แผนบริหารจัดการความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
พ.ศ.๒๕๖๔

คำนำ

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทสส.ทอ. จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการจัดการและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับป้องกันภัยคุกคามทางด้านระบบสารสนเทศและไซเบอร์ ที่มีแนวโน้มจะกิดขึ้นกับหน่วยงานในอนาคต

ทสส.ทอ.เป็นหน่วยขึ้นตรง ทอ. มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านระบบบัญชาการและควบคุม ข่าย เครือข่าย เทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์และการสงครามอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีเจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เป็นผู้บังคับบัญชารับผิดชอบ ซึ่ง ทสส.ทอ. มีระบบสารสนเทศที่ใช้งานทั้งด้านการเตรียมกำลังและใช้กำลังทางอากาศ จึงจำเป็นต้องป้องกันภัยคุกคามรูปแบบต่าง ๆ รวมทั้งภัยคุกคามทางด้านไซเบอร์ อันจะส่งผลกระทบกับการใช้ข้อมูลและระบบสารสนเทศของหน่วย

การจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ. เป็นส่วนหนึ่งที่จะทำให้เกิดความชัดเจนในการเตรียมการบริหารจัดการความเสี่ยงที่อาจส่งผลกระทบกับระบบสารสนเทศของหน่วยงานได้อย่างถูกต้อง เหมาะสม เพื่อลดโอกาสหรือบรรเทาผลกระทบความเสี่ยงที่มีอยู่

คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.
กันยายน ๒๕๖๔

สารบัญ

หน้า

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๑. หลักการและเหตุผล

กองทัพอากาศ กำหนดวิสัยทัศน์การเป็นกองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Force in ASEAN) ตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operation : NCO) ได้นำเอาเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานทั้งด้านการเตรียมกำลังและใช้กำลังทางอากาศ ฉะนั้น เพื่อให้การนำเทคโนโลยีสารสนเทศและการสื่อสารมาสนับสนุน การปฏิบัติงานให้เกิดประโยชน์สูงสุด และลดความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นทั้งในปัจจุบันและอนาคต จนส่งผลกระทบต่อการปฏิบัติงานที่ใช้เทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ดี เพื่อรักษาไว้ซึ่งคุณสมบัติหลักของความมั่นคงปลอดภัยของระบบสารสนเทศ ได้แก่ การรักษาความลับ (Confidentiality) ความครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability)โดยลดความเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารจะต้องถูกกำหนดไว้อย่างเหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานให้พ้นจากความสูญเสียที่อาจเกิดขึ้นในระหว่างการปฏิบัติภารกิจให้ประสบผลสำเร็จลุล่วง ทั้งนี้ การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของหน่วยงาน ที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า

๒. วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ภัยคุกคาม ความผิดพลาด หรือเหตุอันไม่พึงประสงค์ที่อาจเกิดขึ้นกับระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้มีแผนในการควบคุมและกำหนดแนวทางปฏิบัติต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๓. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานให้เจ้าหน้าที่ที่เกี่ยวข้องนำไปใช้ประโยชน์

๔. เพื่อให้การจัดการภายในหน่วยงาน มีประสิทธิภาพในการปรับตัวให้ทันต่อการเปลี่ยนแปลงที่รวดเร็วของเทคโนโลยีสารสนเทศและการสื่อสาร และมีความยืดหยุ่นต่อภัยคุกคามทางไซเบอร์ของหน่วยงาน

๓. ขอบเขตการดำเนินการ

เป็นแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ. โดยกำหนดแนวทางปฏิบัติให้กับผู้รับผิดชอบระบบสารสนเทศและการสื่อสาร รวมทั้งบุคลากร คอมพิวเตอร์และอุปกรณ์เครือข่าย พร้อมกับการสร้างจิตสำนึกและความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

๔. การวิเคราะห์ความเสี่ยง

ความเสี่ยงด้านต่างๆ ที่หน่วยงานเผชิญอยู่ เมื่อนำมาวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ. สามารถระบุความเสี่ยงจำแนกตามประเภทความเสี่ยงได้เป็น ๔ ด้าน ดังนี้

๔.๑ ความเสี่ยงด้านเทคนิค (Risk of Technical Operation : RT) เป็นความเสี่ยงที่อาจเกิดขึ้นจากการขัดข้องของคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง การถูกโจมตีจากไวรัสหรือโปรแกรมประสงค์ร้าย (Malware) หรือ การถูกก่อกวนจากผู้ไม่ประสงค์ดี เช่น Hacker หรือ Cracker เป็นต้น ซึ่งสามารถวิเคราะห์ความเสี่ยงด้านเทคนิค (RT) ได้ดังนี้

ชื่อความเสี่ยง	รหัส
๑. อุปกรณ์เครือข่าย และเครื่องแม่ข่ายในระบบสารสนเทศชำรุด ขัดข้องไม่สามารถทำงานได้โดยสาเหตุทางเทคนิค	RT01
๒. ระบบจัดเก็บข้อมูลชำรุด หรือขัดข้องโดยสาเหตุทางเทคนิค	RT02
๓. เครือข่ายอินเทอร์เน็ต และเครือข่ายภายใน ทสส.ทอ.ไม่สามารถใช้งานได้	RT03
๔. เครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ในเครือข่ายติดมัลแวร์ หรือไวรัสคอมพิวเตอร์โดยสาเหตุทางเทคนิค	RT04
๕. รางปลั๊กไม่ได้มาตรฐาน/กำลังไฟฟ้าที่ไม่รองรับหรือไม่เพียงพอต่อการใช้งาน	RT05
๖. ข้อมูลในระบบสารสนเทศสูญหาย ถูกทำลาย หรือถูกแก้ไขเปลี่ยนแปลง	RT06

๔.๒ ความเสี่ยงจากผู้ปฏิบัติงาน (Risk of Personnel : RP) เป็นความเสี่ยงที่อาจเกิดขึ้นจากผู้ใช้ขาดความรู้ ความระมัดระวังในการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการดำเนินการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ ซึ่งอาจส่งผลให้เกิดความเสียหายต่อสารสนเทศได้ สามารถวิเคราะห์ความเสี่ยงจากผู้ปฏิบัติงาน (RP) ได้ดังนี้

ชื่อความเสี่ยง	รหัส
๑. ผู้ปฏิบัติงานขาดความรู้ในการระบุและแก้ไขปัญหาที่เกิดขึ้นในระบบสารสนเทศ	RP01
๒. ผู้ปฏิบัติงานนำอุปกรณ์คอมพิวเตอร์หรือสมาร์ทดีไวซ์ (Smart Device) ส่วนตัวมาเชื่อมต่อเข้ากับระบบเครือข่ายของ ทสส.ทอ.	RP02
๓. ผู้ใช้งานในระบบถูกหลอกให้เปิดเผยข้อมูลบัญชี รหัสผ่าน โดยการ Phishing หรือข้อมูลในระบบสารสนเทศถูกทำลาย แก้ไขเปลี่ยนแปลง หรือถูกโจรกรรมโดยผู้ไม่ประสงค์ดีจากการสมัครใจเข้าร่วมกิจกรรมผ่านโซเชียลมีเดีย	RP03
๔. ผู้ใช้งานดาวน์โหลดหรือนำซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์มาติดตั้งใช้งาน	RP04
๕. การเข้าถึงข้อมูลของบุคคลอื่น	RP05
๖. การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RP06

๔.๓ ความเสี่ยงจากภัยธรรมชาติหรือสถานการณ์ฉุกเฉิน (Risk of Natural Disasters and Emergency Situations : RE) เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับสารสนเทศ เช่น ไฟฟ้าขัดข้อง เกิดอัคคีภัย อุทกภัย อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น ซึ่งสามารถวิเคราะห์ความเสี่ยงจากภัยธรรมชาติหรือสถานการณ์ฉุกเฉิน (RE) ได้ดังนี้

ชื่อความเสี่ยง	รหัส
๑. ระบบสารสนเทศและทรัพย์สินเสียหายจากระบบไฟฟ้าขัดข้อง	RE01
๒. การเกิดภัยพิบัติทางธรรมชาติ เช่น อุทกภัย, แผ่นดินไหว, อาคารถล่ม เป็นต้น	RE02
๓. ระบบสารสนเทศและทรัพย์สินเสียหายจากอัคคีภัย	RE03
๔. เกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RE04

๔.๔ ความเสี่ยงด้านการบริหารจัดการ (Risk of Management : RM) เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านระบบสารสนเทศ ซึ่งสามารถวิเคราะห์ความเสี่ยงการบริหารจัดการ (RM) ได้ดังนี้

ชื่อความเสี่ยง	รหัส
๑. การขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร	RM01
๒. ขาดการวางแผนในการสำรองข้อมูล และการกู้คืนข้อมูล	RM02
๓. ขาดอุปกรณ์สำรองไฟที่เพียงพอ	RM03
๔. ขาดมาตรการการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศที่ดี	RM04

๕. การประมาณความเสี่ยง (Risk Estimation)

เป็นการกำหนดคะแนนความเสี่ยงของเหตุการณ์ที่จะเกิดโดยใช้ค่าปัจจัย (Factor) ๒ ค่า คือ โอกาส (Likelihood) ของการเกิดเหตุการณ์ว่ามีมากน้อยเพียงไร และผลกระทบ (Impact) ที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด โดยคะแนนความเสี่ยง = ค่าโอกาส x ค่าผลกระทบ

โอกาส แบ่งเป็น ๕ ค่า ดังนี้

ค่าโอกาส	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	เกิดขึ้นบ่อย (๑ เดือนต่อครั้งหรือมากกว่า)
๔	สูง	เกิดขึ้นค่อนข้างบ่อย (๑ – ๖ เดือนต่อครั้ง)
๓	ปานกลาง	เกิดขึ้นตามโอกาส (๑ ปีต่อครั้ง)
๒	น้อย	เกิดขึ้นน้อยครั้ง (๒ – ๓ ปีต่อครั้ง)
๑	น้อยมาก	แทบไม่เกิดขึ้นเลย (๕ ปีต่อครั้ง)

และผลกระทบ แบ่งเป็น ๕ ค่า ดังนี้

ค่าผลกระทบ	ความรุนแรง	คำอธิบาย
๕	สูงมาก	เกิดความเสียหายทางกายภาพต่อระบบสารสนเทศที่สำคัญทั้งหมด ทำให้ไม่สามารถปฏิบัติภารกิจได้ เกิดความเสียหายอย่างมากต่อชีวิตและทรัพย์สิน
๔	สูง	เกิดข้อขัดข้องกับระบบสารสนเทศที่สำคัญ เกิดความล่าช้าในการปฏิบัติงาน มีความเสียหายของข้อมูลบางส่วน
๓	ปานกลาง	เกิดข้อขัดข้องบางระบบงาน แต่ไม่กระทบต่อระบบสารสนเทศที่สำคัญ สามารถฟื้นฟูและซ่อมแซมได้
๒	น้อย	ระบบงานสะดุดหรือล่าช้า ไม่เกิดผลกระทบต่อระบบสารสนเทศ สามารถฟื้นฟูและซ่อมแซมได้รวดเร็ว
๑	น้อยมาก	เกิดข้อขัดข้องระดับบุคคล ไม่เกิดผลกระทบต่อระบบสารสนเทศ

๖. ลักษณะและรายละเอียดของความเสี่ยง (Description of risk)

ลักษณะและรายละเอียดของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ. ได้จากการวิเคราะห์และระดมความคิดของผู้รับผิดชอระบบสารสนเทศของหน่วย รวมถึงเหตุการณ์ที่หน่วยเผชิญ (ตามแนวทางการระบุความเสี่ยง) ดังนี้

ตารางที่ ๑ ลักษณะและรายละเอียดของความเสี่ยง

รหัส	ชื่อความเสี่ยง	ลักษณะ	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส (P)	ผลกระทบ (S)	ระดับความเสี่ยง (P x S)
RT01	๑. อุปกรณ์เครือข่าย และเครื่องแม่ข่ายในระบบสารสนเทศชำรุด ขัดข้อง ไม่สามารถทำงานได้โดยสาเหตุทางเทคนิค	- เกิดข้อผิดพลาด หรือข้อขัดข้องของอุปกรณ์หรือฮาร์ดแวร์ภายในทำให้อุปกรณ์เครือข่าย และเครื่องแม่ข่ายเกิดการชำรุดเสียหายไม่สามารถทำงานได้	- ข้อผิดพลาดจากความชำรุดของฮาร์ดแวร์หรือข้อขัดข้องของซอฟต์แวร์	- ผู้ใช้ไม่สามารถเข้าใช้งานอุปกรณ์นั้นได้ - การรับส่งข้อมูลในระบบสารสนเทศหยุดชะงัก ระบบสารสนเทศไม่สามารถทำงานได้	๑	๕	๕
RT02	๒. ระบบจัดเก็บข้อมูลชำรุด หรือขัดข้องโดยสาเหตุทางเทคนิค	- ระบบจัดเก็บข้อมูล หรือโปรแกรมจัดการฐานข้อมูลชำรุด ขัดข้อง ทำให้ไม่สามารถเรียกใช้ข้อมูลที่ถูกจัดเก็บอยู่ภายในระบบ หรือฐานข้อมูลมาใช้งานได้	- อุปกรณ์จัดเก็บข้อมูลชำรุด ขัดข้อง - ข้อผิดพลาดของซอฟต์แวร์จัดการฐานข้อมูล - โปรแกรมที่ควบคุมการเขียน/อ่านข้อมูลบนอุปกรณ์ เขียน/อ่านตำแหน่งข้อมูลเดิมซ้ำ ๆ ทำให้เกิดความเสื่อมสภาพทางกายภาพ หรือเกิด Bad Sector ตามมา	- ข้อมูลในอุปกรณ์จัดเก็บสูญหาย หรือเสียหาย ส่งผลต่อการประมวลผลและการปฏิบัติงานของผู้ใช้	๒	๕	๑๐
RT03	๓. เครือข่ายอินเทอร์เน็ตและเครือข่ายภายใน ทสส.ทอ.ไม่สามารถใช้งานได้	- อุปกรณ์เครือข่าย หรือเครื่องแม่ข่ายในระบบสารสนเทศชำรุด ขัดข้อง - ระบบสารสนเทศทั้งหมดไม่สามารถใช้งานเครือข่ายได้	- การปรับเปลี่ยนการตั้งค่าของอุปกรณ์ในระบบเครือข่าย - สายสัญญาณขัดข้องหรือชำรุด	- ผู้ใช้งานไม่สามารถใช้งานเครือข่ายทั้งเครือข่ายภายใน ทสส.ทอ. และเครือข่ายอินเทอร์เน็ตเพื่อการปฏิบัติงานได้	๓	๕	๑๕

รหัส	ชื่อความเสี่ยง	ลักษณะ	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส (P)	ผลกระทบ (S)	คะแนนความเสี่ยง (P x S)
RT04	๔. เครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ในเครือข่ายติดมัลแวร์ หรือไวรัสคอมพิวเตอร์โดยสาเหตุทางเทคนิค	- เกิดการโจมตีทางไซเบอร์ เครื่องคอมพิวเตอร์แม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจ่ายไปในระบบ	- ขาดอุปกรณ์ป้องกันบนระบบเครือข่าย (Firewall) ที่ทันสมัยและมีประสิทธิภาพสูง - เครื่องคอมพิวเตอร์ใน ทสส.ทอ.บางส่วนไม่ลงโปรแกรม Antivirus	- ระบบสารสนเทศล้มเหลว และเกิดการแพร่กระจายของ มัลแวร์ขยายเป็นวงกว้าง	๓	๕	๑๕
RT05	๕. รางปลั๊กไม่ได้มาตรฐาน/กำลังไฟฟ้าที่ไม่รองรับหรือไม่เพียงพอต่อการใช้งาน	- การต่อพ่วงอุปกรณ์หลาย ๆ ตัว เข้ากับรางปลั๊กที่ไม่ได้มาตรฐาน ทำให้เกิดความเสียหายที่รางปลั๊ก ส่งผลให้เกิดระบบไฟตัด และอุปกรณ์ระบบที่มีความสำคัญดับโดยไม่ได้ทำการ shut down อย่างถูกต้อง	- รางปลั๊กไม่ได้มาตรฐาน หรือมีกำลังที่รองรับไม่เพียงพอ	- อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เครือข่ายได้รับความเสียหาย - การประมวลผลหยุดชะงัก	๓	๒	๖
RT06	๖. ข้อมูลในระบบสารสนเทศสูญหาย ถูกทำลาย หรือถูกแก้ไขเปลี่ยนแปลง	- ระบบสารสนเทศของหน่วยงานมีช่องโหว่ ทำให้ข้อมูลถูกผู้ไม่ประสงค์ดีเข้ามาทำการแก้ไขเปลี่ยนแปลง ถูกโจรกรรม หรือทำลายข้อมูลในระบบ	- ระบบปฏิบัติการมีช่องโหว่ - การออกแบบซอฟต์แวร์ในระบบสารสนเทศมีช่องโหว่ - ขาดการตรวจสอบสิทธิ์ในการเข้าใช้งานระบบสารสนเทศ	- ระบบสารสนเทศประมวลผลผิดพลาด - ข้อมูลที่มีความสำคัญ/มีชั้นความลับ ถูกละเมิดความปลอดภัย - ข้อมูลของหน่วยงานถูกทำลาย แก้ไข ทำให้ไม่สามารถใช้งานได้	๒	๕	๑๐
RP01	๗. ผู้ปฏิบัติงานขาดความรู้ในการระบุและแก้ไขปัญหาที่เกิดขึ้นในระบบสารสนเทศ	- ระบบสารสนเทศล้มเหลว แต่ผู้ปฏิบัติงานไม่สามารถระบุได้ว่าเกิดจากสาเหตุใด ทำให้ไม่ทราบวิธีการแก้ปัญหาที่ถูกต้อง	- ขาดความรู้ในการปฏิบัติงานที่เกี่ยวกับระบบสารสนเทศ	- ระบบสารสนเทศหยุดชะงัก ไม่สามาถทำงานต่อได้ - อุปกรณ์ระบบสารสนเทศเสียหายจากการแก้ไขไม่ถูกวิธี	๔	๑	๔

รหัส	ชื่อความเสี่ยง	ลักษณะ	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส (P)	ผลกระทบ (S)	คะแนนความเสี่ยง (P x S)
RP02	๘. ผู้ปฏิบัติงานนำอุปกรณ์คอมพิวเตอร์หรือสมาร์ทดีไวซ์ (Smart Device) ส่วนตัวมาเชื่อมต่อเข้ากับระบบเครือข่ายของ ทสส.ทอ.	- โปรแกรมที่ติดตั้งบนคอมพิวเตอร์หรือ สมาร์ทดีไวซ์ (Smart Device) ไม่ได้มาจากแหล่งที่เชื่อถือได้ อาจมีโปรแกรมประสงค์ร้ายฝังอยู่ภายใน และเมื่อนำมาเชื่อมต่อในระบบสารสนเทศของ ทสส.ทอ. ก็จะเข้ามาฝังตัวหรือกระทำการใด ๆ เพื่อก่อให้เกิดความเสียหายต่อระบบ	- ติดตั้งโปรแกรมที่ไม่มีแหล่งที่มาชัดเจน ไม่ได้รับการรับรองลงในเครื่อง - เครื่องที่นำเข้ามาใช้งานในระบบไม่ได้ผ่านการตรวจสอบโดยผู้ดูแลระบบ	- เกิดช่องโหว่ในระบบเครือข่าย - เครื่องคอมพิวเตอร์และเครื่องแม่ข่ายในระบบเครือข่ายติดมัลแวร์ หรือโดนโจมตีจากผู้ไม่ประสงค์ดี	๔	๕	๒๐
RP03	๙. ผู้ใช้งานในระบบถูกหลอกให้เปิดเผยข้อมูลบัญชี รหัสผ่าน โดยการ Phishing หรือ ข้อมูลในระบบสารสนเทศถูกทำลาย แก้ไข เปลี่ยนแปลง หรือถูกโจรกรรมโดยผู้ไม่ประสงค์ดีจากการสมัครใจเข้าร่วมกิจกรรมผ่านโซเชียลมีเดีย	- ถูกหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สาคัญ ในการแสวงหาผลกำไร ข่มขู่ ประจาน กลั่นแกล้งรังแก ให้เสียชื่อเสียง	- ขาดการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศตามความเหมาะสม - การขาดความรู้ความเข้าใจและจิตสำนึกต่อการรักษาความปลอดภัยระบบสารสนเทศ	- ไม่สามารถปฏิบัติงานได้ และเกิดผลกระทบอย่างต่อเนื่อง - การรั่วไหลของข้อมูล ถูกแก้ไขข้อมูล หรือถูกทำลาย - เสียชื่อเสียงและภาพลักษณ์ของหน่วย - ระบบสารสนเทศ ระบบคอมพิวเตอร์และเครือข่ายเกิดการหยุดชะงัก ขัดข้อง และเสียหาย	๓	๕	๑๕
RP04	๑๐. ผู้ใช้งานดาวน์โหลดหรือนำซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์มาติดตั้งใช้งาน	- การดาวน์โหลด หรือนำซอฟต์แวร์ไม่ถูกลิขสิทธิ์มาติดตั้งใช้งานเอง โดยไม่แจ้งผู้ดูแลระบบ ซึ่งซอฟต์แวร์เหล่านั้นอาจจะมีช่องโหว่ หรือ Malware แฝงตัวอยู่ด้วย	- ผู้ใช้งานดาวน์โหลดหรือนำซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์มาติดตั้งเพื่อใช้งานตามความต้องการ	- เครื่องคอมพิวเตอร์ทำงานช้าลง ข้อมูลอาจรั่วไหล รวมทั้งอาจมีช่องโหว่ให้ Hacker โจมตีระบบสารสนเทศได้	๓	๔	๑๒
RP05	๑๑. การเข้าถึงข้อมูลของบุคคลอื่น	- การอำพราง/สวมรอยผู้ใช้งาน หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (ไม่มีสิทธิ์)	- ผู้ใช้ขาดความระมัดระวังในการใช้งานระบบสารสนเทศ - การกำหนดสิทธิ์การเข้าถึงข้อมูลที่ไม่เหมาะสม	- ข้อมูลความลับรั่วไหล หรือบัญชีผู้ใช้ถูกนำไปใช้ในทางที่ไม่ดี/ไม่เหมาะสม	๒	๓	๖

รหัส	ชื่อความเสี่ยง	ลักษณะ	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส (P)	ผลกระทบ (S)	คะแนนความเสี่ยง (P x S)
RP06	๑๒. การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	- การโจรกรรมเครื่องคอมพิวเตอร์/อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายใน เช่น CPU HDD เป็นต้น ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายกับข้อมูลบนเครื่องคอมพิวเตอร์นั้นๆ ได้	- การรักษาความปลอดภัยของสถานที่มีประสิทธิภาพไม่ดี - การขาดจิตสำนึกความรับผิดชอบต่อทรัพย์สินของทางราชการ	- ไม่สามารถปฏิบัติงานได้ และเกิดผลกระทบอย่างต่อเนื่อง - การรั่วไหลของข้อมูล	๒	๔	๘
RE01	๑๓. ระบบสารสนเทศและทรัพย์สินเสียหายจากระบบไฟฟ้าขัดข้อง	- เกิดอุบัติเหตุ หรือข้อขัดข้องของระบบไฟฟ้าภายนอกหน่วยงาน ที่ส่งผลกระทบให้กระแสไฟฟ้าภายในหน่วยงานขัดข้องไปด้วย และอาจเป็นเหตุให้อุปกรณ์ไฟฟ้าต่าง ๆ เสียหาย	- กระแสไฟฟ้าขัดข้อง - ระบบไฟฟ้าของ ทอ. ที่เข้ามายัง ทสส.ทอ. ขัดข้อง จากสาเหตุต่าง ๆ รวมไปถึงแรงดันไฟไม่คงที่	- ระบบสารสนเทศทั้งหมด ไม่สามารถใช้งานเครือข่ายได้อุปกรณ์จัดเก็บข้อมูลเสียหาย ทำให้การปฏิบัติภารกิจหยุดชะงัก	๒	๔	๘
RE02	๑๔. การเกิดภัยพิบัติทางธรรมชาติ เช่น อุทกภัย แผ่นดินไหว อาคารถล่ม เป็นต้น	- เมื่อเกิดภัยพิบัติขึ้นแล้วไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์/อุปกรณ์ต่าง ๆ ได้ทัน ทำให้ได้รับความเสียหายบางส่วนหรือทั้งหมด	- สภาพอากาศที่เปลี่ยนแปลง/มาตรการป้องกัน/ลดผลกระทบขาดประสิทธิภาพ	- เครื่องคอมพิวเตอร์/อุปกรณ์เสียหาย/ระบบสารสนเทศเสียหาย ไม่สามารถใช้งานได้	๑	๕	๕
RE03	๑๕. ระบบสารสนเทศและทรัพย์สินเสียหายจากอัคคีภัย	- เกิดอุบัติเหตุทำให้เกิดอัคคีภัย อันเป็นเหตุให้ทรัพย์สินต่าง ๆ และระบบสารสนเทศของหน่วยเสียหาย	- ไฟฟ้าลัดวงจร - เกิดการติดไฟของวัสดุโดยคาดไม่ถึง จากการเก็บวัสดุไวไฟไม่ถูกต้อง	- เกิดความเสียหายทางกายภาพต่ออุปกรณ์ในระบบสารสนเทศ ทำให้การปฏิบัติภารกิจหยุดชะงัก	๑	๕	๕
RE04	๑๖. เกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	- เกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย มีการปิดกั้นพื้นที่จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- การเมือง/ประชาชนที่ไม่ยอมรับความคิดเห็นที่แตกต่างกัน	- ไม่สามารถเข้ามาปฏิบัติงานได้ตามปกติ	๒	๒	๔
RM01	๑๗. การขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร	- ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีจำนวนไม่เพียงพอที่จะสนับสนุนภาระงานที่มีอยู่	- การไม่ได้รับการบรรจุตามความต้องการกำลังพล - การโยกย้ายบุคลากรด้านสารสนเทศ	- การปฏิบัติงานด้านสารสนเทศล่าช้า/หยุดชะงัก - กระทบต่อการพัฒนาและควบคุมดูแลระบบสารสนเทศ	๒	๓	๖

รหัส	ชื่อความเสี่ยง	ลักษณะ	ปัจจัยเสี่ยง	ผลกระทบ	โอกาส (P)	ผลกระทบ (S)	คะแนนความเสี่ยง (P x S)
RM02	๑๘. ขาดการวางแผนในการสำรองข้อมูล และการกู้คืนข้อมูล	- ไม่สามารถกู้คืนข้อมูลจากอุปกรณ์จัดเก็บข้อมูลได้ เนื่องจากผู้ใช้งานระบบไม่ทราบวิธีปฏิบัติในการแก้ไขที่ถูกต้องได้เอง	- ขาดการวางแผนในการสำรองข้อมูล และการกู้คืนข้อมูล - ไม่มีคู่มือการปฏิบัติ แนวทาง หรือวิธีการที่ชัดเจนสำหรับการสำรองข้อมูลที่สำคัญให้แก่ผู้ใช้งาน	- ข้อมูลสารสนเทศที่สำคัญหรือเป็นความลับที่ใช้ในการประมวลผลชำรุด สูญหาย หรือถูกทำลาย ทำให้การปฏิบัติภารกิจหยุดชะงัก	๒	๓	๖
RM03	๑๙. ขาดการจัดหาอุปกรณ์สำรองไฟฟ้าที่เพียงพอ	- เกิดกระแสไฟฟ้าขัดข้องไม่คงที่ จนส่งผลกระทบต่อข้อมูลและอุปกรณ์ในระบบสารสนเทศที่สำคัญ	- ขาดการใช้งาน และจัดหาอุปกรณ์สำรองไฟฟ้าที่เพียงพอ	- อุปกรณ์เครือข่าย เครื่องลูกข่าย และเครื่องแม่ข่ายเสื่อมสภาพเร็วกว่าอายุการใช้งานปกติ ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย หรือเกิดความเสียหายทางกายภาพจนไม่สามารถให้บริการและปฏิบัติงานได้	๒	๔	๘
RM04	๒๐. ขาดมาตรการการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศที่ดี	- การเข้าถึงระบบสารสนเทศมีหลายระดับ ทั้งการเข้าถึงทางกายภาพ ฐานข้อมูล บัญชีเข้าใช้งานระบบ ซึ่งต้องมีการจำกัดสิทธิ์ตามหน้าที่ที่แต่ละคนได้รับ	- ขาดมาตรการดูแลรักษาความปลอดภัยระบบสารสนเทศ - ขาดมาตรการป้องกันทางกายภาพ ทำให้ผู้ไม่ประสงค์ดีเข้าถึงแหล่งเก็บข้อมูลได้ - ผู้ใช้งานขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ ไม่จัดเก็บชื่อผู้ใช้และรหัสผ่านให้เป็นความลับ	- ข้อมูลที่มีความสำคัญชั้นความลับ ถูกละเมิดความปลอดภัย - ไม่สามารถควบคุมการเข้าถึงและติดตามผู้เข้าใช้งานระบบได้ - ยากต่อการป้องกันอุบัติเหตุอันเกิดจากผู้ไม่เกี่ยวข้องเข้ามาในพื้นที่ติดตั้งระบบ	๑	๕	๕

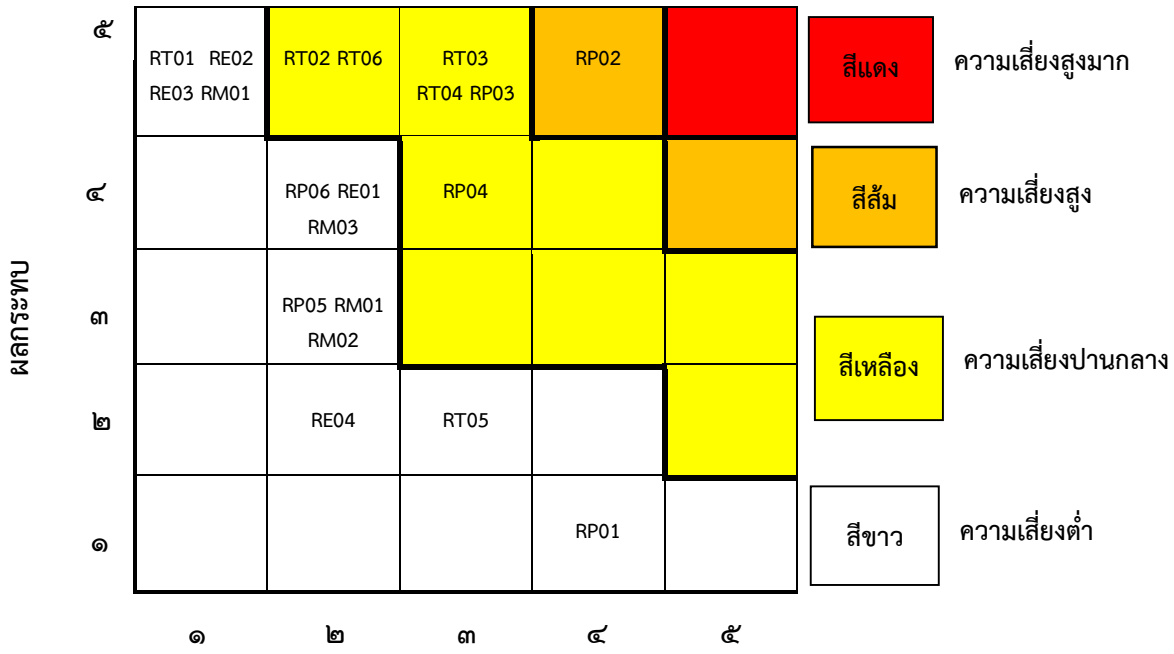
๗. การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยง จะคำนวณค่าผลคะแนนของความเสี่ยง โดยพิจารณาจากปัจจัยของขั้นตอนที่ผ่านมา โดยใช้คะแนนความเสี่ยงซึ่งเป็นผลคูณของโอกาสในการเกิดเหตุการณ์ (ค่า : ๑ - ๕ คะแนน) กับระดับผลกระทบของเหตุการณ์นั้น (ค่า : ๑ - ๕ คะแนน) แล้วแปลงเป็นค่าระดับความเสี่ยง ๔ ระดับ (ต่ำ, ปานกลาง, สูง, สูงมาก) ดังแสดงในตารางที่ ๒ และตารางการแบ่งพื้นที่ระดับความเสี่ยง (ตารางที่ ๓)

ตารางที่ ๒ การแบ่งพื้นที่สีตามคะแนนความเสี่ยงและค่าระดับความเสี่ยง

ผลคะแนนความเสี่ยง	ค่าระดับความเสี่ยง	พื้นที่สี
๑ - ๘	ต่ำ	ขาว
๙ – ๑๖	ปานกลาง	เหลือง
๑๗ - ๒๔	สูง	ส้ม
๒๕	สูงมาก	แดง

ตารางที่ ๓ การแบ่งพื้นที่ความเสี่ยงตามระดับค่าความเสี่ยง



๘. การบรรเทาความเสี่ยง (Risk Mitigation)

การบรรเทาความเสี่ยงเกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยง และการลงมือควบคุมการลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากการประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องยาก ผู้บริหารองค์กรจะต้องเป็นผู้รับผิดชอบการทำงานนี้ด้วยเงื่อนไขในการใช้งบประมาณที่สมดุล เพื่อให้เกิดประสิทธิภาพสูงสุด และใช้วิธีการควบคุมที่เหมาะสมที่สุดเพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยส่งผลกระทบต่อภารกิจและทรัพยากรของหน่วยให้น้อยที่สุด ทางเลือกเพื่อการบรรเทาความเสี่ยงสามารถแบ่งออกเป็น ๔ ประเภท ดังนี้

๘.๑ การยอมรับความเสี่ยง (Risk Acceptance) ใช้กับ ความเสี่ยงที่อยู่ในระดับต่ำ มีค่าโอกาสและผลกระทบไม่รุนแรงที่จะส่งผลต่อการทำงาน ชีวิต หรือทรัพย์สิน ระบบสารสนเทศยังคงดำเนินงานไปตามปกติ ซึ่งพิจารณาแล้วอาจจะยอมรับในผลที่อาจตามมาได้ เช่น การพิสูจน์ตัวตนเพียงใช้ชื่อผู้ใช้งานและรหัสผ่าน มีความเสี่ยง เพราะอาจมีการขโมยไปใช้ได้ แต่การจะลงทุนด้าน Biometrics ในการตรวจลายนิ้วมือหรือม่านตา ที่มีค่าใช้จ่ายสูง พิจารณาได้ว่าไม่คุ้มค่า เป็นต้น หน่วยงานอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปและปรับปรุงเมื่อมีโอกาส

แนวทางการปฏิบัติ ปฏิบัติตามระเบียบปฏิบัติ คู่มือ ที่เกี่ยวข้อง

๘.๒ การถ่ายโอนความเสี่ยง (Risk Transfer) ใช้กับ ความเสี่ยงที่ต้องเผชิญเพื่อให้บรรลุวัตถุประสงค์ขององค์กร แต่มีความเสี่ยงที่ไม่สามารถยอมรับได้ ไม่สามารถหลีกเลี่ยงหรือจัดการได้ด้วยตนเอง จึงต้องถ่ายโอนความเสี่ยงไปให้ผู้อื่น เพื่อเป็นการบรรเทาความสูญเสียหรือแบ่งเอาความเสี่ยงไป เช่น การรับประกันอุปกรณ์เครือข่ายที่มีอายุการใช้งานรับประกันทั่วไปเพียงหนึ่งปี ซึ่งอุปกรณ์ดังกล่าวมีความซับซ้อนไม่สามารถซ่อมเองได้ เพื่อให้การดำรงการปฏิบัติภารกิจของหน่วย อาจพิจารณาเลือกการขยายระยะเวลารับประกันหรือทำสัญญาจ้างเหมาซ่อมบำรุง เพื่อให้บริษัทผู้เชี่ยวชาญจากภายนอกรับความเสี่ยงดังกล่าวแทน เป็นต้น

แนวทางการปฏิบัติ ให้หน่วยงานอื่นที่มีความชำนาญสูงกว่าในการดูแลรับผิดชอบ

๘.๓ การจำกัดความเสี่ยง (Risk Limitation) ใช้กับ ความเสี่ยงที่ไม่สามารถหลีกเลี่ยงได้แต่จำเป็นต้องดำเนินกิจกรรมนั้นต่อไปเพื่อให้บรรลุวัตถุประสงค์ขององค์กร จึงต้องวิเคราะห์หาปัจจัยที่เป็นสาเหตุที่ทำให้เกิดความเสี่ยง และผลกระทบของความเสี่ยงดังกล่าวที่จะตามมา เพื่อหาทางควบคุม ติดตาม ป้องกันไม่ให้เกิดความเสี่ยงนั้นด้วยขีดความสามารถของหน่วยเอง

แนวทางการปฏิบัติ วิเคราะห์หนทางในการลดโอกาสในการเกิดความเสี่ยงและลดความรุนแรงของผลกระทบเมื่อเกิดความเสี่ยง

๘.๔ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) ใช้กับ ความเสี่ยงที่มีความรุนแรง ไม่สามารถยอมให้เกิดได้ ควรหยุดการกระทำที่จะก่อให้เกิดความเสี่ยง โดยหาทนทางอื่นเพื่อหลีกเลี่ยงไม่ให้ความเสี่ยงนั้นเกิด เช่น องค์กรไม่มีขีดความสามารถในการพัฒนาระบบสารสนเทศที่มีความซับซ้อนสูง จะต้องจ้างผู้เชี่ยวชาญจากภายนอกมาให้คำปรึกษา อำนวยความสะดวก หรือดำเนินการแทน เป็นต้น

แนวทางการปฏิบัติ เสนอโครงการจัดซื้อจัดจ้าง เพื่อให้ผู้ที่เชี่ยวชาญกว่าดำเนินการแทน

๙. การจัดการความเสี่ยง (Risk Management)

กำหนดความสนใจต่อความเสี่ยงที่เกิดขึ้นตามคะแนนความเสี่ยงที่ได้จากการประเมิน ดังนี้

ระดับความเสี่ยงระดับต่ำ มีคะแนน = ๑ – ๘
ระดับความเสี่ยงระดับปานกลาง มีคะแนน = ๙ – ๑๖
ระดับความเสี่ยงระดับสูง มีคะแนน = ๑๗ – ๒๔
ระดับความเสี่ยงระดับสูงมาก มีคะแนน = ๒๕

เพื่อไม่เป็นภาระในการดำเนินการ การเตรียมการของผู้ดูแลระบบสารสนเทศ หรือมีการใช้งบประมาณดำเนินการเกินความจำเป็นในการวางแผนรองรับความเสี่ยง คณะจัดทำแผนบริหารความเสี่ยงพิจารณาว่าระดับความเสี่ยงที่จำเป็นให้ความสนใจและต้องบริหารจัดการความเสี่ยงของ ทสส.ทอ. คือ ความเสี่ยงที่มีค่าระดับความเสี่ยงตั้งแต่ ๑๒ ขึ้นไป ส่วนค่าความเสี่ยงในระดับที่ต่ำกว่าซึ่งผลกระทบไม่สูงมากนักให้ผู้ดูแลระบบสารสนเทศและผู้ใช้งานระบบสารสนเทศของหน่วย พิจารณาแก้ไขและดำเนินการตามความเหมาะสมของขีดความสามารถของบุคลากรในหน่วยงาน ทั้งนี้หากการดำเนินการใดที่หน่วยไม่สามารถดำเนินการเองได้ให้ประสานการปฏิบัติกับผู้รับผิดชอบระบบสารสนเทศของหน่วย

สำหรับความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร นำมาจัดเรียงลำดับความเสี่ยงและแนวทางบริหารจัดการความเสี่ยงฯ ดังนี้

ตารางที่ ๔ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ.

ลำดับ	ชื่อความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๑	RP02 ผู้ปฏิบัติงานนำอุปกรณ์คอมพิวเตอร์หรือ สมาร์ทดีไวซ์ (Smart Device) ส่วนตัวมาเชื่อมต่อเข้ากับระบบเครือข่ายของ ทสส.ทอ.	๒๐	จำกัดความเสี่ยง	- ตรวจสอบและลงทะเบียนอุปกรณ์ที่จะขอเชื่อมต่อเข้ามาในระบบสารสนเทศของ ทสส.ทอ.ว่ามีการป้องกันอย่างเพียงพอ และปราศจากโปรแกรมที่มีความเสี่ยง ก่อนอนุญาตให้เชื่อมต่อ - ติดตั้งระบบป้องกันโปรแกรมประสงค์ร้ายบนระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน - ประชาสัมพันธ์ให้ความรู้กับกำลังพลของ ทสส.ทอ. ให้เกิดความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์	- กทส.สนผ.ฯ - กทส.สนผ.ฯ - กคช.สบค.ฯ	- เมื่อมีการขออนุญาตนำอุปกรณ์มาใช้งานในระบบ - เป็นประจำอย่างต่อเนื่อง - เป็นประจำอย่างต่อเนื่อง

ลำดับ	ชื่อความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๒	RT03 เครือข่ายอินเทอร์เน็ตและเครือข่ายภายใน ทสส.ทอ.ไม่สามารถใช้งานได้	๑๕	จำกัดความเสี่ยง	- ตรวจสอบการตั้งค่าให้สอดคล้องกับ สอ.ทอ. - ตรวจสอบสภาพความพร้อมใช้งานอยู่เสมอ	- กทส.ฯ - นขต.ทสส.ทอ.	- เป็นประจำอย่างต่อเนื่อง
๓	RT04 เครื่องแม่ข่าย และเครื่องคอมพิวเตอร์ในเครือข่ายติดมัลแวร์ หรือไวรัสคอมพิวเตอร์โดยสาเหตุทางเทคนิค	๑๕	จำกัดความเสี่ยง	- ตรวจสอบประสิทธิภาพของโปรแกรมป้องกันไวรัสของเครื่องแม่ข่าย - คอมพิวเตอร์ทุกเครื่องใน ทสส.ทอ. ลงโปรแกรม AntiVirus ที่มีประสิทธิภาพ	- กทส.ฯ (ศคพ.สอ.ทอ.และ ศชบ.ทอ.) - นขต.ทสส.ทอ.	- เป็นประจำทุกเดือน - เปิดใช้ตลอดเวลาและ Update สม่ำเสมอ
๔	RP03 ผู้ใช้งานในระบบถูกหลอกให้เปิดเผยข้อมูลบัญชีรหัสผ่าน โดยการ Phishing หรือ ข้อมูลในระบบสารสนเทศถูกทำลาย แก้ไขเปลี่ยนแปลงหรือถูกโจรกรรมโดยผู้ไม่ประสงค์ดีจากการสมัครใจเข้าร่วมกิจกรรมผ่านโซเชียลมีเดีย	๑๕	จำกัดความเสี่ยง	- จัดทำระบบงานและสำรองข้อมูลให้ทำงานแทนเมื่อระบบหลักเกิดปัญหา (ระบบ Database Backup) - หน่วยงานมีผู้ดูแลระบบงานและข้อมูล - มีการจัดทำคู่มือ อบรมเพื่อให้ความรู้ด้านการดูแลรักษาความปลอดภัยของระบบงานและข้อมูลแก่ผู้ใช้ระบบ	- ตามแผนสำรองข้อมูล - นขต.ทสส.ทอ. - กทส.ฯ และ กคช.ฯ	- เป็นประจำตามแผนฯ - เป็นประจำอย่างต่อเนื่อง - เป็นประจำอย่างต่อเนื่อง
๕	RP04 ผู้ใช้งานดาวน์โหลดหรือนำซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์มาติดตั้งใช้งาน	๑๒	จำกัดความเสี่ยง	- มีมาตรการห้ามผู้ใช้งานดาวน์โหลดหรือนำซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์มาติดตั้งเพื่อใช้งาน - ฟรีแวร์ที่ต้องการใช้งานต้องผ่านการตรวจสอบความปลอดภัย - จัดทำโครงการจัดหาซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง	- คณก. ICT ทสส.ทอ. - นขต.ทสส.ทอ.	- ก.ย.๖๔ - เป็นประจำอย่างต่อเนื่อง
๖	RT02 ระบบจัดเก็บข้อมูลชำรุดหรือขัดข้องโดยสาเหตุทางเทคนิค	๑๐	จำกัดความเสี่ยง	- ตรวจสอบสภาพความพร้อมใช้งานของระบบอยู่เสมอ - ตรวจสอบความผิดปกติของโปรแกรมที่ใช้งาน ทรัพยากรของอุปกรณ์เครือข่าย และเครื่องแม่ข่ายจนทำให้ระบบขัดข้องหรือล้มเหลว - ปรับปรุงและซักซ้อมแผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ	- นขต.ทสส.ทอ.	- ตามแผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศ

ลำดับ	ชื่อความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๗	RT06 ข้อมูลในระบบสารสนเทศสูญหาย ถูกทำลาย หรือถูกแก้ไขเปลี่ยนแปลง	๑๐	จำกัดความเสี่ยง	- อัปเดตระบบปฏิบัติการและไดร์เวอร์อุปกรณ์ให้ทันสมัยอยู่เสมอ เพื่อปิดช่องโหว่ - สำรองข้อมูลในระบบสารสนเทศเป็นประจำตามวงรอบ - ปรับปรุงและซักซ้อมแผนการสำรองข้อมูลและฟื้นฟูระบบสารสนเทศเป็นประจำ	- กทส.ฯ (ศคพ.ฯ) - นขต.ทสส.ทอ.	- เป็นประจำอย่างต่อเนื่อง - เป็นประจำตามแผนฯ
๘	RP06 การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๘	จำกัดความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - กำหนดพื้นที่หวงห้ามในการเข้าถึงพื้นที่ปฏิบัติงาน - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ตรวจสอบระบบกล้องวงจรปิดให้สามารถบันทึกเหตุการณ์ได้ตลอดเวลา	- น.รปภ.ฯ	- เป็นประจำอย่างต่อเนื่อง
๙	RE01 ระบบสารสนเทศและทรัพย์สินเสียหายจากระบบไฟฟ้าขัดข้อง	๘	ยอมรับความเสี่ยง	- จัดหาเครื่องกำเนิดไฟฟ้าและเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่	- กนผ.ฯ และ กทส.ฯ	- ก.ย.๖๖
๑๐	RM03 ขาดอุปกรณ์สำรองไฟที่เพียงพอ	๘	ยอมรับความเสี่ยง	- วางแผนเสนอโครงการจัดหาอุปกรณ์สำรองไฟประจำอุปกรณ์ในระบบสารสนเทศที่สำคัญ	- กนผ.ฯ และ กทส.ฯ	- ก.ย.๖๕
๑๑	RM01 การขาดแคลนบุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๖	ยอมรับความเสี่ยง	- ส่งบุคลากรไปอบรมหรือศึกษาเพิ่มเติม - วางแผนการบรรจุบุคลากรที่มีความรู้ความสามารถ จัดทำ KM การจัดการความรู้ จัดทำมาตรฐานงาน	- กนผ.ฯ	- ก.ย.๖๕ - ก.ย.๖๖
๑๒	RT05 รางปลั๊กไม่ได้มาตรฐาน/กำลังไฟฟ้าที่ไม่รองรับหรือไม่เพียงพอต่อการใช้งาน	๖	ยอมรับความเสี่ยง	- ตรวจสอบสภาพรางปลั๊กที่ใช้ในปัจจุบันอย่างสม่ำเสมอ - จัดหารางปลั๊กที่มีความปลอดภัย	- นขต.ทสส.ทอ. - นพด.ผธก.ฯ	- สม่ำเสมอ - ก.ย.๖๕

ลำดับ	ชื่อความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๑๓	RP05 การเข้าถึงข้อมูลของบุคคลอื่น	๖	จำกัดความเสี่ยง	- สร้างความตระหนักในการรักษาข้อมูล/สิทธิส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติรักษาความมั่นคงปลอดภัยสารสนเทศ - กำหนดสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ อย่างเหมาะสม	- กคช.ฯ - นขต.ทสส.ทอ. - กทส.ฯ และ กบค.ฯ	- เป็นประจำอย่างต่อเนื่อง - เป็นประจำตามแผนฯ - เป็นประจำตามแผนฯ
๑๔	RM02 ข้อมูลสำคัญสูญหาย เมื่อเกิดเหตุขัดข้องในระบบ	๖	จำกัดความเสี่ยง	- จัดหาอุปกรณ์สำรองข้อมูลเพิ่มเติม - จัดทำคู่มือสำหรับผู้ใช้งาน - มีการสำรองข้อมูลอยู่เสมอเพื่อกู้คืนข้อมูล	- กทส.ฯ และ กนผ.ฯ - นขต.ทสส.ทอ. - นขต.ทสส.ทอ.	- ก.ย.๖๖ - เป็นประจำอย่างต่อเนื่อง - เป็นประจำตามแผนฯ
๑๕	RT01 อุปกรณ์เครือข่าย และเครื่องแม่ข่ายในระบบสารสนเทศชำรุด ขัดข้อง ไม่สามารถทำงานได้โดยสาเหตุทางเทคนิค	๕	หลีกเลี่ยงความเสี่ยง จำกัดความเสี่ยง	- แนะนำคุณลักษณะอุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐานให้กับ สอ.ทอ. - ตรวจสอบสภาพความพร้อมใช้งานของระบบอยู่เสมอ	- คณก.ICT ทสส.ทอ. - ตรวจสอบสภาพความพร้อมใช้งานของระบบอยู่เสมอ	- เมื่อมีการประชุมพิจารณา - เป็นประจำทุกเดือน
๑๖	RE02 การเกิดภัยพิบัติทางธรรมชาติ เช่น อุทกภัย แผ่นดินไหว อาคารถล่ม เป็นต้น	๕	ถ่ายโอนความเสี่ยง	- จัดหาพื้นที่ปฏิบัติงานสำรองนอกเขตภัยพิบัติและใช้ระบบสำรองข้อมูลระบบ - ปรับปรุง/ซักซ้อมแผนเผชิญเหตุจากภัยพิบัติฯ	- คณก. ICT ทสส.ทอ.	- ก.ย.๖๕ - เป็นประจำตามแผนฯ
๑๗	RE03 ระบบสารสนเทศและทรัพย์สินเสียหายจากอัคคีภัย	๕	จำกัดความเสี่ยง	- ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน - จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุอัคคีภัย - สำรองข้อมูลระบบและฐานข้อมูลไว้ที่อื่นอย่างน้อย ๑ ชุด	- น.นิรภัยฯ - นขต.ทสส.ทอ. - นขต.ทสส.ทอ.	- ก.ย.๖๔ - เป็นประจำอย่างต่อเนื่อง - เป็นประจำตามแผนฯ

ลำดับ	ชื่อความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
๑๘	RM04 ขาดมาตรการการควบคุมการเข้าถึงข้อมูลในระบบสารสนเทศที่ดี	๕	จำกัดความเสี่ยง	- มีมาตรการในการรักษาความปลอดภัยทางกายภาพ กำหนดพื้นที่หวงห้าม และกำหนดสิทธิ์ในการเข้าถึงสถานที่ติดตั้งอุปกรณ์ที่สำคัญทางสารสนเทศ - วางแผนกำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศ อุปกรณ์เครือข่าย และเครื่องแม่ข่าย	- น.รปภ.ฯ - กทส.ฯ กบค. และ กคช.ฯ	- ก.ย.๖๕ - เป็นประจำตามแผนฯ
๑๙	RP01 ผู้ปฏิบัติงานขาดความรู้ในการระบุและแก้ไขปัญหาที่เกิดขึ้นในระบบสารสนเทศ	๔	ยอมรับความเสี่ยง จำกัดความเสี่ยง	- ส่งข้าราชการที่บรรจุใหม่และผู้ที่เหมาะสม เข้ารับการอบรมในหลักสูตรที่เกี่ยวข้อง - จัดทำคู่มือการปฏิบัติงาน/ปรับปรุงให้ทันสมัย	- นขต.ทสส.ทอ. - นขต.ทสส.ทอ.	- เป็นประจำอย่างต่อเนื่อง - เป็นประจำอย่างต่อเนื่อง
๒๐	RE04 เกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๔	ยอมรับความเสี่ยง จำกัดความเสี่ยง	- จัดหาพื้นที่ปฏิบัติงานสำรองนอกหน่วยและใช้ระบบสำรองข้อมูล - ปรับปรุง/ซักซ้อมแผนเผชิญเหตุจากภัยพิบัติฯ	- นขต.ทสส.ทอ. - นขต.ทสส.ทอ.	- ก.ย.๖๕ - เป็นประจำตามแผนฯ

๑๐. บทสรุปแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ.

การบริหารจัดการความเสี่ยงเป็นการป้องกันและลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้นกับเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีความแตกต่างกันไปตามสภาพแวดล้อม ภารกิจ เทคโนโลยี และระบบสารสนเทศที่แต่ละหน่วยมีใช้งาน การระบุความเสี่ยง ผลกระทบและการพิจารณาแนวทางบริหารจัดการความเสี่ยงผู้รับผิดชอบระบบสารสนเทศของแต่ละหน่วยได้ร่วมระดมความคิดและพิจารณาจากประสบการณ์และปัญหาที่แต่ละหน่วยเผชิญ และได้รวบรวมความเสี่ยง ผลกระทบ แนวทางในการบรรเทาผลกระทบหรือป้องกันไว้ในแผนบริหารจัดการความเสี่ยงฯ นี้

แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทสส.ทอ.ฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ. เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อไป

พล.อ.ต.
(ธีระ เกาะประเสริฐ)
ประธานกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.
ก.ย.๖๔

บรรณานุกรม

กองทัพอากาศ. (๒๕๖๒). คู่มือการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กองทัพอากาศ พ.ศ.๒๕๖๒.: กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ.

กองทัพอากาศ. (๒๕๖๓). ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓.: กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ.

ภาคผนวก

คำสั่งแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.

คำสั่งแต่งตั้งนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทสส.ทอ.