัย	5	1 x 5 = 5	ยอมรับความเสี่ยง (มีแผนควบคุมความเสี่ยง)	1) ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิง อย่างน้อย 2 ครั้ง/ปี โดยเจ้าหน้าที่ 2) ทบทวนแผนการเคลื่อนย้ายระบบคอมพิวเตอร์ตามลำดับความสำคัญ 3) ทบทวนและซักซ้อมแผนการจัดการหรือแก้ไขปัญหาจากอัคคีภัย 2 ครั้ง/ปี
TR04	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	5	1 x 5 = 5	ยอมรับความเสี่ยง	1) ตรวจสอบสัญญาณอินเตอร์เน็ตวงจรสำรอง (Backup link) เพื่อสลับช่องทางการใช้อินเตอร์เน็ต 2) ซักซ้อมแผนการหากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้
TR05	ความเสี่ยงจากการละเมิดลิขสิทธิ์	4	1 x 4 = 4	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	1) มีสติ๊กเกอร์เตือนการละเมิดลิขสิทธิ์ 2) ศึกษาแนวทางในการควบคุมการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ 3) แนะนำผู้ใช้งานภายในกรมให้ทราบเกี่ยวกับบริการ (Service) หรือเครื่องมือต่าง ๆ ที่เป็น freeware ผ่านช่องทางออนไลน์

ตารางที่ 13 แสดงความเสี่ยงด้านสารสนเทศคงเหลือหลังดำเนินตามแนวทาง/กลยุทธ์



หมายเหตุ : RIT คือ ความเสี่ยงที่เกิดขึ้น
TR คือ ความเสี่ยงด้านสารสนเทศคงเหลือหลังดำเนินตามแนวทาง/กลยุทธ์

หลังจากกำหนดแนวทางบริหารจัดการความเสี่ยง และควบคุมความเสี่ยงต่าง ๆ ค่าประเมินระดับความเสี่ยงคงเหลืออยู่ในเกณฑ์ความเสี่ยงต่ำ (สามารถยอมรับได้) ซึ่งเป็นเกณฑ์ที่สามารถยอมรับได้แสดงดังตารางที่ 15

คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดทำแผนบริหารความเสี่ยงเพื่อใช้ในการติดตามและควบคุมความเสี่ยงต่าง ๆ ให้เป็นไปตามแนวทางที่วางไว้ และมีแผนการดำเนินงานที่รัดกุมสามารถนำไปเป็นกรอบในการปฏิบัติได้ดังนี้

12. แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ปีงบประมาณ 2567

จากการจัดการความเสี่ยงสามารถนำมาจัดทำแผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีหน่วยงานรับผิดชอบคือ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) มีระยะเวลาดำเนินการระหว่างเดือนตุลาคม 2566 – กันยายน 2567 แสดงดังตารางที่ 14 ซึ่งมีรายละเอียดดังนี้

ตารางที่ 14 แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ปีงบประมาณ 2567

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT01	ความเสี่ยงจากสภาพแวดล้อมความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	จัดทำแผนการบำรุงรักษาเครื่องปรับอากาศในห้องควบคุมและห้องสำรองไฟฟ้า	ทส.	ทั้งปีงบประมาณ 67	←	—	→	—	—	—	—	—	—	—	—	—
RIT02	ความเสี่ยงจากการเกิดอัคคีภัย	1) ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิงโดยเจ้าหน้าที่	ทส. พส.	2 ครั้ง/ปี				●						●		
		2) ทบทวนแผนการเคลื่อนย้ายระบบคอมพิวเตอร์ตามลำดับความสำคัญ	ทส. พส.	ธ.ค.			●									

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT03	การถูกบุกรุกโดยผู้ไม่ประสงค์ดีและ/หรือ การถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์	1) ทดสอบความปลอดภัยของระบบ เช่น SQL Injection, การเจาะระบบ (Penetration test) เป็นต้น	ทส. พส. บภ. อร.	1 ครั้ง/ ปี												●
		2) จัดหา ติดตั้ง และตรวจสอบ Anti-Virus และ update patch บนเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายเพิ่มเติม	ทส. พส.	ทุกครั้งที่จัดซื้อเครื่องคอมพิวเตอร์	←											→
				ติดตั้ง Anti – Virus (Freeware) สำหรับเครื่องคอมพิวเตอร์ที่หมดระยะเวลาประกัน												
		3) เพิ่มความถี่ในการสำรองข้อมูลและ/หรือสำรองข้อมูลไว้ที่อื่นเพิ่มเติม	ทส. พส. บภ. อร.	ทั้งปี งบประมาณ 67	←											→

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT03 (ต่อ)	การถูกบุกรุกโดยผู้ไม่ประสงค์ดีและ/หรือ การถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์	4) บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย การตรวจสอบ Policy และ Log ของระบบ เพื่อป้องกันการบุกรุกผ่านเครือข่ายและติดตามอย่างสม่ำเสมอ	ทส.	ทั้งปีงบประมาณ 67	←											→
		5) บันทึกความผิดปกติที่เกิดกับระบบเทคโนโลยีสารสนเทศ ที่ ศทส. รับผิดชอบ พร้อมทั้งวิธีแก้ไข	ศทส.	ทั้งปีงบประมาณ 67	←											→
RIT04	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	1) ตรวจสอบสัญญาณอินเทอร์เน็ตและมีวงจรสำรอง (Backup link)	ทส.	เดือนละครั้ง	●	●	●	●	●	●	●	●	●	●	●	●
		2) ซักซ้อมแผนการหากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	ทส.	ธ.ค.			●									

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT05	ความเสี่ยงจากการละเมิดลิขสิทธิ์	1) มีสติ๊กเกอร์เตือนการละเมิดลิขสิทธิ์	ทส.	ทุกครั้งที่มีการจัดซื้อจัดจ้าง				●						●		
		2) ศึกษาแนวทางในการควบคุมการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์	ทส. พส.	ต.ค.	●											
		3) แนะนำผู้ใช้งานภายในกรมให้ทราบเกี่ยวกับบริการ (Service) หรือเครื่องมือต่าง ๆ ที่เป็น freeware ผ่านช่องทางออนไลน์	ทส. พส.	ทั้งปีงบประมาณ 67	←											→
RIT06	ความเสี่ยงในการปรับปรุงบำรุงรักษาและจัดหาระบบงานสารสนเทศระบบเครือข่ายระบบคอมพิวเตอร์ไม่เพียงพอ	1) จัดหางบประมาณในส่วนการปรับปรุง/พัฒนาระบบเพิ่มเติมนอกจากการบำรุงรักษา	ศทส.	ต.ค.	●											
		2) ปฏิบัติตามแนวทางประกาศการจัดหา และจัดสรรครุภัณฑ์คอมพิวเตอร์		ทุกครั้งที่มีการจัดซื้อ จัดจ้าง	←											→
		3) บริหารจัดการปรับปรุงกระบวนการในการขอซื้อ การยืมครุภัณฑ์คอมพิวเตอร์		ทั้งปีงบประมาณ 67	←											→

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT07	ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	1) เผยแพร่ความรู้เกี่ยวกับความมั่นคงปลอดภัยภายในกรมตามช่องทางต่าง ๆ	ทส. พส.	ต.ค.	●											
		2) ศึกษามาตรฐานความมั่นคงปลอดภัยของกรม เช่น ISO27001 (ความมั่นคงปลอดภัยของสารสนเทศ) หรือ ISO27701 (มาตรฐานการจัดการข้อมูลส่วนบุคคล)	ทส. พส. บภ.	ม.ค. – เม.ย. 67				←	—	—	—	→				
RIT08	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	1) เจ้าหน้าที่ตรวจสอบความพร้อมของระบบสำรองไฟฟ้าทุก 3 เดือน	ทส.	ทุก 3 เดือน	●			●			●			●		
		2) วางแผนจัดอุปกรณ์การแจ้งเตือนกรณีไฟดับ		1 ครั้ง/ ปี												●

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT09	ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนาและส่งมอบให้กับ พพ.	1) ศึกษาแนวทางมาตรฐานการพัฒนาระบบ สำหรับไปใช้ในการจัดทำข้อกำหนดการจ้าง (TOR) พัฒนาระบบสารสนเทศ โดยกำหนดให้ผู้รับจ้างเพิ่ม E-R Diagram, Data Dictionary และขั้นตอนการบำรุงรักษา (ก่อนร่าง TOR) และหากได้รับงบให้เก็บ TOR และBreakdown	ศทส.	ต.ค. 66 – ม.ค. 67	←	—	—	→								
		2) คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์พิจารณาการจัดหาระบบคอมพิวเตอร์ของกรม	ศทส.	ทุกครั้งที่มีการจัดซื้อ / จัดจ้างพัฒนาระบบ	←	—	—	—	—	—	—	—	—	—	—	→

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2566			พ.ศ. 2567								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT10	ความเสี่ยงจากการไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	1) ทบทวนระบบงานที่จัดเก็บข้อมูลส่วนบุคคลในกรม	ทส. พส.	ทั้งปี งบประมาณ 67	◄	—	—	—	—	—	—	—	—	—	—	►
		2) อบรมให้เจ้าหน้าที่มีความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	ศทส.	ทั้งปี งบประมาณ 67	◄	—	—	—	—	—	—	—	—	—	—	►
		3) ศึกษาเครื่องมือที่นำมาใช้ควบคุมข้อมูลส่วนบุคคล	ศทส.	ต.ค. 66 – ม.ค. 67	◄	—	—	►								

หมายเหตุ

สัญลักษณ์ ● หมายถึง ดำเนินการในเดือนที่ระบุให้เสร็จสิ้น

สัญลักษณ์ ◄——► หมายถึง ดำเนินการในช่วงเดือนที่ระบุให้เสร็จสิ้น

สัญลักษณ์ ◄·····► หมายถึง ดำเนินการเป็นประจำตลอดช่วงเดือนที่ระบุอย่างน้อย เดือนละ 1 ครั้ง

สัญลักษณ์ ◄– · –► หมายถึง ดำเนินการเป็นประจำตลอดช่วงเดือนที่ระบุอย่างน้อย สัปดาห์ละ 1 ครั้ง

บรรณานุกรม

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่ม 136 (ตอนที่ 69 ก), หน้า 2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). สถิติภัยคุกคาม. https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-STATISTICS-2565.aspx

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์ ตั้งแต่วันที่ 1 ต.ค. 2565 – 4 ส.ค. 2566. https://drive.ncsa.or.th/s/yAxrZfxbeZ86jWe/download/สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์%202566.pdf

World Economic Forum, (2023). The Global Risks Report 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

ภาคผนวก

แผนปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ปีงบประมาณ 2566

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT01	ความเสี่ยงจากสภาพแวดล้อม ความชื้นหรืออุณหภูมิในห้องปฏิบัติการคอมพิวเตอร์	1) จัดทำแผนการบำรุงรักษาเครื่องปรับอากาศในห้องควบคุมและห้องสำรองไฟฟ้าอย่างต่อเนื่อง	ทส.	ทั้งปีงบประมาณ 66	←											→
		2) ติดอุปกรณ์ตรวจสอบความชื้นในห้องปฏิบัติการคอมพิวเตอร์และห้องสำรองไฟฟ้า	ศทส.	1 ครั้ง/ ปี												●
RIT02	ความเสี่ยงจากการเกิดอัคคีภัย	1) ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิงโดยเจ้าหน้าที่	ทส. พส.	2 ครั้ง/ปี				●						●		
		2) ทบทวนแผนการเคลื่อนย้ายระบบคอมพิวเตอร์ตามลำดับความสำคัญ	ทส. พส.	ธ.ค.			●									
		3) ทบทวนและซักซ้อมแผนการจัดการหรือแก้ไขปัญหาจากอัคคีภัย	ทส. พส. อร.	2 ครั้ง/ปี					●						●	

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT03	การถูกบุกรุกโดยผู้ไม่ประสงค์ดีและ/หรือ การถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์ (Malware)	1) ทดสอบความปลอดภัยของระบบ เช่น SQL Injection, การเจาะระบบ (Penetration Testing) เป็นต้น	ทส.	2 ครั้ง/ปี					●						●	
		2) จัดหา ติดตั้ง และตรวจสอบ Anti-Virus และ update patch บนเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายเพิ่มเติม	ทส. พส.	ทุกครั้งที่จัดซื้อเครื่องคอมพิวเตอร์	←											→
				ติดตั้ง Anti-Virus (freeware) สำหรับเครื่องคอมพิวเตอร์ที่หมดระยะเวลาประกัน	←											→
		3) เพิ่มความถี่ในการสำรองข้อมูลและ/หรือสำรองข้อมูลไว้ที่อื่นเพิ่มเติม	ทส. พส. อร.	ทั้งปีงบประมาณ 66	←											→

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT03 (ต่อ)	การถูกบุกรุกโดยผู้ไม่ประสงค์ดี และ/หรือ การถูกโจมตีโดยไวรัส (Virus) หรือมัลแวร์ (Malware)	4) บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่าย การตรวจสอบ Policy และ Log ของระบบ เพื่อป้องกันการบุกรุกผ่านเครือข่าย และติดตามอย่างสม่ำเสมอ	ทส.	ทั้งปี งบประมาณ 66	←											→
		5) บันทึกความผิดปกติที่เกิดกับระบบเทคโนโลยีสารสนเทศ ที่ ศทส. รับผิดชอบ พร้อมทั้งวิธีแก้ไข	ศทส.	ทั้งปี งบประมาณ 66	←											→
RIT04	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	1) มีวงจรสำรอง (Backup link) เพื่อสลับช่องทางการใช้อินเตอร์เน็ตเมื่อมีปัญหาในการใช้งาน และ/หรือใช้เครือข่ายสารสนเทศภาครัฐ (GIN) เพื่อเพิ่มแบนด์วิธ (Bandwidth)	ทส.	2 ครั้ง/ปี	●						●					

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT04 (ต่อ)	ความเสี่ยงจากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	2) ซักซ้อมแผนการหากการเชื่อมต่อเครือข่ายอินเทอร์เน็ตล้มเหลวหรือไม่สามารถใช้งานได้	ทส.	ธ.ค.			●									
RIT05	ความเสี่ยงจากการละเมิดลิขสิทธิ์	1) มีสติ๊กเกอร์เตือนการละเมิดลิขสิทธิ์	ทส.	ทุกครั้งที่มีการจัดซื้อจัดจ้าง	←											→
		2) ศึกษาแนวทางในการควบคุมการติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์	ทส. พส.	ต.ค.			●									
		3) แนะนำผู้ใช้งานภายในกรมให้ทราบเกี่ยวกับบริการ (Service) หรือเครื่องมือต่าง ๆ ที่เป็น freeware ผ่านช่องทางออนไลน์	ทส. พส.	ทั้งปีงบประมาณ 66	←											→

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT06	การถูกบุกรุกความเสี่ยงในการปรับปรุงบำรุงรักษาและจัดหาระบบงานสารสนเทศระบบเครือข่ายระบบคอมพิวเตอร์ไม่เพียงพอ	1) จัดหางบประมาณในส่วนการปรับปรุง/พัฒนาระบบเพิ่มเติมนอกจากการบำรุงรักษา	ศทส.	ต.ค.	●											
		2) ปฏิบัติตามแนวทางประกาศการจัดหา และจัดสรรครุภัณฑ์คอมพิวเตอร์	ทส.	ทุกครั้งที่มีการจัดซื้อ จัดจ้าง	◄											►
		3) บริหารจัดการปรับปรุงกระบวนการในการขอซื้อ การยืมครุภัณฑ์คอมพิวเตอร์	ทส. พส.	ทั้งปีงบประมาณ 66	◄											►
		4) มีระบบสำรองเพิ่มเติม และเพิ่มความถี่การสำรองข้อมูล เพื่อป้องกันการโจมตี	ทส. พส.	ต.ค.	●											

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT07	ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวังและการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	1) เผยแพร่ความรู้เกี่ยวกับความมั่นคงปลอดภัยภายในกรมตามช่องทางต่าง ๆ	ทส. พส.	ต.ค.	●											
		2) ศึกษามาตรฐานความมั่นคงปลอดภัยของกรม เช่น ISO27001 (ความมั่นคงปลอดภัยของสารสนเทศ) หรือ ISO27701 (มาตรฐานการจัดการข้อมูลส่วนบุคคล)	ทส. พส. บภ.	ม.ค. – เม.ย. 66				←	—	—	→					
RIT08	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง	1) เจ้าหน้าที่ตรวจสอบความพร้อมของระบบสำรองไฟฟ้าทุก 3 เดือน	ทส.	ทุก 3 เดือน	●			●			●			●		
		2) ติดตั้งอุปกรณ์การแจ้งเตือนกรณีไฟดับ	ศทส.	1 ครั้ง/ ปี												●

รหัส	ความเสี่ยง	แนวทางการควบคุม	ผู้รับผิดชอบหลัก	ระยะเวลา	พ.ศ. 2565			พ.ศ. 2566								
					ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
RIT09	ความเสี่ยงจากคุณภาพของระบบที่จ้างพัฒนาและส่งมอบให้กับ พพ.	1) ผลักดันให้ศูนย์ฯ มีส่วนร่วมกับทุกหน่วยงาน ในการจัดทำข้อกำหนด การจ้าง (TOR) ที่เกี่ยวกับการพัฒนาระบบสารสนเทศ	ทส. พส.	ทุกครั้งที่มีการจัดซื้อ/จัดจ้างพัฒนาระบบ	←	—	—	—	—	—	—	—	—	—	—	→
		2) คณะทำงานขับเคลื่อนเทคโนโลยีดิจิทัล พิจารณาการจัดหาระบบคอมพิวเตอร์ของกรม	ทส. พส.	ทุกครั้งที่มีการจัดซื้อ/จัดจ้างพัฒนาระบบ	←	—	—	—	—	—	—	—	—	—	—	→
		3) ศึกษาแนวทางมาตรฐานการพัฒนาระบบ สำหรับไปใช้ในการจัดทำข้อกำหนดการจ้าง (TOR) พัฒนาระบบสารสนเทศ โดยกำหนดให้ผู้รับจ้างเพิ่ม E-R Diagram, Data Dictionary และขั้นตอนการบำรุงรักษา (ก่อนร่าง TOR) และหากได้รับงบให้เก็บ TOR และBreakdown	ทส. พส. บภ.	ต.ค. 65 – ม.ค. 66	←	—	—	→								

หมายเหตุ สัญลักษณ์ ● หมายถึง ดำเนินการในเดือนที่ระบุให้เสร็จสิ้น

สัญลักษณ์ ◄——► หมายถึง ดำเนินการในช่วงเดือนที่ระบุให้เสร็จสิ้น

สัญลักษณ์ ◄·····► หมายถึง ดำเนินการเป็นประจำตลอดช่วงเดือนที่ระบุอย่างน้อย เดือนละ 1 ครั้ง

สัญลักษณ์ ◄– · –► หมายถึง ดำเนินการเป็นประจำตลอดช่วงเดือนที่ระบุอย่างน้อย สัปดาห์ละ 1 ครั้ง