แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กองบิน ๑

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร กองบิน ๑

๑. หลักการและเหตุผล

การบริหารความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้อง “ภารกิจ” ของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย ขั้นตอนในการบริหารความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงาน

หน่วยงานจะต้องมีกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินภารกิจของหน่วยงานให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเพียงเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของหน่วยงาน ที่จะนำไปสู่การใช้ทรัพยากรอย่างประสิทธิภาพและคุ้มค่า

๒. วัตถุประสงค์

๒.๑ เพื่อให้การจัดการภายในหน่วยงาน มีประสิทธิภาพและมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

๒.๒ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของหน่วยงาน

๒.๓ เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๒.๔ เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๕ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

๓. ขอบเขตการดำเนินการ

เป็นการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของหน่วยงาน

๔. การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของหน่วยงาน สามารถแยกประเภทความเสี่ยงเป็น ๔ ประเภท ดังนี้

๔.๑ ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ อาจถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๔.๒ ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๔.๓. ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๔.๔ ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๕. ลักษณะรายละเอียดของความเสี่ยง (Description of risk) แสดงตามตาราง

รายการความเสี่ยงด้านเทคนิค (RT)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RT01	อุปกรณ์สารสนเทศขัดข้อง	อุปกรณ์ในระบบเครือข่ายไม่สามารถให้บริการระบบสารสนเทศ หรือให้บริการได้ไม่เต็มประสิทธิภาพ	ฮาร์ดแวร์ขัดข้อง / ไม่ได้มาตรฐาน	เครื่องคอมพิวเตอร์ลูกข่ายไม่สามารถใช้บริการระบบสารสนเทศ หรือทรัพยากรที่เครื่องคอมพิวเตอร์แม่ข่ายนั้น ๆ ให้บริการได้	๓	๔	๑๒

รายการความเสี่ยงด้านเทคนิค (RT)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RT02	เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ขัดข้อง	เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ไม่สามารถใช้งานระบบสารสนเทศหรือใช้งานได้ไม่เต็มประสิทธิภาพ	- ประสิทธิภาพของฮาร์ดแวร์ไม่เพียงพอ - ระบบปฏิบัติการขัดข้อง - ถูกโจมตีโดยโปรแกรมประสงค์ร้าย เช่น ไวรัส โทรจัน โปรแกรมเรียกค่าไถ่ ฯลฯ	- เครื่องคอมพิวเตอร์ลูกข่ายขาดประสิทธิภาพในการทำงานและเกิดความเสียหาย - ระบบสารสนเทศเกิดความเสียหาย	๔	๔	๑๖
RT03	เครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง	เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถให้บริการระบบสารสนเทศ หรือให้บริการได้ไม่เต็มประสิทธิภาพ	- ประสิทธิภาพของฮาร์ดแวร์ไม่เพียงพอ - ระบบปฏิบัติการขัดข้อง - โปรแกรมบางตัวรบกวนการทำงานของ ระบบปฏิบัติการ - ถูกโจมตีโดยโปรแกรมประสงค์ร้าย เช่น ไวรัส โทรจัน โปรแกรมเรียกค่าไถ่ ฯลฯ	- เครื่องลูกข่ายไม่สามารถใช้บริการระบบสารสนเทศหรือทรัพยากรที่เครื่องแม่ข่ายนั้นๆ ให้บริการไม่ได้ - ระบบสารสนเทศเกิดความเสียหาย	๓	๔	๑๒

รายการความเสี่ยงด้านเทคนิค (RT)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RT04	ระบบการทำงานของซอฟแวร์ขัดข้องจากช่องโหว่จุดอ่อนที่ไม่เคยถูกพบมาก่อน (Zero Day)	ช่องโหว่จุดอ่อนของซอฟแวร์ที่ยังไม่ถูกค้นพบ เมื่อเกิดปัญหาจากการบุกรุกโดยแฮคเกอร์หรือโปรแกรมประสงค์ร้ายต่าง ๆ ทำให้ระบบทำงานผิดพลาด	- การใช้ซอฟแวร์ที่ไม่มีลิขสิทธิ์ - ช่องโหว่จุดอ่อนของซอฟแวร์ที่ยังไม่ถูกค้นพบ (Zero Day)	เครื่องลูกข่ายไม่สามารถใช้บริการระบบสารสนเทศ หรือทรัพยากรที่เครื่องแม่ข่ายนั้น ๆ ให้บริการไม่ได้	๔	๔	๑๖

รายการความเสี่ยงด้านการบริหารจัดการ (RM)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RM01	การขาดแคลนบุคลากรผู้ปฏิบัติงาน	ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศมีจำนวนไม่เพียงพอที่จะสนับสนุนภาระงานที่มีอยู่	- การไม่ได้รับการบรรจุตามความต้องการกำลังพล - การโยกย้ายบุคลากรด้านสารสนเทศ	- การปฏิบัติงานด้านเทคโนโลยีสารสนเทศล่าช้า/หยุดชะงัก - กระทบต่อการพัฒนาและควบคุมดูแลระบบ	๔	๒	๘

รายการความเสี่ยงด้านการบริหารจัดการ (RM)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RM02	การแก้ไขปัญหาทางระบบสารสนเทศเกิดความล่าช้า	ผู้ที่ปฏิบัติงานในตำแหน่งที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีความรู้ไม่เพียงพอในการปฏิบัติงาน	- การบรรจุบุคลากรไม่ตรงตามวุฒิการศึกษา - บุคลากรไม่ได้รับการอบรมเกี่ยวกับระบบที่ดูแลที่เพียงพอ	- การปฏิบัติงานที่ต้องอาศัยระบบสารสนเทศเกิดความล่าช้า - ระบบสารสนเทศเกิดความเสียหาย	๓	๒	๖
RM03	อุปกรณ์ในระบบสารสนเทศ ไม่ทันสมัย และเสื่อมสภาพ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ	งบประมาณที่ได้รับไม่ครอบคลุมความต้องการ	ระบบสารสนเทศที่สนับสนุนการปฏิบัติงานหยุดชะงักและขาดประสิทธิภาพ	๓	๒	๖
RM04	การเปลี่ยนแปลงนโยบายของผู้บังคับบัญชา	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	- นโยบายของผู้บังคับบัญชาไม่สอดคล้องกัน - ขาดความต่อเนื่องในการสานต่อโครงการต่างๆ	การดำเนินงานขาดความต่อเนื่อง	๓	๔	๑๒

รายการความเสี่ยงด้านการบริหารจัดการ (RM)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RM05	ข้อมูลสำคัญถูกโจรกรรม	บุคคลจากภายนอกหน่วย หรือจากภายนอก บน.๑ เข้ามาในพื้นที่ปฏิบัติงานเพื่อกระทำการอันตรายใดๆ ต่อระบบสารสนเทศ	- ขาดมาตรการรักษาความปลอดภัยในการเข้าพื้นที่ - ผู้ไม่ประสงค์ดีที่แฝงตัวมากับบุคคลภายนอกหน่วย หรือจากภายนอก บน.๑	- ระบบสารสนเทศเกิดความเสียหาย - ข้อมูลสำคัญโดยเฉพาะข้อมูลที่มีชั้นความลับถูกเปิดเผย	๑	๕	๕

รายงานความเสี่ยงจากผู้ปฏิบัติงาน (RP)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RP01	การละเมิดสิทธิ์เข้าถึงข้อมูลส่วนบุคคล	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือการละเลยไม่ log out ออกจากระบบหลังเลิกใช้งาน ทำให้ผู้ไม่มีสิทธิ์สามารถเข้าใช้งานระบบสารสนเทศได้	- บุคลากรที่ขาดความเข้าใจเรื่องการรักษาความปลอดภัยระบบสารสนเทศ - ถูก Phishing เมื่อลงชื่อเข้าใช้งานบนเว็บไซต์ปลอม - ถูกโปรแกรม Key logger ขโมยชื่อผู้ใช้และรหัสผ่าน	- ระบบสารสนเทศเกิดความเสียหาย - ข้อมูลส่วนบุคคลสูญหาย หรือถูกเปิดเผย	๓	๓	๙

รายงานความเสี่ยงจากผู้ปฏิบัติงาน (RP)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RP02	ช่องโหว่จากการนำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ที่ไม่ได้รับอนุญาตมาเชื่อมต่อเข้าเครือข่าย	ผู้ใช้นำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) มาเชื่อมต่อโดยไม่ได้รับอนุญาตหรือแจ้งให้ผู้ดูแลระบบทราบ	- บุคลากรของ บน.๑ ที่ขาดความเข้าใจในเรื่องการรักษาความปลอดภัยระบบสารสนเทศ - ขาดมาตรการในการจำกัดการเข้าใช้งานเครือข่าย	ระบบสารสนเทศเกิดความเสียหาย	๓	๔	๑๒
RP03	ระบบงานเสียหายจากความผิดพลาดของผู้ปฏิบัติงาน	บุคลากรที่ใช้งานระบบสารสนเทศปฏิบัติผิดพลาด เช่น เผลอลบข้อมูลที่สำคัญในระบบ ตั้งค่าระบบผิดพลาด กรอกข้อมูลผิด หรือแก้ไขโค้ดโปรแกรมผิดพลาด ทำให้ระบบสารสนเทศทำงานผิดพลาดหรือไม่สามารถทำงานได้	- บุคลากรขาดความรู้ในการใช้งานระบบสารสนเทศ - ขาดความรอบคอบในการปฏิบัติงาน - อุบัติเหตุจากการรู้เท่าไม่ถึงการณ์ประมาท	ระบบสารสนเทศที่สนับสนุนการปฏิบัติงานหยุดชะงักและเกิดความเสียหาย	๓	๒	๖

รายงานความเสี่ยงจากผู้ปฏิบัติงาน (RP)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RP04	ข้อมูลที่มีผลกระทบต่อองค์กร และด้านยุทธการ รั่วไหลผ่านทางระบบสารสนเทศ	มีการเผยแพร่ข้อมูลสำคัญของทางราชการ ที่มีผลต่อการปฏิบัติด้านยุทธการ และความมั่นคง	บุคลากรของ บน.๑ ที่ขาดความเข้าใจในการรักษาความปลอดภัยในระบบสารสนเทศเบื้องต้น	ข้อมูลสำคัญโดยเฉพาะข้อมูลที่มีชั้นความลับถูกเปิดเผย และกระทบต่อความมั่นคง	๑	๕	๕

รายการความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (RE)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RE01	กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	การเกิดกระแสไฟฟ้าขัดข้องแบบกะทันหัน เช่น ไฟฟ้าดับ-กระชากที่มีสาเหตุจากภัยธรรมชาติหรือจากการขัดข้องของอุปกรณ์ในระบบไฟฟ้า	- แหล่งกำเนิดไฟฟ้าขัดข้อง - ภัยธรรมชาติที่ส่งผลให้แหล่งกำเนิดไฟฟ้าขัดข้อง	อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เชื่อมต่อเครือข่ายได้รับความเสียหาย	๕	๔	๒๐

รายการความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (RE)

รหัสความเสี่ยง	**ชื่อความเสี่ยง** (เหตุการณ์)	**ลักษณะ** (อธิบาย)	**ปัจจัยเสี่ยง** (สาเหตุ)	**ผลกระทบ**	O (๑-๕)	E (๑-๕)	SUM (๑-๒๕)
RE02	เครือข่ายภายใน บน.๑ ไม่สามารถใช้งานได้	ไม่สามารถใช้งานระบบเครือข่าย ที่ให้บริการผ่านอุปกรณ์เครือข่ายของ บน.๑ ได้	- เครือข่ายผู้ให้บริการภายนอกขัดข้อง - เครือข่าย ทอ. ขัดข้อง - การถูกโจมตีด้วย DDos (Distributed Denial of-Service)	- ไม่สามารถใช้บริการระบบสารสนเทศ ผ่านเครือข่ายได้ - การปฏิบัติงานที่ต้องอาศัยระบบสารสนเทศ ผ่านเครือข่ายต้องหยุดชะงัก - ข้อมูลสำคัญที่เก็บไว้บนระบบคลาวด์ (Cloud Storage) อาจสูญหาย	๓	๔	๑๒
RE03	อัคคีภัย	เหตุการณ์อัคคีภัยในอาคารที่ลุกลามสร้างความเสียหายให้กับอุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เชื่อมต่อเครือข่าย	- อัคคีภัยจากกระแสไฟฟ้าขัดข้อง - อัคคีภัยจากอุบัติเหตุการใช้อุปกรณ์ไฟฟ้า	อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์เชื่อมต่อเครือข่ายเสียหาย	๒	๕	๑๐

๖. รายการความเสี่ยงตามลำดับและมาตรการจัดการความเสี่ยง

มาตรการจัดการความเสี่ยง : ยอมรับ, ถ่ายโอน, หลีกเลี่ยง, จำกัด

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	SUM (๑-๒๕)	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๑	RE01	กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๒๐	ยอมรับ	- จัดหาเครื่องกำเนิดไฟฟ้าและเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัด จนท.ตรวจสอบตามระยะเวลา	คณก. CIO ฝทสส.ฯ ผสอ.ฯ ผชย.ฯ	โครงการพัฒนาประจำปี
๒	RT04	ระบบการทำงานของซอฟแวร์ขัดข้องจากช่องโหว่จุดอ่อนที่ไม่เคยถูกพบมาก่อน (Zero Day)	๑๖	ถ่ายโอน	ประสาน ทสส.ทอ.จัดหาซอฟแวร์ที่มีลิขสิทธิ์และการอัพเดทการสนับสนุนด้านป้องกันช่องโหว่ จากเจ้าของผลิตภัณฑ์	ฝทสส.ฯ	ตลอดเวลา
๓	RT02	เครื่องคอมพิวเตอร์ลูกข่าย หรืออุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ขัดข้อง	๑๖	ยอมรับ	- จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ทดแทน เพื่อให้สามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์อย่างสม่ำเสมอ	คณก. CIO ฝทสส.ฯ ผสอ.ฯ	ตามวงรอบ
๔	RT01	อุปกรณ์สารสนเทศขัดข้อง	๑๒	ยอมรับ	- จัดหาอุปกรณ์สารสนเทศทดแทน เพื่อให้สามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาอุปกรณ์สารสนเทศอย่างสม่ำเสมอ	คณก. CIO ฝทสส.ฯ ผสอ.ฯ	ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	SUM (๑-๒๕)	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๕	RT03	เครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง	๑๒	ยอมรับ	- จัดหาเครื่องคอมพิวเตอร์แม่ข่ายทดแทน เพื่อให้สามารถปฏิบัติงานได้ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ	คณก. CIO ฝทสส.ฯ ผสอ.ฯ	ตามวงรอบ
๖	RM04	การเปลี่ยนแปลงนโยบายของผู้บังคับบัญชา	๑๒	ยอมรับ	จัดทำแผนแม่บทการพัฒนาระบบ เพื่อเป็นกรอบแนวทางการพัฒนาให้ผู้บังคับบัญชา ใช้เป็นข้อมูลในการพัฒนาระบบในอนาคต	คณก. CIO	ปีละ ๑ ครั้ง
๗	RP02	ช่องโหว่จากการนำอุปกรณ์ส่วนบุคคล (Bring Your Own Device: BYOD) ที่ไม่ได้รับอนุญาตมาเชื่อมต่อเข้าเครือข่าย	๑๒	หลีกเลี่ยง	- จัดฝึกอบรมเพื่อสร้างความตระหนักในเรื่อง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง - ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ส่วนบุคคลที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	คณก. CIO ฝทสส.ฯ ผสอ.ฯ	ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	SUM (๑-๒๕)	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๘	RE02	เครือข่ายภายใน บน.๑ ไม่สามารถใช้งานได้	๑๒	ถ่ายโอน	- จัดหาเครือข่ายสำรองและติดตั้งอุปกรณ์สำรองต่าง ๆ ให้ครบถ้วน - จัดทำแผนเครือข่ายสำรอง	ฝทสส.ฯ ผสอ.ฯ	โครงการพัฒนาประจำปี
๙	RE03	อัคคีภัย	๑๒	ยอมรับ	- จัดหาระบบสำรอง เพื่อให้ระบบสารสนเทศ สามารถทำงานได้ - สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่น อีกหนึ่งชุด	คณก. CIO ฝทสส.ฯ ผสอ.ฯ	- โครงการพัฒนาประจำปี - ตามวงรอบ
๑๐	RP01	การละเมิดสิทธิ์เข้าถึงข้อมูลส่วนบุคคล	๙	หลีกเลี่ยง	- สร้างความตระหนักเรื่องข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	คณก. CIO ฝทสส.ฯ นขต.บน.๑	ตามวงรอบ
๑๑	RM01	การขาดแคลนบุคลากรผู้ปฏิบัติงาน	๘	ยอมรับ	- จัดอบรมเจ้าหน้าที่ให้มีความรู้เพิ่มเติม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้	คณก. CIO ฝทสส.ฯ นขต.บน.๑	ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	SUM (๑-๒๕)	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๑๒	RM02	การแก้ไขปัญหาทางระบบสารสนเทศเกิดความล่าช้า	๖	ถ่ายโอน	- จัดส่งเจ้าหน้าที่เข้ารับการอบรม เพื่อให้มีความรู้เพิ่มเติม - แจ้งข้อขัดข้องในการบรรจุกำลังพลให้สายวิทยาการรับทราบ เพื่อกำหนดคุณสมบัติของเจ้าหน้าที่ให้เหมาะสม	คณก. CIO ฝทสส.ฯ นขต.บน.๑	ตามวงรอบ
๑๓	RM03	อุปกรณ์ในระบบสารสนเทศ ไม่ทันสมัย และเสื่อมสภาพ	๖	ยอมรับ	จัดทำโครงการเพื่อขอรับการสนับสนุนอย่างต่อเนื่อง	ฝทสส.ฯ ผสอ.ฯ	โครงการพัฒนาประจำปี
๑๔	RP03	ระบบงานเสียหายจากความผิดพลาดของผู้ปฏิบัติงาน	๖	จำกัด	- จัดอบรมและทบทวนการปฏิบัติให้เจ้าหน้าที่อย่างสม่ำเสมอ - สำรองข้อมูลระบบและฐานข้อมูลเก็บไว้ในสถานที่อื่น อีกหนึ่งชุด	ฝทสส.ฯ ผสอ.ฯ นขต.บน.๑	ตามวงรอบ
๑๕	RM05	ข้อมูลสำคัญถูกโจรกรรม	๕	จำกัด	- ตรวจสอบการเข้าออกของบุคคลภายนอก - กำหนดพื้นที่หวงห้าม ในการเข้าถึงพื้นที่ปฏิบัติงาน	คณก. CIO ฝทสส.ฯ ผสอ.ฯ ผขว.ฯ	ตามวงรอบ

ลำดับ	รหัสความเสี่ยง	ชื่อความเสี่ยง	SUM (๑-๒๕)	มาตรการจัดการความเสี่ยง	แนวทางการดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา
๑๖	RP04	ข้อมูลที่มีผลกระทบต่อองค์กร และด้านยุทธการ รั่วไหลผ่านทางระบบสารสนเทศ	๕	หลีกเลี่ยง	- จัดฝึกอบรมเพื่อสร้างความตระหนักในเรื่อง นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - กระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง	คณก. CIO ฝทสส.ฯ นขต.บน.๑	ตามวงรอบ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศ เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อไป

(ลงชื่อ) น.อ.

(ปรธร จีนะวัฒน์)

ประธานกรรมการรักษาความปลอดภัยระบบสารสนเทศ

ชื่อหน่วยงาน กองบิน ๑

๑๐ ก.ค.๖๑

น.อ.

(วชิระพล เมืองน้อย)

ผบ.บน.๑

๑๐ ก.ค.๖๑