บันทึกข้อความ

ส่วนราชการ ฝทสส.บก.บน.๑ (โทร.๔-๐๔๐๒)

ที่ กห ๐๖๑๖.๒(๗)/ ๒๖๐ **วันที่** ๙ ธ.ค.๖๘

เรื่อง ขออนุมัติแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร บน.๑ ประจำปี ๖๙

เรียน ผบ.บน.๑

๑. ตามคำสั่ง บน.๑ (เฉพาะ) ที่ ๕๒/๖๗ ลง ๓๐ ธ.ค.๖๗ เรื่อง แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ บน.๑ ให้คณะกรรมการฯ จัดทำแผนบริหารจัดการความเสี่ยงการดำเนินการเกี่ยวกับสารสนเทศและระบบสารสนเทศของ บน.๑ นั้น

๒. ฝทสส.บก.บน.๑ ตรวจสอบแล้ว คณะกรรมการฯ ได้ดำเนินการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร บน.๑ ประจำปี ๖๙ ตามคู่มือการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทอ. พ.ศ.๒๕๖๒ เรียบร้อยแล้ว

๓. ฝทสส.บก.บน.๑ พิจารณาแล้ว เพื่อให้การดำเนินการตามข้อ ๑ เป็นไปด้วยความเรียบร้อย เห็นควรอนุมัติแผนฯ ตามข้อ ๒ และให้ นขต.บน.๑ ประชาสัมพันธ์แผนฯ ให้กำลังพลในหน่วยทราบ เพื่อนำไปยึดถือปฏิบัติต่อไป พร้อมนี้ได้แนบแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร บน.๑ ประจำปี ๖๙ มาด้วยแล้ว

จึงเรียนมาเพื่อพิจารณา หากเห็นสมควรขอได้อนุมัติตามข้อ ๓

น.ต.
หน.ฝทสส.บก.บน.๑

เรียน ผบ.บน.๑

กระผมพิจารณาแล้ว เห็นสมควรอนุมัติตามข้อ ๓ ต่อไป

น.อ.
เสธ.บน.๑
๙ ธ.ค.๖๘

อนุมัติตามข้อ ๓

น.อ.
ผบ.บน.๑
๑๑ ธ.ค.๖๘

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร
กองบิน ๑

คำนำ

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กองบิน ๑ จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการจัดการและบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับป้องกันภัยคุกคามทางด้านระบบสารสนเทศและไซเบอร์ ที่มีแนวโน้มจะเกิดขึ้นกับหน่วยงานในอนาคต

กองบิน ๑ เป็นหน่วยขึ้นตรงกองทัพอากาศ มีภารกิจ เตรียมและปฏิบัติการใช้กำลังตามอำนาจหน้าที่ของกองทัพอากาศ ซึ่งกองบิน ๑ มีระบบสารสนเทศที่ใช้งาน ทั้งด้านการเตรียมกำลังและใช้กำลังทางอากาศ จึงจำเป็นต้องป้องกันภัยคุกคามรูปแบบต่าง ๆ รวมทั้งภัยคุกคามทางด้านไซเบอร์ อันจะส่งผลกระทบกับการใช้ข้อมูลและระบบสารสนเทศของหน่วย

การจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ กองบิน ๑ เป็นส่วนหนึ่งที่จะทำให้เกิดความชัดเจนในการเตรียมการบริหารจัดการกับความเสี่ยงที่อาจส่งผลกระทบกับระบบสารสนเทศของหน่วยงานได้อย่างถูกต้อง เหมาะสม เพื่อลดโอกาสหรือบรรเทาผลกระทบกับความเสี่ยงที่มีอยู่

คณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กองบิน ๑

ธันวาคม ๒๕๖๘

สารบัญ

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กองบิน ๑

๑. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญในการปฏิบัติงานของกองทัพอากาศ ซึ่งอาจกล่าวได้ว่าความสำเร็จของวิสัยทัศน์กองทัพอากาศในการเป็น “หนึ่งในกองทัพอากาศชั้นนำในภูมิภาค” (One of the best Air Forces in ASEAN) จะเกิดขึ้นได้ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร กองทัพอากาศ ต้องมั่นคงปลอดภัย (Security) พร้อมใช้งาน (Availability) และความถูกต้องสมบูรณ์ของข้อมูล (Integrity) การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้อง “ภารกิจ” ของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย

ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงานจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินภารกิจของหน่วยงานให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเพียงเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของหน่วยงาน ที่จะนำไปสู่การใช้ทรัพยากรอย่างประสิทธิภาพและคุ้มค่า

๒. วัตถุประสงค์

๒.๑ เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในหน่วยงานดำเนินการได้อย่างมีประสิทธิภาพ มีความยืดหยุ่นสามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ ภายใต้ข้อจำกัดที่บุคลากรด้านเทคโนโลยีสารสนเทศของหน่วยงานที่มีจำนวนจำกัด และลดโอกาสในการเกิดความเสียหาย หรือความผิดพลาดกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วย

๒.๒ เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ภัยคุกคาม ความผิดพลาด ความไม่พร้อมใช้งานหรือเหตุที่ไม่พึงประสงค์ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒.๓ เพื่อให้มีการวางแผนการปฏิบัติการควบคุม และกำหนดแนวทางแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๔ เพื่อเป็นแนวทางการดำเนินการ การกำกับดูแล การตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๕ เพื่อเพิ่มประสิทธิภาพในการพิจารณาดำเนินการของผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วย โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่อาจส่งผลกระทบกับการดำเนินงานตามวัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น ก่อนตัดสินใจในการดำเนินการหรือปฏิบัติตามแผนอย่างใดอย่างหนึ่ง

๓. ขอบเขตการดำเนินการ

เป็นแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในหน่วยงาน โดยกำหนดแนวทางปฏิบัติให้กับผู้รับผิดชอบระบบสารสนเทศและการสื่อสาร รวมทั้งบุคลากร คอมพิวเตอร์ และอุปกรณ์เครือข่าย พร้อมกับการเสริมสร้างจิตสำนึกและความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

โดยมีคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กองบิน ๑ เป็นผู้รับผิดชอบหลักในการกำหนดแผนบริหารจัดการความเสี่ยง

๔. การวิเคราะห์ความเสี่ยง

๔.๑ การจำแนกประเภทความเสี่ยง

ทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำแนกตามองค์ประกอบของระบบสารสนเทศ สามารถแบ่งออกเป็น ๕ ประเภท ดังนี้

๔.๑.๑ ระบบงาน (Application System) ได้แก่ ขั้นตอนและกระบวนการปฏิบัติงาน

๔.๑.๒ เทคโนโลยี (Technology) ได้แก่ เครื่องคอมพิวเตอร์ (Hardware) โปรแกรมระบบปฏิบัติการ (Operating System) ระบบบริหารฐานข้อมูล (Database Management System) ระบบเครือข่าย (Network) และระบบมัลติมีเดีย

๔.๑.๓ องค์ประกอบ (Facilities) ได้แก่ ทรัพยากรต่าง ๆ ที่ใช้เป็นสถานที่ติดตั้งหรือจัดวาง ตลอดจนสาธารณูปโภคที่จำเป็นเพื่อการปฏิบัติงานของระบบสารสนเทศ

๔.๑.๔ บุคลากร (People) ได้แก่ บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงาน สำหรับการดูแลและจัดระบบ รวมถึงผู้ปฏิบัติงานทั่วไป

๔.๑.๕ ข้อมูล (Data) ได้แก่ ข้อมูลในรูปแบบต่าง ๆ ทั้งที่มีโครงสร้างและไม่มีโครงสร้าง

๔.๒ การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสาร สามารถแยกประเภทความเสี่ยงออกได้เป็น ๔ ด้าน ดังนี้

๔.๒.๑ ความเสี่ยงด้านเทคนิค (Risk of Technical Operation: RT) เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี (Malware) ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Hacker เป็นต้น

๔.๒.๒ ความเสี่ยงด้านการบริหารจัดการ (Risk of Management: RM) เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๔.๒.๓ ความเสี่ยงจากผู้ปฏิบัติงาน (Risk of Personnel: RP) เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๔.๒.๔ ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (Risk of Natural Disasters and Emergency Situations: RE) เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วมไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๕. การประมาณการความเสี่ยง

การประเมินโอกาสหรือความน่าจะเป็นของเหตุการณ์ที่อาจเกิดขึ้น (Probability or Likelihood) กับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วย ตามแผนบริหารจัดการความเสี่ยงฯ นี้ พิจารณาแบ่งความถี่ของโอกาสหรือความน่าจะเป็นของเหตุการณ์ที่อาจเกิดขึ้นเป็น ๕ ระดับจากน้อยไปหามาก ดังนี้

ระดับ	โอกาสที่เกิดขึ้น
๑	แทบไม่เกิดขึ้นเลย (Improbable)
๒	น้อยครั้งมาก (Remote)
๓	ตามโอกาส (Occasional)
๔	ประปราย (Probable)
๕	เกิดขึ้นบ่อย (Frequent)

การประเมินผลกระทบหรือความรุนแรงของเหตุการณ์ (Severity of consequence) แบ่งระดับผลกระทบหรือความรุนแรงเป็น ๕ ระดับจากน้อยไปหามาก ดังนี้

ระดับ	ผลกระทบ/ความรุนแรง
๑	น้อยมาก - เกิดเหตุร้ายที่ไม่มีความสำคัญ
๒	น้อย - เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๓	ปานกลาง - ระบบมีปัญหาและมีความสูญเสียไม่มาก
๔	สูง - เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๕	สูงมาก - เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ

ค่าความเสี่ยง = โอกาสที่จะเกิดขึ้นของเหตุการณ์ X ผลกระทบความรุนแรงของเหตุการณ์

๖. ลักษณะและรายละเอียดของความเสี่ยง

ลักษณะและรายละเอียดของความเสี่ยง (Description of risk) ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยที่ได้จากการร่วมกันวิเคราะห์ และระดมความคิดของผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศ รวมถึงเหตุการณ์ที่หน่วยเผชิญ (ตามแนวทางการการระบุความเสี่ยง) แสดงตามตาราง

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RT01	อุปกรณ์สารสนเทศขัดข้อง	อุปกรณ์ในระบบเครือข่ายไม่สามารถให้บริการระบบสารสนเทศหรือให้บริการได้ไม่เต็มประสิทธิภาพ	ฮาร์ดแวร์ขัดข้อง / ไม่ได้มาตรฐาน / เสื่อมสภาพตามอายุการใช้งาน	เครื่องคอมพิวเตอร์ลูกข่ายไม่สามารถใช้บริการระบบสารสนเทศ หรือเรียกใช้ทรัพยากรที่เครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ ไม่ได้	๓	๔	๑๒
RT02	เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ขัดข้อง	เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ไม่สามารถใช้งานระบบสารสนเทศหรือใช้งานได้ไม่เต็มประสิทธิภาพ	- ประสิทธิภาพของฮาร์ดแวร์ไม่เพียงพอ - ระบบปฏิบัติการขัดข้อง - การถูกโจมตีจากภัยคุกคามทางไซเบอร์ เช่น ติด Malware, Botnet, Phishing เป็นต้น	- เครื่องคอมพิวเตอร์ลูกข่ายขาดประสิทธิภาพในการทำงานและเกิดความเสียหาย - ข้อมูล / ระบบสารสนเทศเกิดความเสียหาย	๔	๔	๑๖

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RT03	เครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง	เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการระบบสารสนเทศ หรือให้บริการได้ไม่เต็มประสิทธิภาพ	- ประสิทธิภาพของฮาร์ดแวร์ไม่เพียงพอ - ระบบปฏิบัติการ ขัดข้อง - โปรแกรมบางตัวรบกวนการทำงานของ ระบบปฏิบัติการ - การถูกโจมตีจากภัยคุกคามทางไซเบอร์ เช่น DDoS, ติด Malware, Brute Force เป็นต้น	- เครื่องลูกข่ายไม่สามารถใช้บริการระบบสารสนเทศหรือเรียกใช้ทรัพยากรที่เครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ ไม่ได้ - ข้อมูล / ระบบสารสนเทศเกิดความเสียหาย	๓	๔	๑๒
RT04	ระบบการทำงานของซอฟต์แวร์ขัดข้องจากช่องโหว่จุดอ่อนที่ไม่เคยถูกพบมาก่อน (Zero Day)	ช่องโหว่จุดอ่อนของซอฟต์แวร์ที่ยังไม่ถูกค้นพบ เมื่อถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ต่างๆ ทำให้ระบบทำงานผิดพลาด	- การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ - ช่องโหว่จุดอ่อนของซอฟต์แวร์ที่ยังไม่ถูกค้นพบ (Zero Day)	เครื่องลูกข่ายไม่สามารถใช้บริการระบบสารสนเทศหรือเรียกใช้ทรัพยากรที่เครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ ไม่ได้	๔	๔	๑๖

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RM01	การขาดแคลนบุคลากรผู้ปฏิบัติงาน	ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีจำนวนไม่เพียงพอที่จะสนับสนุนภาระงานที่มีอยู่	- การไม่ได้รับการบรรจุตามความต้องการกำลังพล - การโยกย้ายบุคลากรด้านสารสนเทศ	- การปฏิบัติงานด้านเทคโนโลยีสารสนเทศล่าช้า/หยุดชะงัก - กระทบต่อการพัฒนาและควบคุมดูแลระบบ	๔	๒	๘
RM02	การแก้ไขปัญหาทางระบบสารสนเทศเกิดความล่าช้า	ผู้ที่ปฏิบัติงานในตำแหน่งที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีความรู้ไม่เพียงพอในการปฏิบัติงาน	- การบรรจุบุคลากรไม่ตรงตามวุฒิการศึกษา - บุคลากรไม่ได้รับการอบรมเกี่ยวกับระบบที่ดูแลที่เพียงพอ	- การปฏิบัติงานที่ต้องอาศัยระบบสารสนเทศเกิดความล่าช้า - ระบบสารสนเทศเกิดความเสียหาย	๓	๒	๖
RM03	อุปกรณ์ในระบบสารสนเทศ ไม่ทันสมัย และเสื่อมสภาพ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ	งบประมาณที่ได้รับไม่ครอบคลุมความต้องการ	ระบบสารสนเทศที่สนับสนุนการปฏิบัติงานหยุดชะงักและขาดประสิทธิภาพ	๓	๒	๖

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RM04	การเปลี่ยนแปลงนโยบายของผู้บังคับบัญชา	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- นโยบายของผู้บังคับบัญชาไม่สอดคล้องกัน - ขาดความต่อเนื่องในการสานต่อโครงการต่าง ๆ	การดำเนินงานขาดความต่อเนื่อง	๓	๔	๑๒
RM05	ข้อมูลสำคัญถูกโจรกรรม	บุคคลจากภายนอกหน่วย หรือจากภายนอก บน.๑ เข้ามาในพื้นที่ปฏิบัติงาน เพื่อกระทำการอันตรายใดๆ ต่อระบบสารสนเทศ	- ขาดมาตรการรักษาความปลอดภัยในการเข้าพื้นที่ - ผู้ไม่ประสงค์ดีที่แฝงตัวมากับบุคคล ภายนอกหน่วย หรือจากภายนอก บน.๑	- ระบบสารสนเทศเกิดความเสียหาย - ข้อมูลสำคัญโดยเฉพาะข้อมูลที่มีชั้นความลับถูกเปิดเผย	๑	๕	๕

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RP01	การละเมิดสิทธิ์เข้าถึงข้อมูลส่วนบุคคล	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือการละเลยไม่ log out ออกจากระบบหลังเลิกใช้งาน ทำให้ผู้ไม่มีสิทธิ์สามารถเข้าใช้งานระบบสารสนเทศได้	- บุคลากรที่ขาดความเข้าใจเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ - ถูก Phishing เมื่อลงชื่อเข้าใช้งานบนเว็บไซต์ปลอม - ถูกโปรแกรม Key logger ขโมยชื่อผู้ใช้และรหัสผ่าน	- ระบบสารสนเทศเกิดความเสียหาย - ข้อมูลส่วนบุคคลสูญหาย หรือถูกเปิดเผย	๓	๓	๙
RP02	ช่องโหว่จากการนำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ที่ไม่ได้รับอนุญาตมาเชื่อมต่อเข้าเครือข่าย	ผู้ใช้นำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) มาเชื่อมต่อโดยไม่ได้รับอนุญาตหรือแจ้งให้ผู้ดูแลระบบทราบ	- บุคลากรของ บน.๑ ที่ขาดความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ - ขาดมาตรการในการจำกัดการเข้าใช้งานเครือข่าย	ระบบสารสนเทศเกิดความเสียหาย	๓	๔	๑๒

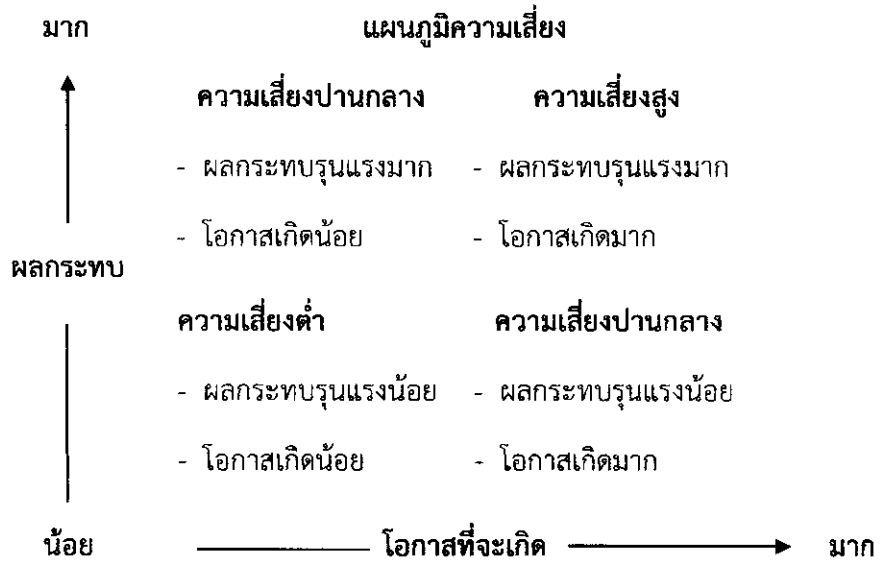
รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RP03	ระบบงานเสียหายจากความผิดพลาดของผู้ปฏิบัติงาน	บุคลากรที่ใช้งานระบบสารสนเทศปฏิบัติผิดพลาด เช่น เผลอลบข้อมูลที่สำคัญในระบบ ตั้งค่าระบบผิดพลาด กรอกข้อมูลผิด หรือแก้ไขโค้ดโปรแกรมผิดพลาด ทำให้ระบบสารสนเทศทำงานผิดพลาดหรือไม่สามารถทำงานได้	- บุคลากรขาดความรู้ในการใช้งานระบบสารสนเทศ - ขาดความรอบคอบในการปฏิบัติงาน - อุบัติเหตุจากการรู้เท่าไม่ถึงการณ์ ประมาท	ระบบสารสนเทศที่สนับสนุนการปฏิบัติงานหยุดชะงักและเกิดความเสียหาย	๓	๒	๖
RP04	ข้อมูลที่มีผลกระทบต่อองค์กร และด้านยุทธการรั่วไหล ผ่านทางระบบสารสนเทศ	มีการเผยแพร่ข้อมูลสำคัญของทางราชการ ที่มีผลต่อการปฏิบัติด้านยุทธการ และความมั่นคง	บุคลากรของ บน.๑ ที่ขาดความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศเบื้องต้น	ข้อมูลสำคัญโดยเฉพาะข้อมูลที่มีชั้นความลับถูกเปิดเผย และกระทบต่อความมั่นคง	๑	๕	๕

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RE01	กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	การเกิดกระแสไฟฟ้าขัดข้องแบบกะทันหัน เช่น ไฟฟ้าดับ-กระชากที่มีสาเหตุจากภัยธรรมชาติหรือจากการขัดข้องของอุปกรณ์ในระบบไฟฟ้า	- แหล่งกำเนิดไฟฟ้าขัดข้อง - ภัยธรรมชาติที่ส่งผลให้แหล่งกำเนิดไฟฟ้าขัดข้อง	อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เชื่อมต่อเครือข่ายได้รับความเสียหาย	๕	๔	๒๐
RE02	เครือข่ายภายใน บน.๑ ไม่สามารถใช้งานได้	ไม่สามารถใช้งานระบบเครือข่าย ที่ให้บริการผ่านอุปกรณ์เครือข่ายของ บน.๑ ได้	- เครือข่ายผู้ให้บริการภายนอกขัดข้อง - เครือข่าย ทอ. ขัดข้อง - การถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ เช่น DDoS (DDos : Distributed Denial of-Service)	- ไม่สามารถใช้บริการระบบสารสนเทศ ผ่านเครือข่ายได้ - การปฏิบัติงานที่ต้องอาศัยระบบสารสนเทศ ผ่านเครือข่ายต้องหยุดชะงัก - ข้อมูลสำคัญที่เก็บไว้บนระบบคลาวด์ (Cloud Storage) อาจสูญหาย	๓	๔	๑๒

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
RE03	อัคคีภัย	เหตุการณ์อัคคีภัยในอาคารที่ลุกลามสร้างความเสียหายให้กับอุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เชื่อมต่อเครือข่าย	- อัคคีภัยจากกระแสไฟฟ้าขัดข้อง - อัคคีภัยจากอุบัติเหตุการใช้อุปกรณ์ไฟฟ้า	อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เชื่อมต่อเครือข่ายเสียหาย	๒	๕	๑๐

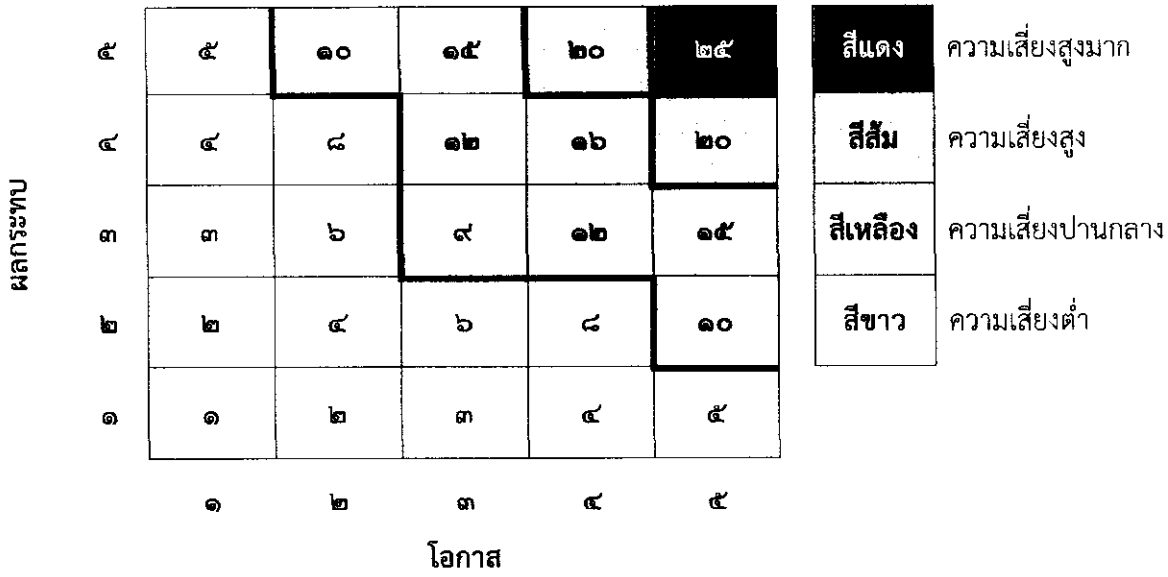
๗. การประเมินค่าความเสี่ยง

พิจารณาจากปัจจัยของโอกาสหรือความน่าจะเป็นของเหตุการณ์ (Probability or Likelihood) กับระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วย รวมถึงประสิทธิภาพของแผนการควบคุมความปลอดภัย การวัดระดับความเสี่ยงพิจารณาจากแผนภูมิความเสี่ยงกับผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้



เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก, สูง, ปานกลาง และต่ำ

การแบ่งพื้นที่ระดับความเสี่ยง



จากผลการระบุความเสี่ยง ร่วมกันวิเคราะห์และประเมินความเสี่ยงโดยผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศ สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของกองบิน ๑ (จากมากไปน้อย) เพื่อใช้ในการบริหารจัดการได้ ดังนี้

ลำดับ	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
๑	RE01 กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ตามตาราง ลักษณะและรายละเอียดของความเสี่ยง (ในข้อ ๖)			๕	๔	๒๐
๒	RT04 ระบบการทำงานของซอฟต์แวร์ขัดข้องจากช่องโหว่จุดอ่อนที่ไม่เคยถูกพบมาก่อน (Zero Day)				๔	๔	๑๖
๓	RT02 เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ขัดข้อง				๔	๔	๑๖

ลำดับ	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ (อธิบาย)	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส (๑-๕)	ผลกระทบ (๑-๕)	ค่าความเสี่ยง (๑-๒๕)
๔	RT01 อุปกรณ์สารสนเทศขัดข้อง	ตามตาราง ลักษณะและรายละเอียดของความเสี่ยง (ในข้อ ๖)			๓	๔	๑๒
๕	RT03 เครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง				๓	๔	๑๒
๖	RM04 การเปลี่ยนแปลงนโยบายของผู้บังคับบัญชา				๓	๔	๑๒
๗	RP02 ช่องโหว่จากการนำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ที่ไม่ได้รับอนุญาตมาเชื่อมต่อเข้าเครือข่าย				๓	๔	๑๒
๘	RE02 เครือข่ายภายใน บน.๑ ไม่สามารถใช้งานได้				๓	๔	๑๒
๙	RE03 อัคคีภัย				๒	๕	๑๐
๑๐	RP01 การละเมิดสิทธิ์เข้าถึงข้อมูลส่วนบุคคล				๓	๓	๙
๑๑	RM01 การขาดแคลนบุคลากรผู้ปฏิบัติงาน				๔	๒	๘
๑๒	RM02 การแก้ไขปัญหาทางระบบสารสนเทศเกิดความล่าช้า				๓	๒	๖
๑๓	RM03 อุปกรณ์ในระบบสารสนเทศ ไม่ทันสมัยและเสื่อมสภาพ				๓	๒	๖
๑๔	RP03 ระบบงานเสียหายจากความผิดพลาดของผู้ปฏิบัติงาน				๓	๒	๖
๑๕	RM05 ข้อมูลสำคัญถูกโจรกรรม				๑	๕	๕
๑๖	RP04 ข้อมูลที่มีผลกระทบต่อองค์กร และด้านยุทธการ รั่วไหล ผ่านทางระบบสารสนเทศ				๑	๕	๕

๘. การบรรเทาความเสี่ยง

ทางเลือกเพื่อการบรรเทาความเสี่ยง สามารถแบ่งออกเป็น ๔ ประเภท ดังนี้

๘.๑ การยอมรับความเสี่ยง (Risk Acceptance) คือ การยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบข้อมูลสารสนเทศดำเนินงานไปตามปกติซึ่งเป็นการยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวตนเพียงใช้ชื่อผู้ใช้งานและรหัสผ่าน มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้การใช้ Biometrics เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า หน่วยงานอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปและปรับปรุงเมื่อมีโอกาส

๘.๒ การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยงด้วยการกำจัดสาเหตุของความเสี่ยง เช่น เมื่อพบว่าปัจจุบันหน่วยงาน มีการสำรองข้อมูลเพียง ๑ ชุด และจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้ อาจได้แก่ การทำสำรองข้อมูล ๒ ชุด และแยกเก็บในสถานที่ต่างกันหรือระบบงานที่มีความละเอียดอ่อนหรือเป็นความลับ ต้องห้ามมีการเชื่อมต่อกับอินเทอร์เน็ต เพื่อหลีกเลี่ยงภัยจาก Hacker เป็นต้น

๘.๓ การจำกัดความเสี่ยง (Risk Limitation) คือ การทำระบบควบคุม เพื่อให้เกิดผลกระทบจากการถูกคุกคามระบบ หรือจากความไม่มั่นคงของระบบให้น้อยที่สุด เช่น การใช้ Firewall ป้องกันระบบจากภัยคุกคามในอินเทอร์เน็ต

๘.๔ การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การถ่ายโอนความเสี่ยงด้วยการหาทางเลือกอื่นเพื่อชดเชยความสูญเสีย เช่น อุปกรณ์เครือข่าย เมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน หน่วยงานอาจเลือกซื้อประกัน หรือสัญญาการซ่อมบำรุง เป็นต้น

กองบิน ๑ กำหนดกลยุทธ์ในการบรรเทาความเสี่ยงต่อความเสี่ยงที่เกิดขึ้นตามค่าความเสี่ยงที่ได้จากการประเมิน ดังนี้

ผลคะแนนความเสี่ยง	ระดับความเสี่ยง	กลยุทธ์ในการบรรเทาความเสี่ยง	พื้นที่สี
๑ - ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙ - ๑๖	ปานกลาง	หลีกเลี่ยงความเสี่ยง	เหลือง
๑๗ - ๒๔	สูง	จำกัดความเสี่ยง	ส้ม
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

๙. การจัดการความเสี่ยง

เพื่อไม่เป็นภาระในการดำเนินการ การเตรียมการของผู้ดูแลระบบสารสนเทศ หรือมีการใช้งบประมาณดำเนินการเกินความจำเป็นในการวางแผนรองรับความเสี่ยง คณะจัดทำแผนบริหารความเสี่ยงพิจารณาว่าระดับความเสี่ยงที่จำเป็นให้ความสนใจและต้องบริหารจัดการความเสี่ยงของกองบิน ๑ คือ ความเสี่ยงที่มีค่าระดับความเสี่ยงตั้งแต่ ๑๒ ขึ้นไป ส่วนความเสี่ยงในระดับที่ต่ำกว่า ซึ่งผลกระทบไม่สูงมากนัก ให้ผู้ดูแลระบบสารสนเทศของหน่วย และผู้ใช้งานระบบสารสนเทศพิจารณาแก้ไข และพิจารณาดำเนินการตามความเหมาะสมของ

ขีดความสามารถของบุคลากรในหน่วยงาน ทั้งนี้หากการดำเนินการใดที่หน่วยไม่สามารถดำเนินการได้เอง ให้ประสานการปฏิบัติกับผู้รับผิดชอบระบบสารสนเทศของกองบิน ๑

สำหรับความเสี่ยงที่เกิดขึ้นในกองบิน ๑ มีการจัดเรียงลำดับความเสี่ยงเทียบกับการแบ่งพื้นที่ระดับความเสี่ยง พร้อมทั้งพิจารณามาตรการจัดการความเสี่ยงที่จะใช้ (ได้แก่ ยอมรับความเสี่ยง หลีกเลี่ยงความเสี่ยง จำกัดความเสี่ยง และถ่ายโอนความเสี่ยง) รวมถึงแนวทางการดำเนินการ และระบุถึงผู้รับผิดชอบกับระยะเวลา ดังแสดงในตาราง

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๑	RE01	กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	สูง ๕x๔=๒๐	จำกัดความเสี่ยง	- จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัด จนท.ตรวจสอบตามระยะเวลา	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ - ผชย.ฯ	โครงการพัฒนาประจำปี
๒	RT04	ระบบการทำงานของซอฟต์แวร์ขัดข้องจากช่องโหว่จุดอ่อนที่ไม่เคยถูกพบมาก่อน (Zero Day)	ปานกลาง ๔x๔=๑๖	หลีกเลี่ยงความเสี่ยง	ประสาน ทสส.ทอ.จัดหาซอฟต์แวร์ที่มีลิขสิทธิ์และการอัพเดทการสนับสนุนด้านป้องกันช่องโหว่ จากเจ้าของผลิตภัณฑ์	- ฝทสส.ฯ	ตลอดเวลา
๓	RT02	เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ขัดข้อง	ปานกลาง ๔x๔=๑๖	หลีกเลี่ยงความเสี่ยง	- จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ทดแทน เพื่อให้สามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๔	RT01	อุปกรณ์สารสนเทศขัดข้อง	ปานกลาง ๓x๔=๑๒	หลีกเลี่ยงความเสี่ยง	- จัดหาอุปกรณ์สารสนเทศทดแทนเพื่อให้สามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาอุปกรณ์สารสนเทศอย่างสม่ำเสมอ	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	ตามวงรอบ
๕	RT03	เครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง	ปานกลาง ๓x๔=๑๒	หลีกเลี่ยงความเสี่ยง	- จัดหาเครื่องคอมพิวเตอร์แม่ข่ายทดแทน เพื่อให้สามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	ตามวงรอบ
๖	RM04	การเปลี่ยนแปลงนโยบายของผู้บังคับบัญชา	ปานกลาง ๓x๔=๑๒	หลีกเลี่ยงความเสี่ยง	จัดทำแผนแม่บทการพัฒนาระบบ เพื่อเป็นกรอบแนวทางการพัฒนาให้ผู้บังคับบัญชาใช้เป็นข้อมูลในการพัฒนาระบบในอนาคต	- คณก.บริหารเทคโนโลยีสารสนเทศฯ	ปีละ ๑ ครั้ง

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๗	RP02	ช่องโหว่จากการนำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ที่ไม่ได้รับอนุญาตมาเชื่อมต่อเข้าเครือข่าย	ปานกลาง ๓x๔=๑๒	หลีกเลี่ยงความเสี่ยง	- จัดฝึกอบรมเพื่อสร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศ อย่างจริงจัง - ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ส่วนบุคคลที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	- คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	ตามวงรอบ
๘	RE02	เครือข่ายภายใน บน.๑ ไม่สามารถใช้งานได้	ปานกลาง ๓x๔=๑๒	หลีกเลี่ยงความเสี่ยง	- จัดหาเครือข่ายสำรองและติดตั้งอุปกรณ์สำรองต่าง ๆ ให้ครบถ้วน - จัดทำแผนเครือข่ายสำรอง	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	โครงการพัฒนาประจำปี
๙	RE03	อัคคีภัย	ปานกลาง ๒x๕=๑๐	หลีกเลี่ยงความเสี่ยง	- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่น อีกหนึ่งชุด	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	- โครงการพัฒนาประจำปี - ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๑๐	RP01	การละเมิดสิทธิ์เข้าถึงข้อมูลส่วนบุคคล	ปานกลาง ๓x๓=๙	หลีกเลี่ยงความเสี่ยง	- สร้างความตระหนักเรื่อง ข้อมูลส่วนบุคคลในการพึงรักษาสิทธิ์ส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	- คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศฯ - นขต.บน.๑	ตามวงรอบ
๑๑	RM01	การขาดแคลนบุคลากรผู้ปฏิบัติงาน	ต่ำ ๔x๒=๘	ยอมรับความเสี่ยง	- จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบ ไม่สามารถมาปฏิบัติงานได้	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - นขต.บน.๑	ตามวงรอบ
๑๒	RM02	การแก้ไขปัญหาทางระบบสารสนเทศเกิดความล่าช้า	ต่ำ ๓x๒=๖	ยอมรับความเสี่ยง	- จัดส่งเจ้าหน้าที่เข้ารับการอบรม เพื่อให้มีความรู้เพิ่มเติม - แจ้งข้อขัดข้องในการบรรจุกำลังพลให้สายวิทยาการรับทราบ เพื่อกำหนดคุณสมบัติของเจ้าหน้าที่ให้เหมาะสม	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - นขต.บน.๑	ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๑๓	RM03	อุปกรณ์ในระบบสารสนเทศ ไม่ทันสมัย และเสื่อมสภาพ	ต่ำ ๓x๒=๖	ยอมรับความเสี่ยง	จัดทำโครงการเพื่อขอรับการสนับสนุนอย่างต่อเนื่อง	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ	โครงการพัฒนาประจำปี
๑๔	RP03	ระบบงานเสียหายจากความผิดพลาดของผู้ปฏิบัติงาน	ต่ำ ๓x๒=๖	ยอมรับความเสี่ยง	- จัดอบรมและทบทวนการปฏิบัติให้เจ้าหน้าที่อย่างสม่ำเสมอ - สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่น อีกหนึ่งชุด	- คณก.บริหารเทคโนโลยีสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ - นขต.บน.๑	ตามวงรอบ
๑๕	RM05	ข้อมูลสำคัญถูกโจรกรรม	ต่ำ ๑x๕=๕	ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - กำหนดพื้นที่หวงห้ามในการเข้าถึงพื้นที่ปฏิบัติงาน	- คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศฯ - ฝทสส.ฯ - ผสอ.ฯ - ผขว.ฯ	ตามวงรอบ
๑๖	RP04	ข้อมูลที่มีผลกระทบต่อองค์กร และด้านยุทธการ รั่วไหลผ่านทางระบบสารสนเทศ	ต่ำ ๑x๕=๕	ยอมรับความเสี่ยง	- จัดฝึกอบรมเพื่อสร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศ อย่างจริงจัง	- คณก.รักษาความมั่นคงปลอดภัยระบบสารสนเทศฯ - นขต.บน.๑	ตามวงรอบ

๑๐. บทสรุปแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กองบิน ๑

การบริหารจัดการความเสี่ยงเป็นการป้องกันหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร และมีความแตกต่างกันไปตามสภาพแวดล้อม ภารกิจ เทคโนโลยี และระบบสารสนเทศที่แต่ละหน่วยมีใช้งาน การระบุความเสี่ยง ผลกระทบและการพิจารณาแนวทางบริหารจัดการความเสี่ยง ผู้รับผิดชอบระบบสารสนเทศของแต่ละหน่วยได้ร่วมระดมความคิดและพิจารณาจากประสบการณ์และปัญหาที่แต่ละหน่วยเผชิญ และได้รวบรวมความเสี่ยง ผลกระทบ แนวทางในการบรรเทาผลกระทบหรือป้องกันไว้ในแผนบริหารจัดการความเสี่ยงนี้

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กองบิน ๑ เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อไป

(ลงชื่อ) น.อ.
(เบญจพล เขียวชอุ่ม)
ประธานกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
ชื่อหน่วยงาน กองบิน ๑
ธ.ค.๖๘

อนุมัติ

น.อ.
(พิชญาณ อะสีติรัตน์)
ผบ.บน.๑
๑๑ ธ.ค.๖๘