



**แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
(Cyber Risk Management)
ของสำนักงานนโยบายและแผนการขนส่งและจราจร**

ประจำปีงบประมาณ พ.ศ. 2569

โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
(Cyber Risk Management)
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

คำนำ

ความเสี่ยง (Risk) คือ เหตุการณ์ใด ๆ ที่อาจเกิดขึ้นได้ตลอดเวลาภายใต้สถานการณ์ที่ไม่แน่นอน และส่งผลกระทบต่อสร้างความเสียหาย ความล้มเหลว หรือลดโอกาสที่จะทำให้ไม่บรรลุเป้าหมายที่กำหนดไว้ หน่วยงานจึงต้องรู้และเข้าใจความเสี่ยงประเภทต่าง ๆ ที่หน่วยงานเผชิญอยู่ เพื่อเลือกวิธีการจัดการกับ ความเสี่ยงเหล่านั้นอย่างเหมาะสมและมีประสิทธิภาพ โดยไม่ส่งผลกระทบและหรือความเสียหายกับหน่วยงาน หรือเกิดขึ้นน้อยที่สุดและอยู่ในระดับที่หน่วยงานยอมรับได้

“แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่ง และจราจร (สนข.) ประจำปีงบประมาณ พ.ศ. ๒๕๖๙” จัดทำขึ้นเพื่อใช้เป็นแนวปฏิบัติในการบริหาร และจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ ได้แก่ การบ่งชี้/ระบุความเสี่ยง วิเคราะห์ความเสี่ยง การกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดปัจจัยที่จะก่อให้เกิดความเสี่ยง ติดตามผล และรายงานผลการดำเนินงาน สร้างความเชื่อมั่นว่าระบบเทคโนโลยีสารสนเทศของ สนข. สามารถใช้งาน ได้อย่างปลอดภัยและพร้อมใช้งานได้อย่างต่อเนื่องตลอดเวลา สามารถสนับสนุนการปฏิบัติงานของ สนข. ให้บรรลุเป้าหมายที่กำหนดไว้ได้

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยง ด้านความมั่นคงปลอดภัยไซเบอร์ ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ฉบับนี้ จะเป็นแนวปฏิบัติ สำหรับการบริหารและจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. ต่อไป ทั้งนี้ ศทท. ยินดีรับ ข้อเสนอแนะ/ข้อแนะนำที่เป็นประโยชน์ต่อแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. เพื่อปรับปรุงให้การบริหารความเสี่ยงครอบคลุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. ให้มากยิ่งขึ้น เป็นปัจจุบันและทันต่อสถานการณ์อยู่ตลอดเวลา

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

สารบัญ

	หน้า
บทที่ ๑ บทนำ	
๑.๑ หลักการและเหตุผล	๑
๑.๒ วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ของ สนข.	๑
๑.๓ เป้าหมาย	๑
๑.๔ ขอบเขตการดำเนินงาน	๑
๑.๕ ประโยชน์ที่คาดว่าจะได้รับ	๒
บทที่ ๒ การบริหารความเสี่ยง	
๒.๑ กระบวนการบริหารความเสี่ยง	๒
๒.๒ ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.	๘
๒.๓ ปัจจัยเสี่ยง	๙
บทที่ ๓ การทบทวนและวิเคราะห์ความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ของ สนข.	
๓.๑ แนวทางและขั้นตอนการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สนข.	๑๐
๓.๒ กระบวนการจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.	๑๑
๓.๓ การทบทวนและวิเคราะห์ปัจจัยความเสี่ยงด้านไซเบอร์ของ สนข.	๑๑
๓.๔ การบ่งชี้และระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.	๑๕
๓.๕ ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.	๒๒
๓.๖ สรุปผลการประเมินและแนวทางควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙	๒๕
๓.๗ การจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙	๓๘
บทที่ ๔ บทสรุปและข้อเสนอแนะ	
๔.๑ สรุปความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	๔๓
๔.๒ บทสรุป	๔๓
๔.๓ ข้อเสนอแนะ	๔๔

สารบัญภาพ

	หน้า
รูปภาพที่ ๒-๑	การบริหารความเสี่ยงตามแนวทางของ COSO-ERM
รูปภาพที่ ๒-๒	แผนผังค่าความเสี่ยงแต่ละระดับ (Risk Matrix)
รูปภาพที่ ๓-๑	แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของ สนช.
รูปภาพที่ ๓-๒	กระบวนการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนช.
รูปภาพที่ ๓-๓	แผนผังค่าความเสี่ยงแต่ละระดับ (Risk Matrix)

สารบัญตาราง

	หน้า
ตารางที่ ๒-๑	ระดับของโอกาสที่จะเกิด
ตารางที่ ๒-๒	ระดับของความรุนแรงด้านการปฏิบัติงาน
ตารางที่ ๒-๓	ระดับของความรุนแรงด้านการเงิน
ตารางที่ ๒-๔	ระดับของความรุนแรงด้านภาพลักษณ์และชื่อเสียง
ตารางที่ ๒-๕	ระดับของความรุนแรงด้านบุคลากร
ตารางที่ ๒-๖	แสดงอันตรายภาคขึ้น ระดับความเสี่ยง แลปสี่ และควาหมายของความเสี่ยงแต่ละชั้น
ตารางที่ ๓-๑	แสดงอันตรายภาคขึ้น ระดับความเสี่ยง แลปสี่ และควาหมายของความเสี่ยงแต่ละชั้น
ตารางที่ ๓-๒	การทบทวนและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
ตารางที่ ๓-๓	การระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Register) ของ สนช.
ตารางที่ ๓-๔	ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
ตารางที่ ๓-๕	สรุปผลการประเมินและแนวทางควบคุมความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
ตารางที่ ๓-๖	แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

บทที่ ๑ บทนำ

๑.๑ หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี ซึ่งจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผล การปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ ลดการสูญเสีย และโอกาสที่ทำให้เกิดความเสียหายแก่หน่วยงาน โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่ปัจจุบันได้เข้ามามีบทบาทสำคัญอย่างมากในการดำเนินงานของหน่วยงาน ทั้งการใช้งานเครื่องคอมพิวเตอร์ในการปฏิบัติงานสำนักงาน การจัดเก็บข้อมูล การติดต่อสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ การใช้งานเอกสารอิเล็กทรอนิกส์แทนกระดาษ และการปรับเปลี่ยนกระบวนการปฏิบัติงานของหน่วยงานเป็นรูปแบบดิจิทัล

ระบบเทคโนโลยีสารสนเทศของทุก ๆ หน่วยงานล้วนแล้วแต่มีปัจจัยเสี่ยงซึ่งก็คือต้นเหตุหรือสาเหตุที่จะทำให้ระบบสารสนเทศของหน่วยงานหยุดทำงานหรือทำงานได้เพียงบางส่วน ซึ่งส่งผลกระทบต่อการทำงานหรือเป้าหมายของหน่วยงาน ดังนั้น สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) จึงจำเป็นต้องมีแผนในการบริหารและจัดการกับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศของ สนข. อย่างถูกต้องและเหมาะสม โดยเริ่มจากการค้นหาและระบุความเสี่ยง วิเคราะห์ความเสี่ยงจากโอกาสที่จะเกิดและระดับความรุนแรงของผลกระทบจากความเสี่ยงนั้น ประเมินระดับความเสี่ยง จัดลำดับความสำคัญของความเสี่ยง และกำหนดมาตรการในการตอบสนองต่อความเสี่ยงอย่างเหมาะสม และหน่วยงานสามารถยอมรับได้

๑.๒ วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.

๑.๒.๑ เป็นคู่มือในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. และติดตามผลการดำเนินงานอย่างถูกต้องและเหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่หน่วยงานสามารถยอมรับได้

๑.๒.๒ เป็นแนวปฏิบัติในการดูแลรักษาระบบสารสนเทศต่าง ๆ ของ สนข. ให้มีเสถียรภาพ มีความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA ทั้ง ๓ ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

๑.๒.๓ สร้างความเชื่อมั่นและรับประกันว่าระบบสารสนเทศของ สนข. จะยังคงสามารถให้บริการได้อย่างต่อเนื่องทั้งในสถานการณ์ปกติ และ/หรือสถานการณ์ฉุกเฉิน

๑.๓ เป้าหมาย

ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ได้รับการขจัด ลด หรือควบคุมผลกระทบและความเสียหายที่เกิดขึ้นให้อยู่ในระดับที่หน่วยงานยอมรับได้

๑.๔ ขอบเขตการดำเนินงาน

ระบบสารสนเทศภายในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.)

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

ระบบสารสนเทศของ สนข. สามารถใช้งานได้อย่างปลอดภัยและพร้อมใช้งานได้อย่างต่อเนื่องตลอดเวลา สามารถสนับสนุนการปฏิบัติงานของ สนข. ให้บรรลุเป้าหมายที่กำหนดไว้ได้

บทที่ ๒

การบริหารความเสี่ยง

๒.๑ กระบวนการบริหารความเสี่ยง



รูปภาพที่ ๒-๑ การบริหารความเสี่ยงตามแนวทางของ COSO-ERM

การบริหารความเสี่ยงตามแนวทางของ COSO-ERM (The Committee of Sponsoring Organization of the Treadway Commission - Enterprise Risk Management) ประกอบด้วยองค์ประกอบ ๘ ประการ ซึ่งสัมพันธ์กับการดำเนินการธุรกิจและกระบวนการบริหารงาน ดังต่อไปนี้

๒.๑.๑ สภาพแวดล้อมภายในหน่วยงาน (Internal Environment)

เป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการบริหารความเสี่ยงและเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงของหน่วยงาน ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมหน่วยงาน นโยบายของผู้บริหาร แนวปฏิบัติงานของบุคลากร กระบวนการทำงาน ระบบสารสนเทศ เป็นต้น โดยสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศของ สนข. มีดังนี้

(๑) สารสนเทศและฐานข้อมูล (Information & Database) เช่น เว็บไซต์ (Web Portal) และเว็บอินทราเน็ต (Intranet) ฐานข้อมูลเว็บไซต์ และเว็บไซต์อินทราเน็ต (Intranet) ของ สนข. เป็นต้น

(๒) เว็บแอปพลิเคชันและระบบฐานข้อมูลภายใน (Back End Office) เช่น เว็บแอปพลิเคชันระบบบริหารงานสำนักงานอัตโนมัติ (e-Office) และฐานข้อมูล เว็บแอปพลิเคชันระบบสารสนเทศทรัพยากรบุคคล (DPIS) และฐานข้อมูล ฐานข้อมูลครุภัณฑ์คอมพิวเตอร์ (ICT Asset) เป็นต้น

(๓) ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ภายในทั้งแบบมีสาย (Wire LAN) และแบบไร้สาย (Wireless LAN หรือ Wi-Fi) และระบบเครือข่ายอินเทอร์เน็ต (Internet)

(๔) อุปกรณ์คอมพิวเตอร์ (Hardware) เป็นต้น เครื่องคอมพิวเตอร์แม่ข่าย (Server) ของระบบงานต่าง ๆ ทั้งแบบ Physical Machine และแบบ Virtual Machine เครื่องคอมพิวเตอร์ Desktop, เครื่องคอมพิวเตอร์ All In One, เครื่องคอมพิวเตอร์ Notebook, เครื่อง Scanner, เครื่องพิมพ์ Laser, เครื่องพิมพ์ Ink-Jet, เครื่องสำรองไฟฟ้าฉุกเฉิน (UPS), อุปกรณ์เครือข่าย เช่น L๓ Switch, Router, Wireless Access point เป็นต้น

(๕) ระบบรักษาความปลอดภัย ทั้งแบบอุปกรณ์ (Hardware appliance) เช่น Firewall, Web Application และแบบโปรแกรมประยุกต์ (Software) เช่น ระบบพิสูจน์ตัวตน (Active Directory : AD) เป็นต้น

๒.๑.๒ การกำหนดวัตถุประสงค์ (Objective Setting)

หน่วยงานต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยงให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่หน่วยงานยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงของหน่วยงานได้อย่างชัดเจนและเหมาะสม โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษร โดยสามารถพิจารณาในด้านต่าง ๆ ได้ ดังนี้

- (๑) วิสัยทัศน์ พันธกิจ เป้าหมาย วัตถุประสงค์ด้านยุทธศาสตร์
- (๒) ด้านการปฏิบัติงาน เกี่ยวข้องกับประสิทธิภาพ ผลการปฏิบัติงาน
- (๓) ด้านการรายงาน เกี่ยวข้องกับการรายงานทั้งภายในและภายนอกหน่วยงาน
- (๔) ด้านกฎ ระเบียบ ข้อบังคับ เกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ

๒.๑.๓ การระบุความเสี่ยง (Risk Identification)

เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งปัจจัยเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอกหน่วยงาน และเมื่อเกิดขึ้นแล้วส่งผลให้หน่วยงานไม่บรรลุวัตถุประสงค์หรือเป้าหมาย เช่น นโยบายการบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบข้อบังคับ เป็นต้น ทั้งนี้ เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น ๆ และเพื่อให้ผู้บริหารพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้เป็นอย่างดี วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- (๑) การประชุมระดมความคิด (Brainstorm) เพื่อให้ได้ความเสี่ยงที่หลากหลาย
- (๒) การใช้รายการตรวจสอบ (Checklist)
- (๓) การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- (๔) การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- (๕) การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ขั้นตอนการระบุความเสี่ยงนี้ สิ่งสำคัญ คือ การจัดเก็บข้อมูลที่เกี่ยวข้องในอดีต เช่น ระดับความเสียหาย มูลค่าความสูญเสีย จำนวนความถี่ที่เกิดขึ้น วิธีการจัดการ ปัญหาและอุปสรรค การแก้ไขปัญหา ผลการดำเนินงาน เพื่อนำมาใช้ในการวิเคราะห์ร่วมด้วยซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๒.๑.๔ การประเมินความเสี่ยง (Risk Assessment)

เป็นการวัดระดับความรุนแรงของความเสี่ยง เพื่อพิจารณาจัดลำดับความสำคัญในการนำความเสี่ยงที่อยู่ในอันตรายมาดำเนินการก่อน ประกอบด้วย ๒ มิติ คือ

- (๑) โอกาสที่จะเกิดความเสี่ยง (Likelihood) หมายถึง ความถี่ที่ปัจจัยเสี่ยงจะเกิดขึ้นมีมากน้อยเพียงใด ซึ่งเกณฑ์ในการพิจารณาโอกาสที่จะเกิดความเสี่ยงในแผนฯ ฉบับนี้ ดังแสดงในตารางที่ ๒-๑

ตารางที่ ๒-๑ ระดับของโอกาสที่จะเกิด

เกณฑ์การพิจารณา		โอกาสที่จะเกิด ความเสี่ยง	ระดับคะแนน
เชิงปริมาณ	เชิงคุณภาพ		
ไม่เกิน ๑ ครั้ง/ปี	แทบไม่มีโอกาสเกิดขึ้นเลย	น้อยมาก	๑
๒ ครั้ง/ปี	มีโอกาสดังขึ้นแต่นาน ๆ ครั้ง	น้อย	๒
๓ ครั้ง/ปี	มีโอกาสดังขึ้นในบางครั้ง	ปานกลาง	๓
๔ ครั้ง/ปี	มีโอกาสดังขึ้นบ่อยครั้ง	สูง	๔
มากกว่า ๔ ครั้ง/ปี	มีโอกาสดังขึ้นเกือบทุกครั้ง	สูงมาก	๕

(๒) ผลกระทบ (Impact) หรือความรุนแรง หรือความเสียหายในด้านต่าง ๆ เช่น ด้านการปฏิบัติงาน (Operational Risk) ด้านการเงิน (Financial Risk) ด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk) ด้านบุคลากร (People Risk) มีมากน้อยเพียงใด เป็นผลต่อเนื่องมาจากการเกิดเหตุการณ์นั้น ๆ ซึ่งเกณฑ์ในการพิจารณาผลกระทบในแผนฯ ฉบับนี้ ดังแสดงในตารางที่ ๒-๒ ตารางที่ ๒-๓ ตารางที่ ๒-๔ และตารางที่ ๒-๕

ตารางที่ ๒-๒ ระดับของความรุนแรงด้านการปฏิบัติงาน

รายละเอียด	ผลกระทบ/ความรุนแรง/ ความเสียหาย	ระดับคะแนน
ไม่ส่งผลกระทบต่อการทำงานของระบบสารสนเทศ หรือ ระยะเวลาหยุดชะงักไม่เกิน ๓๐ นาที	ต่ำมาก	๑
กระทบต่อการทำงานของระบบสารสนเทศของหน่วยงาน แต่แก้ไขได้ หรือ ระยะเวลาหยุดชะงักไม่เกิน ๑ ชั่วโมง	ต่ำ	๒
ระบบสารสนเทศมีปัญหา และมีความสูญเสียไม่มาก หรือ ระยะเวลาหยุดชะงักไม่เกิน ๖ ชั่วโมง	ปานกลาง	๓
ระบบสารสนเทศที่สำคัญและระบบความปลอดภัย ซึ่งส่งผลกระทบต่อความถูกต้องของข้อมูลบางส่วน หรือ ระยะเวลาหยุดชะงักไม่เกิน ๑๒ ชั่วโมง	สูง	๔
เกิดความสูญเสียต่อระบบสารสนเทศที่สำคัญทั้งหมด และ เกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูล หรือ ระยะเวลาหยุดชะงักมากกว่า ๑๒ ชั่วโมง	สูงมาก	๕

ตารางที่ ๒-๓ ระดับของความรุนแรงด้านการเงิน

รายละเอียด	ผลกระทบ/ความรุนแรง/ /ความเสียหาย	ระดับคะแนน
มูลค่าน้อยกว่า ๕ แสนบาท	ต่ำมาก	๑
มูลค่า ๕ แสนบาท - ๑ ล้านบาท	ต่ำ	๒
มูลค่า ๑ ล้านบาท - ๕ ล้านบาท	ปานกลาง	๓
มูลค่า ๕ ล้านบาท - ๑๐ ล้านบาท	สูง	๔
มูลค่ามากกว่า ๑๐ ล้านบาท	สูงมาก	๕

ตารางที่ ๒-๔ ระดับของความรุนแรงด้านภาพลักษณ์และชื่อเสียง

รายละเอียด	ผลกระทบ/ความรุนแรง/ความเสียหาย	ระดับคะแนน
มีการเผยแพร่ข่าว/รับรู้เฉพาะภายในแต่ละกลุ่ม/ฝ่ายเท่านั้น	ต่ำมาก	๑
มีการเผยแพร่ข่าว/รับรู้เฉพาะภายในแต่ละสำนัก/กอง/ศูนย์เท่านั้น	ต่ำ	๒
มีการเผยแพร่ข่าว/รับรู้ผ่านทางสื่อสิ่งพิมพ์ต่าง ๆ	ปานกลาง	๓
มีการเผยแพร่ข่าว/รับรู้ผ่านทางสื่อสิ่งพิมพ์ต่าง ๆ และสังคมออนไลน์	สูง	๔
มีการเผยแพร่ข่าว/รับรู้ผ่านทางสื่อสิ่งพิมพ์ต่าง ๆ สื่อโทรทัศน์ และสื่อสังคมออนไลน์	สูงมาก	๕

ตารางที่ ๒-๕ ระดับของความรุนแรงด้านบุคลากร

รายละเอียด	ผลกระทบ/ความรุนแรง/ความเสียหาย	ระดับคะแนน
ไม่มีการบาดเจ็บ	ต่ำมาก	๑
บาดเจ็บเล็กน้อย/ไม่ต้องเข้ารับการรักษาที่โรงพยาบาล	ต่ำ	๒
บาดเจ็บ/เข้ารับการรักษาที่โรงพยาบาล	ปานกลาง	๓
บาดเจ็บสาหัส/สูญเสียอวัยวะ/เข้ารับการรักษาที่โรงพยาบาลโดยเร่งด่วน	สูง	๔
เสียชีวิต	สูงมาก	๕

(๓) ค่าความเสี่ยง (Risk Score) หลังจากพิจารณาระดับของโอกาสที่จะเกิดความเสี่ยง (Likelihood Score) และผลกระทบ (Impact Score) ของปัจจัยเสี่ยงต่าง ๆ แล้ว จึงคำนวณหาระดับความเสี่ยงจากสูตร ดังนี้

$$\text{Risk Score} = \text{Likelihood Score} \times \text{Impact Score}$$

๒.๑.๕ การจัดระดับความเสี่ยงและแผนผังระดับความเสี่ยง (Risk Matrix)

ค่าความเสี่ยงเกิดจากผลคูณระหว่างระหว่างโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ในแผนฯ ฉบับนี้ มีการจัดค่าความเสี่ยงตามคะแนนที่ได้โดยเรียงลำดับจากคะแนนมากที่สุดไปน้อยที่สุด ค่าความเสี่ยงแต่ถูกแบ่งด้วยอันตรายภาคชั้นแต่ละชั้น ทั้งหมด ๔ ชั้น และมีแถบสีแสดงแทนความหมายของระดับความเสี่ยงแต่ละชั้น และการปฏิบัติเพื่อใช้ในการบริหารความเสี่ยงต่อไป

การประเมินความเสี่ยง

ผลกระทบ	๕	๑๐	๑๕	๒๐	๒๕
	๔	๘	๑๒	๑๖	๒๐
	๓	๖	๙	๑๒	๑๕
	๒	๔	๖	๘	๑๐
	๑	๒	๓	๔	๕

โอกาสที่จะเกิด

รูปภาพที่ ๒-๒ แผนผังค่าความเสี่ยงแต่ละระดับ (Risk Matrix)

ตารางที่ ๒-๖ แสดงอันตรายภาคขึ้น ระดับความเสี่ยง แถบสี และความหมายของความเสี่ยงแต่ละชั้น

อันตรายภาคขึ้น	ระดับความเสี่ยง	แถบสี	ความหมาย
๑๕ - ๒๕	สูงมาก		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้ลดลงมาอยู่ในระดับที่ยอมรับได้โดยทันที
๘ - ๑๔	สูง		ระดับที่ไม่สามารถยอมรับได้ ต้องมีการควบคุมและติดตามความเสี่ยงเพื่อไม่ให้เคลื่อนย้ายไประดับสูงมาก
๔ - ๗	ปานกลาง		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเพิ่มระดับไปสู่ระดับที่ยอมรับไม่ได้
๑ - ๓	ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องมีการควบคุมความเสี่ยงหรือไม่ต้องการจัดการเพิ่มเติม

๒.๑.๖ การตอบสนองความเสี่ยง (Risk Response)

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงและผลของการจัดการความเสี่ยงเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงระดับความเสี่ยงที่สามารถยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพ ผู้บริหารอาจต้องเลือกวิธีการตอบสนองความเสี่ยงวิธีใดวิธีหนึ่งหรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดและผลกระทบของความเสี่ยงให้อยู่ในช่วงที่หน่วยงานสามารถยอมรับได้ (Risk Tolerance) โดยวิธีการตอบสนองความเสี่ยงมี ๔ วิธีการ คือ

(๑) **หลีกเลี่ยง (Terminate)** เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย โดยอาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ ข้อเสียของวิธีการนี้ คือ หน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมโดยมิได้พิจารณาทบทวนถึงผลประโยชน์ที่จะได้รับ นำมาซึ่งการสูญเสียโอกาสของหน่วยงานได้

(๒) **การยอมรับ (Take)** เป็นการยอมรับความเสี่ยงและผลที่อาจตามมาหรือความเสียหายที่เกิดขึ้นไว้เองโดยไม่ทำอะไรเลย เนื่องจากพิจารณาแล้วเห็นว่าอยู่ในวิสัยที่หน่วยงานสามารถยอมรับได้ หรือไม่คุ้มค่าสำหรับการดำเนินการจัดการกับความเสี่ยง

(๓) **ควบคุม (Treat)** เป็นการปรับปรุงกระบวนการปฏิบัติงานหรือออกแบบกระบวนการปฏิบัติงานใหม่ เพื่อลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากไม่สามารถป้องกันได้ ก็ควรจัดให้หมดไป หรือลดระดับความเสี่ยงลงโดยใช้วิธีการควบคุม ทั้งนี้วิธีการควบคุมความเสี่ยงมี ๒ วิธี คือ การควบคุมเพื่อป้องกันมิให้เกิดความเสี่ยง เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความเสี่ยง และการควบคุมขอบเขตของความเสี่ยงภายหลังจากที่เกิดขึ้น เป็นวิธีการจำกัดความเสี่ยงมิให้ขยายวงกว้างออกไปเกินกว่าขอบเขตที่กำหนด

(๔) **การถ่ายโอน (Transfer)** เป็นการโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ แทนหรือรับผิดชอบร่วมกัน

๒.๑.๗ การควบคุมความเสี่ยง (Risk control)

การกำหนดวิธีการดำเนินการเพื่อควบคุมความเสี่ยงที่อาจเกิดขึ้นในระยะต่าง ๆ ก่อนเกิดขณะเกิด หรือหลังเกิดความเสี่ยงขึ้นแล้ว ได้อย่างถูกต้อง เพื่อให้ความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ โดยแบ่งได้เป็น ๔ ประเภท คือ

(๑) **การควบคุมเพื่อป้องกัน (Preventive Control)** เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างหน่วยงาน การควบคุมการเข้าถึงเอกสาร เป็นต้น

(๒) **การควบคุมเพื่อให้ตรวจพบ (Detective Control)** เป็นวิธีการควบคุม เพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

(๓) **การควบคุมโดยการชี้แนะ (Direction Control)** เป็นวิธีการควบคุมที่ส่งเสริม หรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

(๔) **การควบคุมเพื่อการแก้ไข (Corrective Control)** เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้ข้อผิดพลาดนั้นเกิดซ้ำอีกในอนาคต

โดยหลังจากขั้นตอนการประเมินความเสี่ยงแล้ว จึงวิเคราะห์ความเสี่ยงใดควรนำมาดำเนินการเป็นอันดับแรก โดยมีขั้นตอนดังนี้

(๔.๑) พิจารณารisk ที่มีค่าคะแนนอยู่ในลำดับสูงมาก (สีแดง) และลำดับสูง (สีส้ม) มาดำเนินการก่อน

(๔.๒) พิจารณาว่าในปัจจุบันความเสี่ยงตามข้อ (๔.๑) มีวิธีการควบคุมอยู่แล้วหรือไม่

(๔.๓) ถ้ามีวิธีการควบคุมแล้ว วิธีการดังกล่าวได้ผลตามความต้องการหรือไม่

(๔.๔) ถ้ายังไม่มีวิธีการควบคุม ให้พิจารณาเลือกวิธีการที่เหมาะสมกับความเสี่ยงนั้น ๆ

๒.๑.๘ สารสนเทศและการสื่อสาร (Information and Communication)

หน่วยงานจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงต่อไปตามกรอบและขั้นตอนการปฏิบัติที่หน่วยงานกำหนด

๒.๑.๙ การติดตามประเมินผล (Monitoring)

เป็นการติดตามประเมินผลการดำเนินการที่ผ่านมาว่า ยังมีความเสี่ยงหลงเหลืออยู่จากการประเมินความเสี่ยงหรือไม่ มาตรการหรือวิธีควบคุมที่ใช้กับความเสี่ยงเหมาะสมหรือไม่ สามารถขจัด ลด หรือควบคุมผลกระทบและความเสียหายที่เกิดขึ้นให้อยู่ในระดับที่หน่วยงานยอมรับได้หรือไม่ เพื่อนำมาวางแผนในการบริหารความเสี่ยง โดยสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยง ความเสี่ยง

เมื่อหน่วยงานทราบความเสี่ยงที่ และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้ และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

(๑) พิจารณาวាយอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับ

(๒) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

(๓) กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

(๔) ในรอบปีต่อไป ให้พิจารณาผลการติดตามการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานของหน่วยงานให้นำมาระบุงการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ ประเมิน และบริหารความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๒.๒ ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.

สนข. ได้กำหนดความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ ออกเป็น ๘ ด้าน ประกอบด้วย

๒.๒.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยธรรมชาติและภัยที่มนุษย์สร้างขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ไฟฟ้า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการมีโครงสร้างพื้นฐานไม่เพียงพอต่อความปลอดภัย เช่น ระบบไฟฟ้าส่องสว่างไม่เพียงพอ ระบบปรับอากาศชำรุดเสียหาย เจ้าหน้าที่รักษาความปลอดภัยไม่เพียงพอ เป็นต้น

๒.๒.๒ ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Network and Communication Risk)

หมายถึง ความเสี่ยงที่เกิดขึ้นกับระบบเครือข่ายเทคโนโลยีสารสนเทศต่าง ๆ เช่น ระบบเครือข่ายอินเทอร์เน็ต ไวรัสคอมพิวเตอร์ การเคลื่อนย้ายตัวเครื่อง อุปกรณ์ และการติดตั้งอุปกรณ์ในพื้นที่ที่ไม่เหมาะสม ภัยคุกคามทางคอมพิวเตอร์ต่าง ๆ

๒.๒.๓ ความเสี่ยงด้านระบบสารสนเทศและฐานข้อมูล (Information & Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากข้อมูลถูกทำลาย ฐานข้อมูลถูกบุกรุกเพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้ข้อมูลของหน่วยงานเกิดความเสียหายขาดความน่าเชื่อถือ และสร้างความเสื่อมเสียแก่ชื่อเสียงของหน่วยงาน ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารความเสี่ยงด้านระบบฐานข้อมูล เนื่องจากข้อมูลเป็นปัจจัยสำคัญสำหรับผู้บริหาร

๒.๒.๔ ความเสี่ยงด้านบุคลากร (Personal Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด เพื่อให้บุคลากรมีความรู้ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

๒.๒.๕ ความเสี่ยงในการบริหารจัดการ (Mangement Risk)

หมายถึง ความเสี่ยงต่อการได้รับการจัดสรรงบประมาณไม่เพียงพอ การบริหารไม่รัดกุม ไม่มีแผนงานในการดำเนินการที่ดี และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา

๒.๓ ปัจจัยเสี่ยง

ปัจจัยเสี่ยงที่จะก่อให้เกิดความเสียหายกับระบบสารสนเทศของ สนข. ได้แก่

๒.๓.๑ ปัจจัยภายนอก ไม่สามารถควบคุมได้ เช่น

- (๑) ภัยธรรมชาติ
- (๒) อุบัติภัย
- (๓) การโจรกรรม
- (๔) ระบบเครือข่ายคอมพิวเตอร์ขัดข้อง
- (๕) ระบบไฟฟ้าขัดข้อง
- (๖) ระบบเครือข่ายคอมพิวเตอร์ถูกบุกรุกหรือถูกเจาะ (Hack) จากบุคคลภายนอก (Hacker)
- (๗) สถานการณ์ความไม่สงบในบ้านเมือง
- (๘) สถานการณ์การแพร่ระบาดของโรคติดต่อร้ายแรง

๒.๓.๒ ปัจจัยภายใน สามารถควบคุมหรือป้องกันได้ เช่น

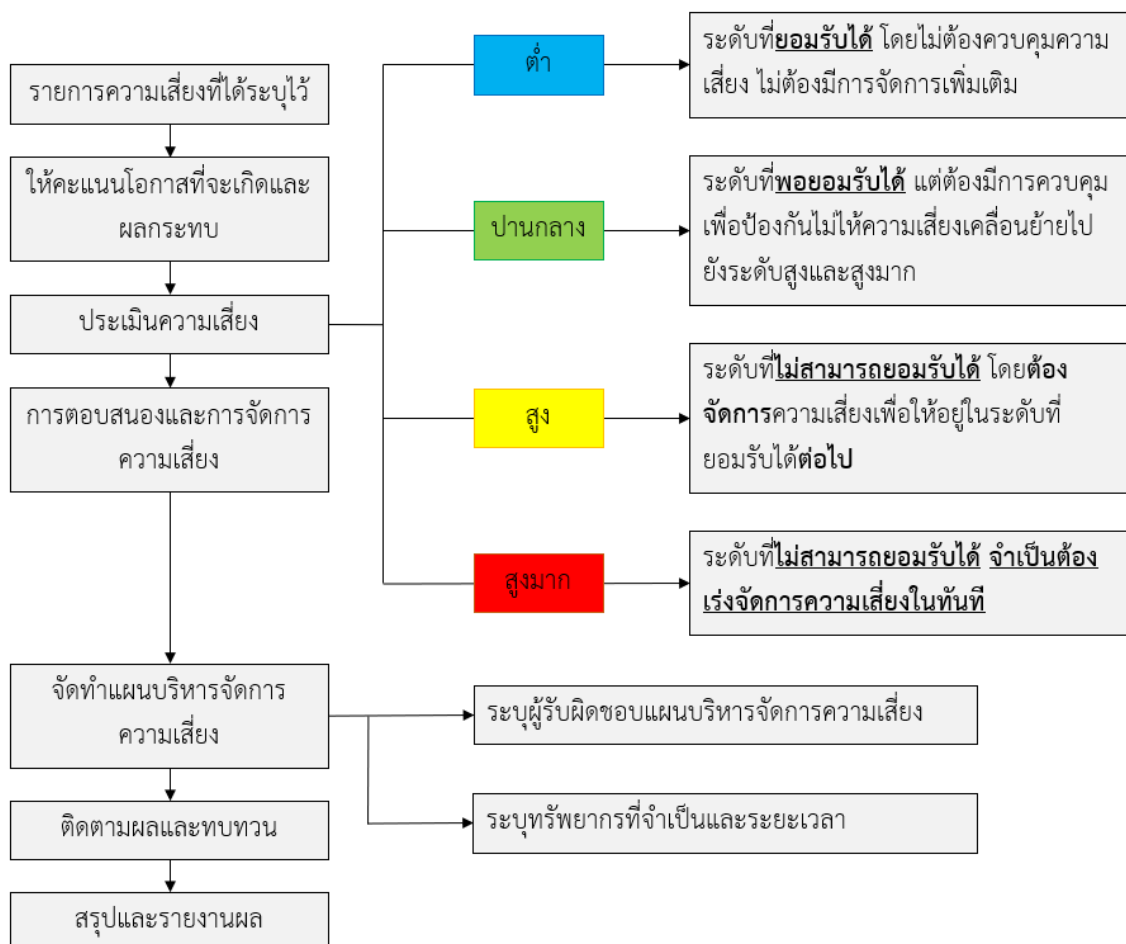
- (๑) อุปกรณ์ชำรุดหรือเสื่อมสภาพตามอายุการใช้งาน
- (๒) ระบบฐานข้อมูลหลักหรือข้อมูลเสียหาย
- (๓) ระบบงานอิเล็กทรอนิกส์และเว็บแอปพลิเคชันขัดข้อง
- (๔) มีโปรแกรมมัลแวร์ (Malware) เช่น Virus, Worm, Trojan horse, Spyware, Adware, Ransamware ที่แพร่กระจายภายในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน
- (๕) การใช้งานระบบเครือข่ายคอมพิวเตอร์ผิดวัตถุประสงค์ เช่น การเล่นเกมส์ การพนัน การนำเข้าข้อมูลที่ไม่เหมาะสม เป็นต้น

บทที่ ๓

การทบทวนและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.

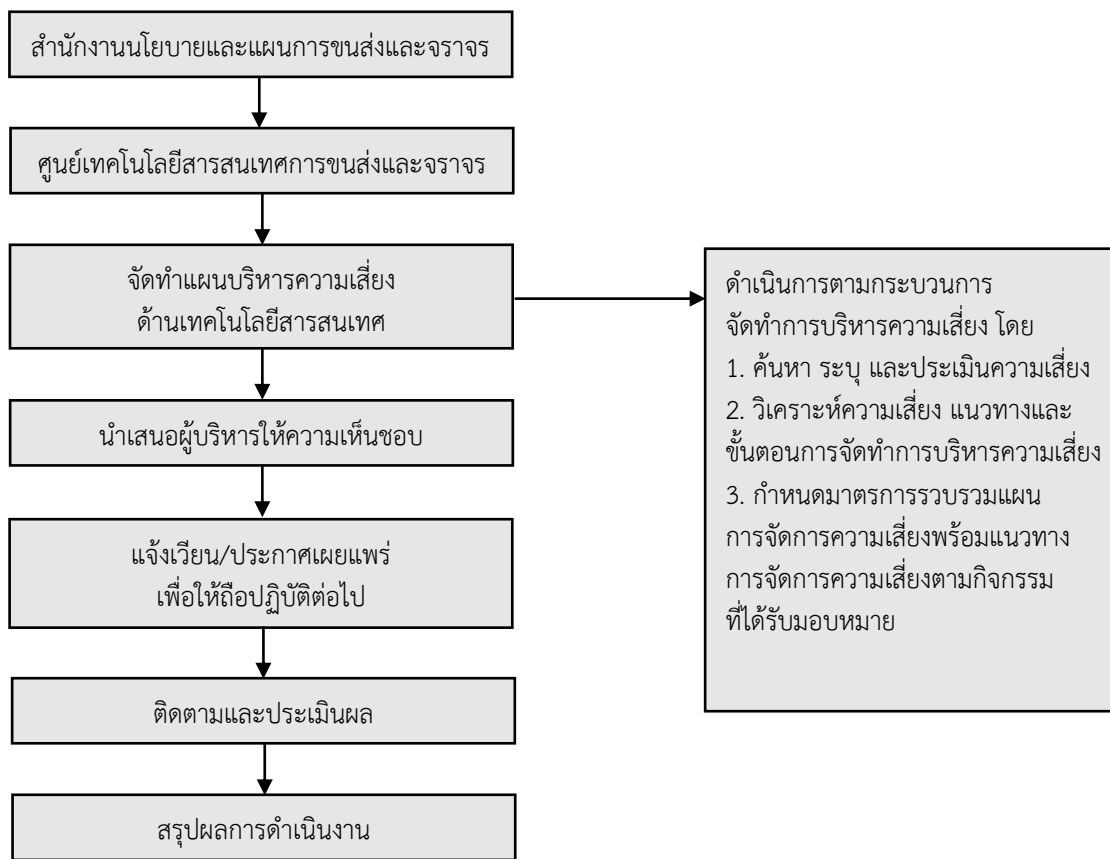
ศทท. ตระหนักถึงสถานการณ์ภัยคุกคามทางไซเบอร์และได้เฝ้าระวังติดตามเทคโนโลยีในปัจจุบันอย่างใกล้ชิด รวมทั้งตระหนักถึงปัจจัยต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศของ สนข. จนอาจทำให้ไม่สามารถใช้งาน หรือให้บริการระบบงานอิเล็กทรอนิกส์ต่าง ๆ ได้ จึงได้มีการทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. และจัดทำเป็น “แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ประจำปีงบประมาณ พ.ศ. ๒๕๖๙” เพื่อใช้เป็นแนวปฏิบัติในการบริหารจัดการกับความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. และสร้างความเชื่อมั่นว่าระบบสารสนเทศของ สนข. สามารถใช้งานได้อย่างปลอดภัยและพร้อมใช้งานได้อย่างต่อเนื่องตลอดเวลา สามารถสนับสนุนการปฏิบัติงานของ สนข. ให้บรรลุเป้าหมายที่กำหนดไว้ได้ โดยมีรายละเอียดในขั้นตอนต่าง ๆ ดังนี้

๓.๑ แนวทางและขั้นตอนการบริหารความมั่นคงปลอดภัยไซเบอร์ของ สนข.



รูปภาพที่ ๓-๑ แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.

๓.๒ กระบวนการจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.



รูปภาพที่ ๓-๒ กระบวนการจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.

๓.๓ การทบทวนและวิเคราะห์ปัจจัยความเสี่ยงด้านไซเบอร์ของ สนข.

ค่าความเสี่ยงเกิดจากผลคูณระหว่างระหว่างโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบ (Impact) ในแผนฯ ฉบับนี้ มีการจัดค่าความเสี่ยงตามคะแนนที่ได้โดยเรียงลำดับจากคะแนนมากที่สุดไปน้อยที่สุด ค่าความเสี่ยงแต่ถูกแบ่งด้วยอันตรภาคชั้นแต่ละชั้น ทั้งหมด ๔ ชั้น และมีแถบสีแสดงแทนความหมายของระดับความเสี่ยงแต่ละชั้นและการปฏิบัติเพื่อใช้ในการบริหารความเสี่ยงต่อไป

		การประเมินความเสี่ยง				
ผลกระทบ	๕	๑๐	๑๕	๒๐	๒๕	
	๔	๘	๑๒	๑๖	๒๐	
	๓	๖	๙	๑๒	๑๕	
	๒	๔	๖	๘	๑๐	
	๑	๒	๓	๔	๕	
		โอกาสที่จะเกิด				

รูปภาพที่ ๓-๓ แผนผังค่าความเสี่ยงแต่ละระดับ (Risk Matrix)

ตารางที่ ๓-๑ แสดงอันตรายภาคขึ้น ระดับความเสี่ยง แลปสี และความหมายของความเสี่ยงแต่ละชั้น

อันตรายภาคขึ้น	ระดับความเสี่ยง	แลปสี	ความหมาย
๑๕ - ๒๕	สูงมาก		ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้ลดลงมาอยู่ในระดับที่ยอมรับได้โดยทันที
๘ - ๑๔	สูง		ระดับที่ไม่สามารถยอมรับได้ ต้องมีการควบคุมและติดตามความเสี่ยงเพื่อไม่ให้เคลื่อนย้ายไประดับสูงมาก
๔ - ๗	ปานกลาง		ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเพิ่มระดับไปสู่ระดับที่ยอมรับไม่ได้
๑ - ๓	ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องมีการควบคุมความเสี่ยงหรือไม่ต้องการจัดการเพิ่มเติม

ตารางที่ ๓-๒ การทบทวนและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

ที่	กิจกรรม/ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับความเสี่ยง
๑. ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)					
๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑	๕	๕	 (ปานกลาง)
๒	ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๓	๓	๙	 (สูง)
๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และระบบเครือข่ายคอมพิวเตอร์ของ สนข.	๒	๑	๒	 (ต่ำ)
๔	เกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕	 (ปานกลาง)
๕	การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๑	๕	๕	 (ปานกลาง)
๒. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)					
๖	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์ เทคโนโลยีและการสื่อสาร	๑	๔	๔	 (ปานกลาง)
๗	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สนข.	๑	๕	๕	 (ปานกลาง)
๘	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓	 (ต่ำ)

ที่	กิจกรรม/ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับความเสี่ยง
๙	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๑	๒	๒	 (ต่ำ)
๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	๒	๒	 (ต่ำ)
๑๑	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑	๑	๑	 (ต่ำ)
๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๓	๓	 (ต่ำ)
๑๓	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่ายหรือระบบฐานข้อมูลไม่เพียงพอ	๒	๒	๔	 (ปานกลาง)
๑๔	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับหรือไม่สามารถให้บริการได้	๒	๓	๖	 (ปานกลาง)
๓. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)					
๑๕	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๓	๕	๑๕	 (สูง)
๑๖	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๓	๕	๑๕	 (สูง)
๑๗	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษาหรือเกิดช่องโหว่ของโปรแกรม	๒	๓	๖	 (ปานกลาง)
๑๘	ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	๕	๓	๑๕	 (สูง)
๔. ความเสี่ยงด้านระบบข้อมูล (Database Risk)					
๑๙	ข้อมูลสำคัญรั่วไหล	๒	๔	๘	 (สูง)
๕. ความเสี่ยงด้านบุคลากร (Human Risk)					
๒๐	การนำเข้าข้อมูลผิดพลาดไม่ครบถ้วนหรือไม่เป็นปัจจุบัน	๑	๓	๓	 (ต่ำ)
๒๑	การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓	 (ต่ำ)
๒๒	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ไม่เพียงพอ	๑	๒	๒	 (ต่ำ)

ที่	กิจกรรม/ความเสี่ยง	โอกาส	ผลกระทบ	คะแนน	ระดับ ความเสี่ยง
๒๓	ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๔	๒	๘	 (สูง)
๒๔	การเชื่อมอีเมลหรือหน้าเว็บไซต์ปลอม เพื่อหลอกลวง (Mail Phishing)	๓	๒	๖	 (ปานกลาง)
๒๕	การโดนดักจับข้อมูลจากการใช้เครือข่าย เดียวกันกับบุคคลน่าสงสัย	๑	๒	๒	 (ต่ำ)
๒๖	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕	 (ปานกลาง)
๖. ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)					
๒๗	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑	๒	๒	 (ต่ำ)
๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ ตามแผนดิจิทัลฯ	๑	๑	๑	 (ต่ำ)
๒๙	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบ ไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑	๑	๑	 (ต่ำ)
๓๐	ไม่สามารถปฏิบัติตามกฎหมาย และระเบียบ ที่เกี่ยวข้อง	๑	๑	๑	 (ต่ำ)
๓๑	การเปลี่ยนแปลงนโยบายด้านเทคโนโลยี สารสนเทศของหน่วยงาน	๑	๑	๑	 (ต่ำ)

๓.๔ การบ่งชี้และระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Register) ของ สนข.

ตารางที่ ๓-๓ การระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Register) ของ สนข.

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)			
๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑. ไฟไหม้จากอุบัติเหตุไฟฟ้า ลัดวงจร หรือการวางเพลิง ๒. ภัยที่เกิดจากธรรมชาติ เช่น พายุ ๓. นำเข้าหรือมีวัสดุไวไฟ เช่น แอลกอฮอล์ ภายในห้อง ปฏิบัติการศูนย์ข้อมูล	๑. เครื่องคอมพิวเตอร์แม่ข่ายและ อุปกรณ์เครือข่ายต่าง ๆ เสียหาย ๒. สูญเสียข้อมูลสำคัญที่เก็บอยู่ ภายในเครื่องคอมพิวเตอร์แม่ข่าย ๓. ระบบสารสนเทศของหน่วยงาน ไม่สามารถให้บริการได้ (ล่ม) ๔. สูญเสียงบประมาณในการจัดซื้อ เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายใหม่ทดแทน ๕. เสียเวลาในการติดตั้งระบบ และกู้คืนข้อมูลใหม่ ๖. การดำเนินงานหยุดชะงัก จนไม่สามารถปฏิบัติงานต่อได้ ส่งผลให้แล้วเสร็จไม่ทัน ตามกำหนดเวลา
๒	ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ	๑. ไฟฟ้าขัดข้อง/ลัดวงจร ๒. แรงดันไฟฟ้าไม่คงที่ ๓. ไฟฟ้ากระชาก ๔. ภัยที่เกิดจากธรรมชาติ เช่น พายุ	๑. เครื่องคอมพิวเตอร์แม่ข่ายและ อุปกรณ์เครือข่ายต่าง ๆ เสียหาย จากการหยุดทำงานกะทันหัน ๒. อุปกรณ์ฮาร์ดดิสก์ภายในเครื่อง คอมพิวเตอร์แม่ข่ายเสียหาย ส่งผลให้สูญเสียข้อมูลภายใน ฮาร์ดดิสก์ ๓. ระบบสารสนเทศของหน่วยงาน ไม่สามารถให้บริการได้ (ล่ม) ๔. เสียเวลาในการกู้คืนข้อมูลใหม่ ๕. การดำเนินงานหยุดชะงัก จนไม่สามารถปฏิบัติงานต่อ ได้ ส่งผลให้แล้วเสร็จไม่ทัน ตามกำหนดเวลา
๓	การควบคุมอุณหภูมิ/ความชื้น ภายในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และเครือข่าย คอมพิวเตอร์ของ สนข.	๑. ไฟฟ้าดับ ๒. เครื่องปรับอากาศเสีย/หยุด ทำงาน/ไม่มีความเย็น ๓. ความชื้นไม่เหมาะสม	๑. ห้องเซิร์ฟเวอร์มีอุณหภูมิสูงส่งผล ให้เครื่องคอมพิวเตอร์แม่ข่ายร้อน จนหยุดทำงาน ๒. เกิดความเสียหายขึ้นกับอุปกรณ์ อิเล็กทรอนิกส์ในห้องปฏิบัติการ ศูนย์ข้อมูล (Data Center) และเครือข่ายคอมพิวเตอร์

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
			๓. การดำเนินงานหยุดชะงัก จนไม่สามารถปฏิบัติงานต่อได้ ส่งผลให้แล้วเสร็จไม่ทันตาม กำหนดเวลาจนไม่สามารถ ปฏิบัติงานต่อได้ ส่งผลให้แล้ว เสร็จไม่ทันตามกำหนดเวลา
๔	เกิดสถานการณ์ภัยพิบัติ/ ความไม่สงบทางการเมือง/ชุมนุม ประท้วง	๑. การชุมนุมประท้วง ๒. การจลาจล ๓. การก่อการร้าย ๔. ภัยที่เกิดจากธรรมชาติ	๑. เจ้าหน้าที่ไม่สามารถเข้าไป ปฏิบัติงานได้ตามปกติ เนื่องจาก ถูกปิดล้อมสถานที่ทำงาน ๒. ระบบงานหยุดทำงานไม่สามารถ ให้บริการได้ ๓. จำเป็นต้องเข้าระบบงาน จากระยะไกล (Remote)
๕	การถูกบุกรุกหรือเข้าถึงพื้นที่ หวงห้าม	๑. ผู้ไม่มีสิทธิ์เข้าถึงระบบ คอมพิวเตอร์แม่ข่าย อุปกรณ์ สารสนเทศ ข้อมูลสารสนเทศ ข้อมูลสำคัญ หรือความลับ ๒. ถูกคัดลอก แก้ไข ลบ หรือถูก ขโมยข้อมูล	๑. ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศ ไม่สามารถ ให้บริการต่อเนื่องได้ ๒. อุปกรณ์ฮาร์ดแวร์ได้รับความ เสียหายร้ายแรง
ความเสี่ยงด้านระบบเครือข่ายและความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Hardware and Data Communication Risk)			
๖	ไม่มีการควบคุม/จัดทำบัญชี/ ปรับปรุงบัญชีทรัพย์สินของ อุปกรณ์เทคโนโลยีและการสื่อสาร	๑. ไม่มีการควบคุมบัญชี ทรัพย์สินของอุปกรณ์ เทคโนโลยีและการสื่อสาร	๑. ครุภัณฑ์คอมพิวเตอร์ ครุภัณฑ์ เครือข่าย หรืออุปกรณ์สูญหาย
๗	ขาดแผนรองรับระบบฮาร์ดแวร์ ภายในศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ สนข.	๑. ไม่มีการกำหนดแผนรองรับ อุปกรณ์เครือข่าย และ ระบบแม่ข่ายของ สนข.	๑. ระบบข้อมูลเสียหาย/ถูกทำลาย หรือระบบสารสนเทศ ไม่สามารถให้บริการต่อเนื่องได้ เมื่อเกิดข้อผิดพลาด ด้านฮาร์ดแวร์ หรือฮาร์ดแวร์ ได้รับความเสียหายร้ายแรง
๘	ขาดการบริหารจัดการสิทธิ์ การใช้งานอุปกรณ์เทคโนโลยี สารสนเทศและการสื่อสาร ในทุก ๆ ระดับ ของผู้ใช้งาน	๑. ไม่มีการควบคุมสิทธิการใช้งาน ของอุปกรณ์เทคโนโลยี สารสนเทศ	๑. เกิดความผิดพลาดในการ ให้บริการระบบสารสนเทศ และการสื่อสารทั้งระบบ ๒. ไม่สามารถระบุตัวตนผู้ใช้งานได้ ๓. ไม่สามารถหาผู้กระทำความผิดได้
๙	ระบบเครือข่ายไม่เพียงพอ ต่อการให้บริการ	๑. การขัดข้องของผู้ให้บริการ อินเทอร์เน็ต (ISP) ๒. IP Address ไม่เพียงพอ สำหรับผู้ใช้งาน ๓. ปริมาณการรับ - ส่งข้อมูล (Bandwidth) ไม่เพียงพอ สำหรับการใช้งาน	๑. ผู้ให้บริการอินเทอร์เน็ตขัดข้อง ๒. IP Address ไม่เพียงพอสำหรับ ผู้ใช้งาน ๓. ปริมาณการรับ-ส่ง ข้อมูล (Bandwidth) ไม่เพียงพอต่อ การใช้งาน

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑. ความเสี่ยงด้านการบริหารจัดการ หรือจากเจ้าหน้าที่ผู้ปฏิบัติงาน	๑. ไม่มีการควบคุมอุปกรณ์ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน ๒. มีจำนวนบุคลากรเพิ่มขึ้น ทำให้การจัดการไม่ครอบคลุม
๑๑	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑. ครุภัณฑ์อุปกรณ์ไม่ได้มาตรฐานหรือตอบสนองได้ไม่ครอบคลุมกับการทำงาน ๒. การติดตั้งใช้งานไม่สมบูรณ์	๑. เกิดความเสียหายจากการใช้งานครุภัณฑ์ ๒. ติดตั้งใช้งานได้ไม่สมบูรณ์ ๓. การทำงานล่าช้า
๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑. ไม่มีการกำหนดวิธีการรักษาความปลอดภัยจากการปฏิบัติงานจากระยะไกล	๑. อาจถูกลักลอบขโมยข้อมูลหรือข้อมูลถูกทำลายทำให้เกิดความสูญเสีย ๒. ไม่มีผู้รับผิดชอบ เนื่องจากไม่สามารถยืนยันตัวตนของผู้ที่ใช้งานทำให้เกิดความเสียหายได้ต่อระบบ ๓. ถูกโจมตีระบบทำให้ไม่สามารถให้บริการได้
๑๓	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	๑. ไม่มีการวางแผนการดำเนินโครงการ และอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน ๒. ผู้ใช้งานไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน	๑. การให้บริการระบบสารสนเทศหยุดชะงักส่งผลต่อการให้บริการระบบต่อประชาชนและผู้ใช้บริการทั่วไป
๑๔	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	๑. เสื่อมสภาพตามอายุการใช้งาน ๒. ถูกทำลายโดยผู้บุกรุก ๓. การตก หล่น ชน กระแทกจากการเคลื่อนย้าย หรือการติดตั้งไม่มั่นคงแน่นหนา ๔. เกิดจากระบบไฟฟ้าขัดข้อง	๑. เกิดความผิดพลาดในการให้บริการระบบสารสนเทศ ๒. ระบบข้อมูลเสียหาย/ถูกทำลายหรือไม่สามารถให้บริการต่อเนื่องได้ ๓. ระบบสารสนเทศของหน่วยงานไม่สามารถให้บริการได้สูญเสียข้อมูลสำคัญที่เก็บอยู่ภายในเครื่องคอมพิวเตอร์แม่ข่าย
ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)			
๑๕	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๑. ถูกบุคคลที่ไม่มีสิทธิ์หรือไม่มีอำนาจเจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ๒. ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์ ๓. ไม่มีการดำเนินการตามแผนสำรองข้อมูล และกู้คืนข้อมูลและระบบฐานข้อมูล	๑. ข้อมูลถูกเปลี่ยนแปลง หรือถูกทำลาย ๒. ทำให้ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้ ๓. ทรัพยากรในระบบถูกนำไปใช้ ทำให้ประสิทธิภาพของระบบลดลง ๔. ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
		๔. เกิดช่วงโหว่ของซอฟต์แวร์ ที่ใช้งาน ๕. ไม่มีแผนรับรองสถานการณ์ ฉุกเฉิน (IT Contingency Plan)	
๑๖	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๑. ถูกบุคคลที่ไม่มีสิทธิ์หรือ ไม่มีอำนาจเจาะระบบ หรือลักลอบ (Hack) เข้าสู่ ระบบฐานข้อมูล (Database) ๒. ขาดการป้องกันและตรวจจับ ไวรัสคอมพิวเตอร์ ๓. ไม่มีการดำเนินการตามแผน สำรองข้อมูล และกู้คืนข้อมูล และระบบฐานข้อมูล ๔. เกิดช่วงโหว่ของซอฟต์แวร์ ที่ใช้งาน ๕. ไม่มีแผนรับรองสถานการณ์ ฉุกเฉิน (IT Contingency Plan)	๑. การให้บริการระบบสารสนเทศ หยุดชะงักส่งผลกระทบต่อให้บริการ ระบบต่อประชาชนและผู้ใช้ บริการทั่วไป ๒. ข้อมูลสารสนเทศและการทำงาน ของระบบเสียหาย ส่งผลให้มี การประมวลผลไม่ถูกต้อง ครบถ้วน ๓. ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข ๔. ขาดความน่าเชื่อถือและให้บริการ ไม่มีประสิทธิภาพ
๑๗	เกิดช่องโหว่ของซอฟต์แวร์ ขาดการบำรุงรักษา หรือ เกิดช่องโหว่ของโปรแกรม	๑. ไม่มีการอัปเดตซอฟต์แวร์ ให้เป็นปัจจุบัน ๒. ไม่มีการบำรุงรักษาโปรแกรม อย่างต่อเนื่อง	๑. ระบบสารสนเทศไม่ได้รับ การปรับปรุงให้มีความทันสมัย หรือความปลอดภัยตามที่ ผู้พัฒนาระบบได้กำหนด ๒. ทำให้มีความเสี่ยงจาก การถูกบุกรุกโจมตีได้ ๓. อาจเกิดข้อขัดข้องจนระบบ ไม่สามารถทำงานได้ อันเกิดจาก ไม่มีการอัปเดตเวอร์ชันใหม่ ๆ ๔. อย่างสม่ำเสมอทำให้ไม่สามารถ ใช้ระบบได้อย่างต่อเนื่อง
๑๘	ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	๑. การใช้งานโปรแกรมที่ละเมิด ลิขสิทธิ์จากโปรแกรม ประเภทไวรัส หรือมัลแวร์ ๒. ผิดกฎหมาย	๑. หน่วยงาน/บุคคลต้องรับผิดชอบ ค่าปรับในคดีละเมิดลิขสิทธิ์ ทรัพย์สินทางปัญญา ๒. เกิดภัยคุกคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิดลิขสิทธิ์
ความเสี่ยงด้านระบบข้อมูล (Database Risk)			
๑๙	ข้อมูลสำคัญรั่วไหล	๑. เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลถูกโจมตี จากโปรแกรมประเภทไวรัส หรือมัลแวร์	๑. มีข้อมูลสำคัญสูญหาย หรือ หลุดรั่วไปยังภายนอกหน่วยงาน ๒. อาจถูกดำเนินคดีหรือถูกฟ้อง เรียกค่าเสียหายร่วมด้วย

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
		๒. นำเครื่องคอมพิวเตอร์เก่า กลับมาใช้ใหม่ ๓. ถูกโจมตีหรือถูกเจาะระบบ (Hack)	๓. หน่วยงานเสื่อมเสียชื่อเสียง และความน่าเชื่อถือ
ความเสี่ยงด้านบุคลากร (Human Risk)			
๒๐	การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือไม่เป็นปัจจุบัน	๑. การนำเข้าข้อมูลที่ไม่ถูกต้อง เข้าสู่ระบบ ๒. ระบบมีความผิดพลาด (Bug) ๓. การนำเข้าข้อมูลที่ไม่ถูกต้อง เข้าสู่ระบบ ๔. ไม่มีการตรวจสอบและ ปรับปรุงข้อมูลให้เป็นปัจจุบัน	๑. ข้อมูลไม่มีคุณภาพ ๒. ไม่สามารถออกรายงานได้ ๓. ไม่สามารถเชื่อมโยงข้อมูลได้ ๔. ไม่สามารถออกรายงานได้ถูกต้อง และเป็นปัจจุบัน
๒๑	การจ้างบุคคลภายนอกที่ขาด ความรู้ ความชำนาญ ความเชี่ยวชาญในการดูแล บำรุงรักษาระบบ/พัฒนาระบบ	๑. ระบบเกิดปัญหา ขัดข้อง ๒. การให้บริการติดขัด ล่าช้า ๓. อุปกรณ์หรือระบบสารสนเทศ เสียหาย ๔. ไม่สามารถให้บริการได้	๑. ระบบมีข้อผิดพลาดและ ไม่เป็นไปตามแผน ๒. เสียเวลาในการแก้ไขปัญหา ๓. เกิดความผิดพลาดในการทำงาน ทำให้ระบบทำงานบกพร่อง ๔. ไม่สามารถแก้ไขปัญหา ที่เกิดขึ้นได้ หรือแก้ไขได้ล่าช้า ๕. เกิดความเสียหายแก่ระบบ หรือ หน่วยงาน
๒๒	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ไม่เพียงพอ	๑. ขาดการอบรมบุคลากร ด้านไอที ๒. หน่วยงานขาดบุคลากร ด้านไอที	๑. เกิดความผิดพลาดในการใช้ระบบ ส่งผลทำให้การทำงาน ของระบบบกพร่อง และอาจเกิด ความเสียหายทั้งระบบได้ ๒. งบประมาณที่ใช้ในการบำรุงรักษา มีปริมาณเพิ่มขึ้นทุกปี ๓. อาจเกิดความเสียหายแก่ระบบ หรือหน่วยงาน
๒๓	ผู้ใช้งาน (User) ไม่มีความรู้ ความชำนาญ และทักษะ การใช้งานระบบ	๑. ไม่มีการอบรมการใช้งาน ระบบแก่ผู้ใช้งาน ๒. ระบบมีความซับซ้อนยาก ต่อการใช้งาน	๑. การใช้ระบบงานไม่เป็นไป ตาม Workflow ที่กำหนดทำให้ เกิดข้อขัดข้อง ไม่สามารถ แก้ไข ปัญหาด้วยตัวเองในเบื้องต้นได้ ๒. ความล่าช้าในการปฏิบัติงานและ เพิ่มปริมาณงานให้กับผู้ดูแลระบบ ๓. การปฏิบัติงานผิดพลาด คลาดเคลื่อน จนทำให้ขาดความ น่าเชื่อถือ
๒๔	การเชื่อมโยงอีเมลหรือหน้าเว็บไซต์ ปลอมเพื่อหลอกลวง (Mail Phishing)	๑. การเปิดไฟล์ หรือ URL ที่แนบมากับอีเมลที่น่าสงสัย ๒. การหลงเชื่อเว็บไซต์ปลอม	๑. โดนหลอกลวงเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูล ที่เป็นความลับ

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
		๓. ให้ข้อมูลส่วนตัวหรือลงโปรแกรมที่มาจากแหล่งที่ไม่น่าเชื่อถือ	๒. โดนหลอกเพื่อติดตั้งไวรัสลงบนคอมพิวเตอร์ หรือคอมพิวเตอร์แม่ข่าย
๒๕	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	๑. การเข้าใช้งานระบบจากระยะไกลด้วยเครือข่ายที่ไม่น่าเชื่อถือ ๒. การให้บุคคลที่น่าสงสัยมาใช้งานระบบเครือข่ายเดียวกัน	๑. โดนดักเก็บข้อมูลการดำเนินการ เช่น รหัสผ่าน ข้อมูลสำคัญ ข้อมูลที่เป็นความลับ ๒. เกิดความผิดพลาดในการให้บริการระบบสารสนเทศ และการสื่อสารทั้งระบบ ๓. ไม่สามารถระบุตัวตนผู้ใช้งาน/หาผู้กระทำความผิดไม่ได้
๒๖	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๑. ผู้ใช้งานลืมนอกจากระบบ ๒. ผู้ใช้งานละเลยเรื่องความปลอดภัยของระบบ	๑. ข้อมูลสูญหาย ๒. อาจถูกผู้ไม่หวังดีเข้าใช้ระบบ ๓. ระบบงานเกิดความผิดพลาดในการให้บริการ ๔. ไม่สามารถระบุตัวตนผู้ใช้งาน หรือหาผู้กระทำความผิดได้
ความเสี่ยงในด้านการบริหารจัดการ (Management Risk)			
๒๗	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑. โดนตัด/ปรับลดงบประมาณในการดำเนินโครงการตามนโยบายการปรับลดเงินเป็นร้อยละ ทำให้โครงการที่จำเป็นต้องดำเนินการโดนตัดหรือปรับลดไปด้วย	๑. อาจต้องลดระยะเวลา ลดคุณภาพ หรือประสิทธิภาพของงานหรือโครงการที่โดนตัดหรือปรับลดงบประมาณ ๒. ไม่ได้ดำเนินโครงการตามเป้าที่วางไว้ ๓. งบประมาณ และงานที่ปรับ อาจไม่สอดคล้องกัน ๔. ไม่ได้จัดหาอุปกรณ์หรือครุภัณฑ์ทดแทน ทำให้การปฏิบัติงานมีประสิทธิภาพลดลง
๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัล	๑. ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัลได้	๑. ผู้บริหารปรับลดระยะเวลาดำเนินโครงการ ๒. ไม่สามารถดำเนินงานให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด
๒๙	กระบวนการจัดซื้อจัดจ้าง การบำรุงรักษาระบบไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑. ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที ๒. การดำเนินการโครงการล่าช้า ๓. การเปลี่ยนแปลงวิธีการระหว่างการดำเนินการ	๑. เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง ๒. อนุมัติโครงการล่าช้า ๓. ไม่สามารถหาผู้รับจ้างได้ตามแผนการดำเนินการ ๔. ไม่สามารถเบิกจ่ายงบประมาณตามแผนการเบิกจ่ายงบประมาณรายจ่ายประจำปีส่งผลกระทบต่อ การรายงานผลตัวชี้วัดขององค์กร

ลำดับ ที่	ความเสี่ยง	ปัจจัยเสี่ยง	ความเสียหาย
๓๐	ไม่สามารถปฏิบัติตามกฎหมาย และระเบียบที่เกี่ยวข้อง	๑. กฎหมาย/ระเบียบที่เกี่ยวข้อง กับการปฏิบัติงาน ด้านเทคโนโลยีสารสนเทศ มีผลบังคับใช้ ๒. ไม่สามารถดำเนินการ ตามกฎหมาย/ระเบียบ ที่เกี่ยวข้องได้ทันภายในระยะ เวลาที่กำหนด	๑. การดำเนินงานไม่สามารถรองรับ การปฏิบัติงานตามกฎหมาย/ ระเบียบที่บังคับใช้ได้ ๒. ไม่มีระบบสารสนเทศรองรับ การดำเนินงานตามที่กฎหมาย กำหนด
๓๑	การเปลี่ยนแปลงนโยบาย ด้านเทคโนโลยีสารสนเทศ ของหน่วยงาน	๑. การปรับเปลี่ยนตำแหน่งงาน ๒. การปรับเปลี่ยนบุคลากร ๓. การเปลี่ยนแปลงนโยบาย ด้านเทคโนโลยีสารสนเทศ ของหน่วยงาน	๑. การดำเนินงานล่าช้า ติดขัด

๓.๕ ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข.

ตารางที่ ๓-๔ ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ลำดับที่	ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๑	ละเมิดลิขสิทธิ์โปรแกรมหรือประโยชน์ (Utilities Program)	๕	๓	๑๕	 (สูงมาก)
๒	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๓	๕	๑๕	 (สูงมาก)
๓	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๓	๕	๑๕	 (สูงมาก)
๔	ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๓	๓	๙	 (สูง)
๕	ข้อมูลสำคัญรั่วไหล	๒	๔	๘	 (สูง)

ลำดับที่	ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๖	ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๔	๒	๘	 (สูง)
๗	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	๒	๓	๖	 (ปานกลาง)
๘	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	๒	๓	๖	 (ปานกลาง)
๙	การเชื่อมต่ออีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๓	๒	๖	 (ปานกลาง)
๑๐	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑	๕	๕	 (ปานกลาง)
๑๑	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ภัยพิบัติ/ ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕	 (ปานกลาง)
๑๒	การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๑	๕	๕	 (ปานกลาง)
๑๓	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการ ระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ สนข.	๑	๕	๕	 (ปานกลาง)
๑๔	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕	 (ปานกลาง)
๑๕	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สิน ของอุปกรณ์ เทคโนโลยีและการสื่อสาร	๑	๔	๔	 (ปานกลาง)
๑๖	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบ ฐานข้อมูลไม่เพียงพอ	๒	๒	๔	 (ปานกลาง)
๑๗	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์ เทคโนโลยีสารสนเทศในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓	 (ต่ำ)

ลำดับที่	ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๑๘	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงาน จากระยะไกลไม่ทั่วถึง	๑	๓	๓	 (ต่ำ)
๑๙	การนำเข้าข้อมูลผิดพลาดไม่ครบถ้วน หรือ ไม่เป็นปัจจุบัน	๑	๓	๓	 (ต่ำ)
๒๐	การจ้างบุคคลภายนอก ที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓	 (ต่ำ)
๒๑	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการ ศูนย์ข้อมูล (Data Center) และระบบเครือข่าย คอมพิวเตอร์ของ สนข.	๒	๑	๒	 (ต่ำ)
๒๒	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๑	๒	๒	 (ต่ำ)
๒๓	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ไม่เพียงพอ	๑	๒	๒	 (ต่ำ)
๒๔	การโดนดักจับข้อมูลจากการใช้เครือข่ายเดียวกัน กับบุคคลน่าสงสัย	๑	๒	๒	 (ต่ำ)
๒๕	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑	๒	๒	 (ต่ำ)
๒๖	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์ สื่อสารเคลื่อนที่	๑	๑	๑	 (ต่ำ)
๒๗	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ ไม่เหมาะสมกับลักษณะงาน	๑	๑	๑	 (ต่ำ)
๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัลฯ	๑	๑	๑	 (ต่ำ)
๒๙	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบ ไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑	๑	๑	 (ต่ำ)

ลำดับที่	ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๓๐	ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	๑	๑	๑	 (ต่ำ)
๓๑	การเปลี่ยนแปลงนโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน	๑	๑	๑	 (ต่ำ)

๓.๖ สรุปผลการประเมินและแนวทางควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ตารางที่ ๓-๕ สรุปผลการประเมินและแนวทางควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
๑. ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	๑. การใช้งานโปรแกรมที่ละเมิด ลิขสิทธิ์จากโปรแกรมประเภท ไวรัส หรือมัลแวร์ ๒. ผิดกฎหมาย	๑. หน่วยงาน/บุคคลต้อง รับผิดชอบค่าปรับในคดีละเมิด ลิขสิทธิ์ทรัพย์สินทางปัญญา ๒. เกิดภัยคุกคามจากไวรัส เช่น Malware ได้แก่ ไวรัส Trojan แฝงมากับโปรแกรมละเมิด ลิขสิทธิ์	 (สูงมาก)	<ul style="list-style-type: none">- สร้างความตระหนัก ในเรื่องนโยบายและแนว ปฏิบัติความมั่นคงปลอดภัย ด้านสารสนเทศและการใช้งาน ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง ตามกฎหมาย- กระตุ้นให้เกิดการปฏิบัติ ตามแนวนโยบายหรือ ระเบียบฯ อย่างจริงจัง- ส่งเสริมให้ใช้โปรแกรม อรรถประโยชน์แบบ OpenSource แทนโปรแกรม ที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์- จัดหาโปรแกรมที่มีลิขสิทธิ์ ถูกต้องตามกฎหมาย	ศทท.	เร่งจัดการ ความเสี่ยง ให้อยู่ในระดับ ที่ยอมรับได้
๒. ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๑. ถูกบุคคลที่ไม่มีสิทธิ์หรือ ไม่มีอำนาจเจาะระบบหรือ ลักลอบ (Hack) เข้าสู่เครื่อง คอมพิวเตอร์แม่ข่าย (Server) ๒. ขาดการป้องกันและตรวจจับ ไวรัสคอมพิวเตอร์	๑. ข้อมูลถูกเปลี่ยนแปลงหรือ ถูกทำลาย ๒. ทำให้ไม่สามารถเข้าถึงข้อมูล และระบบคอมพิวเตอร์ได้ ๓. ทรัพยากรในระบบถูกนำไปใช้ ทำให้ประสิทธิภาพของระบบ ลดลง	 (สูงมาก)	<ul style="list-style-type: none">- มีการติดตั้งอุปกรณ์รักษา ความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall- ตรวจสอบการตั้งค่าของ อุปกรณ์รักษาความปลอดภัย ระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ	ศทท.	เร่งจัดการ ความเสี่ยง ให้อยู่ในระดับ ที่ยอมรับได้

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางการจัดการ/ กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
	๓. ไม่ดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล ๔. เกิดช่วงโหว่ของซอฟต์แวร์ที่ใช้งาน ๕. ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)	๔. ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ		- ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ		
๓. ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๑. ถูกบุคคลที่ไม่มีสิทธิ์หรือไม่มีอำนาจ เจาะระบบหรือลักลอบ (Hack) เข้าสู่ ระบบฐานข้อมูล (Database) ๒. ขาดการป้องกันและตรวจจับไวรัสคอมพิวเตอร์ ๓. ไม่ดำเนินการตามแผนสำรองข้อมูลและกู้คืนข้อมูลและระบบฐานข้อมูล ๔. เกิดช่วงโหว่ของซอฟต์แวร์ที่ใช้งาน ๕. ไม่มีแผนรับรองสถานการณ์ฉุกเฉิน (IT Contingency Plan)	๑. การให้บริการระบบสารสนเทศหยุดชะงักส่งผลกระทบต่อการทำงานของระบบฯ ต่อประชาชนและผู้ใช้บริการทั่วไป ๒. ข้อมูลสารสนเทศและการทำงานของระบบเสียหายส่งผลให้มีการประมวลผลไม่ถูกต้องครบถ้วน ๓. ไฟล์ข้อมูลถูกเปลี่ยนแปลงแก้ไข ๔. ขาดความน่าเชื่อถือและให้บริการไม่มีประสิทธิภาพ	 (สูงมาก)	- มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส	ศทท.	เร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/ กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
				<ul style="list-style-type: none"> - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ทดสอบช่องโหว่ของโปรแกรม - กำหนดมาตรฐานในการพัฒนาโปรแกรมให้มีความปลอดภัย 		
๔. ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๑. ไฟฟ้าขัดข้อง/ลัดวงจร ๒. แรงดันไฟฟ้าไม่คงที่ ๓. ไฟฟ้ากระชาก ๔. ภัยที่เกิดจากธรรมชาติ เช่น ฟ้าผ่าฯ	๑. ทำให้ระบบเครือข่ายเครื่องคอมพิวเตอร์แม่ข่ายเครื่องคอมพิวเตอร์ลูกข่ายและระบบฐานข้อมูลหยุดทำงาน ๒. เกิดความเสียหายไม่สามารถให้บริการได้	 (สูง)	<ul style="list-style-type: none"> - ตรวจสอบระบบสำรองไฟฟ้า (UPS) สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ - มีการจัดจ้างผู้เชี่ยวชาญเพื่อดำเนินการบำรุงรักษา 	ศทท.	ควบคุมและติดตามความเสี่ยง
๕. ข้อมูลสำคัญรั่วไหล	๑. เครื่องคอมพิวเตอร์แม่ข่ายหรือระบบฐานข้อมูลถูกโจมตีจากโปรแกรมประเภทไวรัสหรือมัลแวร์ ๒. นำเครื่องคอมพิวเตอร์เก่ากลับมาใช้ใหม่	๑. ข้อมูลสำคัญสูญหาย หรือหลุดรั่วไปยังภายนอกหน่วยงาน ๒. อาจถูกดำเนินคดีหรือถูกฟ้องเรียกค่าเสียหายร่วมด้วย ๓. หน่วยงานเสื่อมเสียชื่อเสียงและความน่าเชื่อถือ	 (สูง)	<ul style="list-style-type: none"> - มีระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์ ระบบเครือข่ายระบบสารสนเทศ - มีกระบวนการทบทวนสิทธิผู้ใช้งานเป็นประจำ 	ศทท.	ควบคุมและติดตามความเสี่ยง

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
	๓. ถูกโจมตีหรือถูกเจาะระบบ (Hack)			<ul style="list-style-type: none"> - มีการเก็บประวัติการใช้งานคอมพิวเตอร์ - มีกระบวนการบริหารจัดการคอมพิวเตอร์และอุปกรณ์ - มีแนวปฏิบัติในการลบหรือทำลายข้อมูลหลังจากไม่ได้ใช้งาน 		
๖. ผู้ใช้งาน (Users) ไม่มีความรู้ความชำนาญ และทักษะการใช้งานระบบ	๑. ไม่มีการอบรมการใช้งานระบบแก่ผู้ใช้งาน ๒. ระบบมีความซับซ้อนยากต่อการใช้งาน	๑. การใช้ระบบงานไม่เป็นไปตาม Workflow ที่กำหนดทำให้เกิดข้อขัดข้อง ไม่สามารถแก้ไขปัญหาด้วยตัวเองในเบื้องต้นได้ ๒. ความล่าช้าในการปฏิบัติงานและเพิ่มปริมาณงานให้กับผู้ดูแลระบบ ๓. การปฏิบัติงานผิดพลาดคลาดเคลื่อน จนทำให้ขาดความน่าเชื่อถือ	 (สูง)	<ul style="list-style-type: none"> - อบรมการใช้งานระบบ - จัดทำคู่มือสำหรับการใช้งานระบบ - ให้มีเจ้าหน้าที่สำหรับให้คำปรึกษาเกี่ยวกับการใช้งานระบบ และช่วยแก้ไขปัญหาให้ผู้ใช้งาน 	ศทท.	ควบคุมและติดตามความเสี่ยง
๗. เกิดช่องโหว่ของซอฟต์แวร์ ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	๑. ไม่มีการอัปเดตซอฟต์แวร์ให้เป็นปัจจุบัน ๒. ไม่มีการบำรุงรักษาโปรแกรมอย่างต่อเนื่อง	๑. ระบบสารสนเทศไม่ได้รับการปรับปรุงให้ทันสมัยหรือปลอดภัย ๒. เกิดความเสี่ยงที่จะถูกบุกรุกโจมตี ๓. เกิดข้อขัดข้องจนระบบไม่สามารถใช้งานได้	 (ปานกลาง)	<ul style="list-style-type: none"> - ติดตั้ง Patch ของระบบปฏิบัติการ - Update Software ระบบต่าง ๆ อย่างสม่ำเสมอ - ติดตามข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์เป็นประจำ 	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
		๔. ระบบงานไม่ปลอดภัย		- มีการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง		
๘. เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	๑. เสื่อมอายุตามการใช้งาน ๒. ถูกทำลายจากผู้บุกรุก ๓. การตก หล่น กระแทกจากการเคลื่อนย้ายหรือการติดตั้งที่ไม่มั่นคง ๔. เกิดจากระบบไฟฟ้าขัดข้อง	๑. เกิดความผิดพลาดในการให้บริการ ๒. ระบบสารสนเทศเสียหายหรือไม่สามารถให้บริการต่อเนื่องได้ ๓. ข้อมูลสำคัญที่จัดเก็บอยู่เสียหายหรือสูญหาย	 (ปานกลาง)	- มีแผนการบำรุงรักษา ตรวจสอบ และซ่อมแซม แก๊ซครักเก็ตคอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการจ้างผู้เชี่ยวชาญภายนอก (Outsource) ที่มีความเชี่ยวชาญเพื่อบำรุงรักษาระบบ - มีการบำรุงรักษาโปรแกรมและระบบงานอย่างต่อเนื่อง	ศทท.	
๙. การเชื่อมอีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๑. การเปิดไฟล์หรือ URL ที่แนบมากับอีเมล ๒. การหลงเชื่อเข้าเว็บปลอม ๓. ให้ข้อมูลส่วนตัวหรือลงโปรแกรมที่มาจากแหล่งที่ไม่น่าเชื่อถือ	๑. โดนหลอกเพื่อขอรหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลความลับ ๒. โดนหลอกให้ติดตั้งไวรัสลงบนเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย	 (ปานกลาง)	- จัดอบรมให้ความตระหนักรู้แก่เจ้าหน้าที่ในองค์กร - มีการแจ้งข่าวสารให้เจ้าหน้าที่ในองค์กรทราบเมื่อมีการพบเจออีเมลหรือหน้าเว็บไซต์หลอกลวง	ศทท.	
๑๐. ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑. ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจรหรือการวางเพลิง ๒. ภัยที่เกิดจากธรรมชาติ เช่น ฟ้าผ่าฯ ๓. นำเข้าหรือมีวัตถุไวไฟ เช่น แอลกอฮอล์ ภายในห้องปฏิบัติการศูนย์ข้อมูล	๑. เกิดความเสียหายต่อทรัพย์สิน ระบบเครือข่าย อุปกรณ์ และฐานข้อมูล ๒. ระบบคอมพิวเตอร์แม่ข่ายหยุดทำงาน ๓. การดำเนินงานหยุดชะงักทั้งระบบ	 (ปานกลาง)	- ตรวจสอบความพร้อมใช้งานของอุปกรณ์ดับเพลิงอัตโนมัติ สัญญาณเตือนภัยให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ - มีการจัดจ้างผู้เชี่ยวชาญเพื่อดำเนินการบำรุงรักษา	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
๑๑. เกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑. การชุมนุมประท้วง ๒. การจลาจล ๓. การก่อการร้าย ๔. ภัยที่เกิดจากธรรมชาติ เช่น อุทกภัย แผ่นดินไหว อัคคีภัย และवादภัย	๑. เจ้าหน้าที่ไม่สามารถเข้าปฏิบัติงานได้ตามปกติเนื่องจาก ถูกปิดล้อมสถานที่ทำงาน ๒. ระบบงานทั้งหมดหยุดชะงักไม่สามารถให้บริการได้ ๓. อุปกรณ์หรือฮาร์ดแวร์ได้รับความเสียหาย ๔. จำเป็นต้องเข้าระบบงานจากระยะไกล (Remote)	 (ปานกลาง)	- จัดทำ/ทบทวน แผนเตรียมความพร้อมกรณีเหตุฉุกเฉิน (IT Contingency Plan) ให้เป็นปัจจุบัน - จัดทำ/ทบทวน แผนบริหารความต่อเนื่อง Business Continuity Plan (BCP) ด้านสารสนเทศให้เป็นปัจจุบัน	ศทท.	
๑๒. การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๑. ผู้ไม่มีสิทธิ์เข้าถึงระบบคอมพิวเตอร์แม่ข่าย อุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ ข้อมูลสำคัญ หรือความลับ ๒. ถูกคัดลอก แก้ไข ลบ หรือถูกขโมยข้อมูล	๑. อุปกรณ์ฮาร์ดแวร์ ระบบงานสารสนเทศ หรือข้อมูลเสียหาย สูญหาย หรืออาจถูกทำลาย ๒. ไม่สามารถให้บริการระบบงานต่อเนื่องได้	 (ปานกลาง)	- มีการควบคุมทางกายภาพเพื่อควบคุมการเข้าถึงพื้นที่หวงห้าม เช่น ระบบ Access Control และระบบ CCTV	ศทท.	
๑๓. ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่ายและเครือข่ายคอมพิวเตอร์ สนข.	๑. ไม่มีการกำหนดแผนรองรับอุปกรณ์ฮาร์ดแวร์ และระบบคอมพิวเตอร์แม่ข่ายของ สนข.	๑. ระบบข้อมูลเสียหาย หรือถูกทำลาย หรือระบบสารสนเทศไม่สามารถให้บริการต่อเนื่องได้เมื่อเกิดข้อผิดพลาดด้านฮาร์ดแวร์ หรือฮาร์ดแวร์ได้รับความเสียหายร้ายแรง	 (ปานกลาง)	- มีแผนการบำรุงรักษา ตรวจสอบและซ่อมแซมแก้ไขครุภัณฑ์คอมพิวเตอร์และอุปกรณ์เป็นประจำ - มีการประชุมติดตามและรายงานผล - จัดทำการสำรองข้อมูลและกู้คืนระบบในรายการครุภัณฑ์ที่มีความสำคัญ	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
๑๔. ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๑. ผู้ใช้งานลืมนอกจากระบบงาน ๒. ผู้ใช้งานละเลยเรื่องความมั่นคงปลอดภัยในการใช้งานระบบ	๑. ข้อมูลสูญหาย ๒. อาจถูกผู้ไม่หวังดีเข้าใช้ระบบ ๓. ระบบงานเกิดความผิดพลาดในการให้บริการ ๔. ไม่สามารถระบุตัวตนผู้ใช้งานหรือหาผู้กระทำความผิดได้	 (ปานกลาง)	- มีการกำหนดให้ระบบทำการออกจากระบบเมื่อผู้ใช้ไม่มีการเคลื่อนไหวตามระยะเวลาที่กำหนด - อบรมและสร้างความตระหนักรู้ถึงความสำคัญในการออกจากระบบเมื่อไม่ได้ใช้งานระบบ	ศทท.	
๑๕. ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	๑. ไม่มีการควบคุมบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	๑. ครุภัณฑ์คอมพิวเตอร์ ครุภัณฑ์เครือข่าย หรืออุปกรณ์สูญหาย	 (ปานกลาง)	- จัดทำทะเบียนครุภัณฑ์ - จัดทำฐานข้อมูลทะเบียนประวัติครุภัณฑ์และระบบสารสนเทศสำคัญของ สนข.	ศทท.	
๑๖. ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	๑. ไม่มีการวางแผนการดำเนินโครงการ และอุปกรณ์เครือข่ายที่ต้องใช้ทรัพยากรร่วมกัน ๒. ผู้ใช้งานไม่ปรับปรุงข้อมูลให้เป็นปัจจุบัน	๑. การให้บริการระบบสารสนเทศหยุดชะงักส่งผลกระทบต่อให้บริการต่อประชาชน และผู้ใช้บริการทั่วไป ๒. ทรัพยากรไม่เพียงพอต่อการให้บริการ	 (ปานกลาง)	- คอยตรวจสอบทรัพยากรของระบบคอมพิวเตอร์แม่ข่ายเป็นประจำ - กำหนดแนวทางการบริหารจัดการทรัพยากร เช่น ขนาดของไฟล์ในการจัดเก็บ	ศทท.	
๑๗. ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศในทุก ๆ ระดับผู้ใช้งาน	๑. ไม่มีการควบคุมสิทธิการใช้งานของอุปกรณ์เทคโนโลยีสารสนเทศ	๑. เกิดความผิดพลาดในการให้บริการระบบสารสนเทศและการสื่อสารทั้งระบบ ๒. ไม่สามารถระบุตัวตนผู้ใช้งาน ๓. ไม่สามารถหาผู้กระทำความผิดได้	 (ต่ำ)	- มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ตามระดับ - มีการทบทวนสิทธิ์การเข้าใช้งานเป็นประจำทุก ๖ เดือนหรือเมื่อมีการเปลี่ยนแปลงปรับปรุง เพิ่มเติม แก้ไข	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
๑๘. การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑. ไม่มีการกำหนดวิธีการรักษาความมั่นคงปลอดภัยจากการปฏิบัติงานระยะไกล	๑. อาจถูกลักลอบขโมยข้อมูลหรือข้อมูลถูกทำลายทำให้เกิดความสูญเสีย ๒. ไม่สามารถหาผู้กระทำความผิดเนื่องจากไม่สามารถยืนยันตัวตนได้ ๓. ระบบถูกโจมตีจนไม่สามารถให้บริการได้	 (ต่ำ)	- มีการทำ VPN สำหรับผู้ปฏิบัติงานที่มีความต้องการเข้าถึงระบบในการเข้าถึง - มีนโยบายและแนวปฏิบัติในการเข้าถึงระบบจากระยะไกล	ศทท.	
๑๙. การนำเข้าข้อมูลผิดพลาด ไม่ครบถ้วน หรือไม่ปัจจุบัน	๑. การนำเข้าข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ ๒. ระบบมีความผิดพลาด (Bug) ๓. การนำเข้าข้อมูลที่ไม่ถูกต้องเข้าสู่ระบบ ๔. ไม่มีการตรวจสอบและปรับปรุงข้อมูลให้เป็นปัจจุบัน	๑. ข้อมูลไม่มีคุณภาพ ๒. ไม่สามารถเชื่อมโยงข้อมูลได้ ๓. ไม่สามารถนำข้อมูลไปใช้ได้ ๔. ไม่สามารถออกรายงานได้	 (ต่ำ)	- มีการตรวจสอบข้อมูลให้ถูกต้องก่อนนำเข้าข้อมูลสู่ระบบ - ตรวจสอบและแก้ไขข้อผิดพลาดของระบบหากพบเจอความผิดพลาด (Bug) ของโปรแกรม - มีการตรวจสอบข้อมูลที่ได้เคยนำเข้าระบบไปแล้ว โดยปรับปรุงข้อมูลให้ถูกต้องและเป็นปัจจุบัน	ศทท.	
๒๐. การจ้างบุคคลภายนอกที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑. ระบบเกิดปัญหา ชัดข้อง ๒. การให้บริการติดขัด ล่าช้า ๓. อุปกรณ์หรือระบบสารสนเทศเสียหาย ๔. ระบบไม่สามารถให้บริการได้	๑. ระบบมีข้อผิดพลาดและไม่เป็นไปตามแผน ๒. เสียเวลาในการแก้ไขปัญหา ๓. เกิดความผิดพลาดในการทำงานทำให้ระบบทำงานบกพร่อง	 (ต่ำ)	- มีการกำหนดคุณสมบัติของบุคลากรภายนอก (Outsource) ให้ชัดเจนและตรงตามความต้องการ - มีการติดตามงานของบุคลากรภายนอก (Outsource)	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
		๔. ไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้ หรือแก้ไขได้ล่าช้า ๕. เกิดความเสียหายแก่ระบบหรือหน่วยงาน		และตรวจสอบการทำงานก่อนตรวจรับงาน - มีเจ้าหน้าที่ในการควบคุมดูแลการปฏิบัติงานของบุคลากรภายนอก (Outsource) - มีการติดตามเพื่อป้องกันการผิดพลาดและให้เกิดการแก้ไขปัญหาได้ทันที		
๒๑. การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และระบบเครือข่ายคอมพิวเตอร์ของ สนช.	๑. ไฟฟ้าดับ ๒. เครื่องปรับอากาศเสีย/หยุดทำงาน/ไม่มีความเย็น ๓. ความชื้นไม่เหมาะสม	๑. ห้องเซิร์ฟเวอร์มีอุณหภูมิสูงส่งผลให้เครื่องคอมพิวเตอร์แม่ข่ายร้อนจนหยุดทำงาน ๒. เกิดความเสียหายขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และเครือข่ายคอมพิวเตอร์	 (ต่ำ)	- ติดตั้งระบบเผื่อสำรองอุณหภูมิและความชื้น - ตรวจสอบความพร้อมใช้งานของระบบปรับอากาศแบบควบคุมความชื้นให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ - มีการจัดจ้างผู้เชี่ยวชาญเพื่อดำเนินการบำรุงรักษา	ศทท.	
๒๒. ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๑. ผู้ให้บริการอินเทอร์เน็ตขัดข้อง ๒. IP Address ไม่เพียงพอสำหรับผู้ใช้งาน ๓. ปริมาณการรับ-ส่ง ข้อมูล (Bandwidth) ไม่เพียงพอต่อการใช้งาน	๑. ผู้ใช้งานไม่สามารถเชื่อมต่ออินเทอร์เน็ต หรือมีความล่าช้า ๒. ไม่สามารถเข้าถึงระบบงานสารสนเทศได้	 (ต่ำ)	- มีระบบเครือข่ายสำรองในการให้บริการ - มีการตรวจสอบการเข้าถึงระบบเครือข่าย - มีเจ้าหน้าที่ที่ได้รับมอบหมายติดตามดูแลการใช้งานของผู้ใช้งานภายในหน่วยงาน	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
				<ul style="list-style-type: none"> - มีการบำรุงรักษาและแก้ไข ปัญหาจากผู้ให้บริการ เครือข่ายหลัก - กำหนดแบ่งช่วง IP Address สำหรับอุปกรณ์ที่เชื่อมต่อ เครือข่าย - การติดตั้งสายสัญญาณ ให้เพียงพอต่อการใช้งาน - มีการตัดสัญญาณเมื่อไม่ได้ ใช้งานระบบเป็นระยะเวลา นาน (Session Timeout) 		
๒๓. บุคลากรด้านไอทีที่มีความรู้ ความเข้าใจด้านเทคโนโลยี อย่างไม่เพียงพอ	๑. ขาดการฝึกอบรมบุคลากรด้านไอที ๒. หน่วยงานขาดบุคลากรด้านไอที	๑. เกิดความผิดพลาดในการใช้ ระบบส่งผลทำให้การทำงาน ของระบบบกพร่อง และ อาจเกิดความเสียหาย ทั้งระบบได้ ๒. งบประมาณที่ใช้ในการบำรุง รักษาไม่เพียงพอเพิ่มขึ้นทุกปี ๓. อาจเกิดความเสียหายแก่ระบบ หรือหน่วยงาน	 (ต่ำ)	<ul style="list-style-type: none"> - ส่งเสริมให้มีอบรม/การสอบ มาตรฐานวิชาชีพด้านไอที - การให้บุคลากรภายนอก (Outsource) ที่มีความเชี่ยวชาญ เฉพาะด้านอบรมให้แก่ บุคลากรไอทีของหน่วยงาน - ส่งเสริมบุคลากรไอที ที่ติดตามและเรียนรู้เกี่ยวกับ เทคโนโลยีใหม่ 	ศทท.	
๒๔. การโดนดักจับข้อมูลจาก การใช้เครือข่ายเดียวกันกับบุคคล น่าสงสัย	๑. การใช้งานระบบจากระยะไกล ด้วยเครือข่ายที่ไม่น่าเชื่อถือ ๒. การให้บุคคลที่น่าสงสัยมาใช้งาน ระบบเครือข่ายเดียวกัน	๑. โดนดักเก็บข้อมูล เช่น รหัสผ่าน ข้อมูลสำคัญ และข้อมูลลับ ๒. เกิดความผิดพลาดในการให้ บริการระบบสารสนเทศ	 (ต่ำ)	<ul style="list-style-type: none"> - มีการตรวจสอบการเข้าถึง ระบบเครือข่าย - มีระบบการยืนยันตัวตน เมื่อมีการเข้าใช้งานเครือข่าย - มีการแบ่งระบบเครือข่าย 	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
		๓. ไม่สามารถระบุตัวตนผู้ใช้งานหรือผู้กระทำความผิดได้		- มีการติดตามและเฝ้าระวังผู้ใช้งานระบบเครือข่าย		
๒๕. งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑. โดนตัด/ปรับลดงบประมาณในการดำเนินโครงการตามนโยบายการปรับลดเงินเป็นร้อยละทำให้โครงการที่จำเป็นต้องดำเนินการโดนตัดหรือปรับลดไปด้วย	๑. อาจต้องลดระยะเวลาลดคุณภาพ หรือประสิทธิภาพของงานหรือโครงการที่โดนตัดหรือปรับลดงบประมาณ ๒. ไม่ได้ดำเนินโครงการตามเป้าที่วางไว้ ๓. งดเงิน และงดงานที่ปรับอาจไม่สอดคล้องกัน ๔. ไม่ได้จัดหาอุปกรณ์หรือครุภัณฑ์ทดแทน ทำให้การปฏิบัติงานมีประสิทธิภาพลดลง	■ (ต่ำ)	- หน่วยงานวิเคราะห์งบประมาณ ต้องมีการดำเนินการตัด ปรับลด โดยมีการจัดทำความเสี่ยง และการให้น้ำหนักของ ความสำคัญของโครงการ ที่ใช้หมวดเงินประเภทเดียวกัน - ปรับลดโครงการตามลำดับความสำคัญ - ปรับแผนการดำเนินงานตามแผนการใช้จ่ายงบประมาณตามงวดงานที่ได้รับ	ศทท.	
๒๖. ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑. ความเสี่ยงด้านการบริหารจัดการหรือจากเจ้าหน้าที่ผู้ปฏิบัติงาน	๑. ไม่มีการควบคุมอุปกรณ์ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน ๒. มีจำนวนบุคลากรเพิ่มขึ้น ทำให้การจัดการไม่ครอบคลุม	■ (ต่ำ)	- มีระบบการยืนยันตัวตนเมื่อมีการเข้าใช้งานเครือข่าย - มีการแบ่งระบบเครือข่ายเฉพาะสำหรับให้บริการอุปกรณ์แบบพกพา	ศทท.	
๒๗. ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑. ครุภัณฑ์อุปกรณ์ไม่ได้มาตรฐานหรือตอบสนองได้ไม่ครบครุภัณฑ์กับการทำงาน ๒. การติดตั้งใช้งานไม่สมบูรณ์	๑. เกิดความเสียหายจากการใช้งานครุภัณฑ์ ๒. ติดตั้งใช้งานได้ไม่สมบูรณ์ ๓. การทำงานล่าช้า	■ (ต่ำ)	- ทำการตรวจสอบลักษณะของงานเพื่อจัดหาอุปกรณ์ที่เหมาะสมกับลักษณะการใช้งาน	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับความเสี่ยง	แนวทางจัดการ/กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
๒๘. ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัลฯ	๑. ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัลฯ	๑. ผู้บริหารปรับลดระยะเวลาดำเนินโครงการ ๒. ไม่สามารถดำเนินงานให้บรรลุเป้าหมายและตัวชี้วัดที่กำหนด	 (ต่ำ)	- ทบทวนการดำเนินงานโครงการให้เป็นไปตามแผน หากไม่เป็นไปตามแผนต้องปรับแผนการดำเนินโครงการ	ศทท.	
๒๙. กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑. ไม่สามารถดำเนินงานได้อย่างต่อเนื่องทันที ๒. การดำเนินการโครงการล่าช้า ๓. การเปลี่ยนแปลงวิธีการระหว่างการดำเนินการ	๑. เกิดความล่าช้า ไม่สามารถทำงานได้ต่อเนื่อง ๒. อนุมัติโครงการล่าช้า ๓. ไม่สามารถหาผู้รับจ้างได้ตามแผนการดำเนินการ	 (ต่ำ)	- จัดทำแผนปฏิบัติการและดำเนินการให้เป็นไปตามแผนที่กำหนด - รับผิดชอบและติดตามการอนุมัติให้ดำเนินโครงการให้เป็นไปตามแผน หากไม่เป็นไปตามแผนต้องเร่งดำเนินการ - กรณีพบปัญหาในการดำเนินการให้รีบแจ้งผู้บริหารเพื่อหาวิธีแก้ไขโดยเร่งด่วน - ตรวจสอบสัญญาให้เป็นไปตามร่างข้อกำหนด โดยการประสานกับเจ้าหน้าที่พัสดุก่อนทุกครั้ง - จัดทำแผนการตรวจรับงานให้เหมาะสมเพื่อให้สามารถตรวจรับงานและเบิกจ่ายได้ทันตามแผนที่กำหนด	ศทท.	

ความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ/ความเสียหาย	ระดับ ความเสี่ยง	แนวทางจัดการ/ กิจกรรมควบคุม	ผู้รับผิดชอบ	หมายเหตุ
๓๐. ไม่สามารถปฏิบัติตามกฎหมาย และระเบียบที่เกี่ยวข้อง	๑. กฎหมาย/ระเบียบที่เกี่ยวข้อง กับการปฏิบัติงานด้านเทคโนโลยี สารสนเทศมีผลบังคับใช้ ๒. ไม่สามารถดำเนินการ ตามกฎหมาย/ระเบียบ ที่เกี่ยวข้องได้ทันภายในระยะ เวลาที่กำหนด	๑. การดำเนินงานไม่สามารถ รองรับการปฏิบัติงานตาม กฎหมาย/ระเบียบที่บังคับใช้ได้ ๒. ไม่มีระบบสารสนเทศรองรับ การดำเนินงานตามที่กฎหมาย กำหนด	 (ต่ำ)	- ติดตามกฎหมาย ประกาศ และระเบียบที่เกี่ยวข้อง - จัดลำดับความสำคัญและ วางแผนการดำเนินงาน ให้สอดคล้องและเป็นไปตาม กฎหมายและระเบียบ ที่เกี่ยวข้อง	ศทท.	
๓๑ การเปลี่ยนแปลงนโยบาย ด้านเทคโนโลยีสารสนเทศ ของหน่วยงาน	๑. การปรับเปลี่ยนตำแหน่งงาน ๒. การปรับเปลี่ยนบุคลากร ๓. การเปลี่ยนแปลงนโยบาย ด้านเทคโนโลยีสารสนเทศ ของหน่วยงาน	๑. การดำเนินงานล่าช้า ติดขัด	 (ต่ำ)	- ติดตามและปรับปรุงแผน การดำเนินงานให้สอดคล้อง กับนโยบายด้านเทคโนโลยี สารสนเทศของหน่วยงาน	ศทท.	

๓.๗ การจัดทำแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

หน่วยงาน : สำนักงานนโยบายและแผนการขนส่งและจราจร

ผู้รับผิดชอบหลัก : ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

ระยะเวลาดำเนินการ : มกราคม - พฤษภาคม ๒๕๖๙

ตารางที่ ๓-๖ แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ประเด็นความเสี่ยง/ กิจกรรม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง	แนวทางจัดการ/ กิจกรรม	ปี พ.ศ. ๒๕๖๙						ผู้รับผิดชอบ
			เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ระดับสูงมาก									
ละเมิดลิขสิทธิ์โปรแกรม อรรถประโยชน์ (Utilities Program)	<ul style="list-style-type: none">- เจ้าหน้าที่ของ สนข. มีความเข้าใจเกี่ยวกับโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย- เจ้าหน้าที่ของ สนข. ไม่ใช้งานโปรแกรมละเมิดลิขสิทธิ์- มีการจัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	๑. ตรวจสอบการติดตั้งโปรแกรม ละเมิดลิขสิทธิ์			←→			ศทท.	
		๒. จัดอบรมสร้างความตระหนักรู้ ในเรื่องนโยบายและแนวปฏิบัติ ความมั่นคงปลอดภัยด้านสารสนเทศ และการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ ถูกต้องตามกฎหมาย และกระตุ้น ให้เกิดการปฏิบัติตามแนวนโยบาย หรือระเบียบฯ อย่างจริงจัง			←→				
		๓. ส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์ แบบ OpenSource แทนโปรแกรม ละเมิดลิขสิทธิ์	←→						
		๔. จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้อง ตามกฎหมาย	←→						

ประเด็นความเสี่ยง/ กิจกรรม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง	แนวทางจัดการ/ กิจกรรม	ปี พ.ศ. ๒๕๖๙						ผู้รับผิดชอบ
			เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ระดับสูงมาก									
ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์เจาะระบบหรือ ลักลอบ (Hack) เข้าสู่ เครื่องคอมพิวเตอร์แม่ข่าย (Server)	<ul style="list-style-type: none">- ระบบเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายของ สนข. มีความมั่นคงปลอดภัย- มีกระบวนการแก้ไขปัญหากรณี ระบบเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายของ สนข. ถูกโจมตี	๑. ตรวจสอบการตั้งค่าอุปกรณ์รักษา ความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall	←					→	ศทท.
		๒. ตรวจสอบ ติดตาม และเฝ้าระวัง การบุกรุกเครือข่ายอย่างสม่ำเสมอ	←					→	
		๓. ติดตามข่าวสารภัยคุกคาม ทางไซเบอร์อย่างสม่ำเสมอ	←					→	
		๔. ติดตั้งและอัปเดตโปรแกรมป้องกัน ไวรัสอย่างสม่ำเสมอ	←					→	
		๕. ติดตั้งและอัปเดต Patch ของ ระบบปฏิบัติการอย่างสม่ำเสมอ	←					→	
		๖. เปลี่ยนรหัสผ่านตามแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ	←					→	

ประเด็นความเสี่ยง/ กิจกรรม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง	แนวทางการจัดการ/ กิจกรรม	ปี พ.ศ. ๒๕๖๙						ผู้รับผิดชอบ
			เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ระดับสูงมาก									
ถูกโจมตีโดยบุคคล ที่ไม่มีสิทธิ์เจาะระบบหรือ ลักลอบ (Hack) เข้าสู่ระบบ ฐานข้อมูล (Database)	<ul style="list-style-type: none">- ระบบสารสนเทศและฐานข้อมูล ของ สนข. มีความมั่นคงปลอดภัย- มีกระบวนการแก้ไขปัญหา กรณีระบบฐานข้อมูลระบบงาน สารสนเทศของ สนข. ถูกโจมตี	๑. ตรวจสอบการตั้งค่าอุปกรณ์รักษา ความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall	←						ศทท.
		๒. ตรวจสอบ ติดตาม และเฝ้าระวัง การบุกรุกเครือข่ายอย่างสม่ำเสมอ	←						
		๓. ติดตามข่าวสารภัยคุกคาม ทางไซเบอร์อย่างสม่ำเสมอ	←						
		๔. ติดตั้งและอัปเดตโปรแกรมป้องกัน ไวรัสอย่างสม่ำเสมอ	←						
		๕. ติดตั้งและอัปเดต Patch ของ ระบบปฏิบัติการอย่างสม่ำเสมอ	←						
		๖. เปลี่ยนรหัสผ่านตามแนวปฏิบัติ ด้านการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ	←						

ประเด็นความเสี่ยง/ กิจกรรม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง	แนวทางการจัดการ/ กิจกรรม	ปี พ.ศ. ๒๕๖๙						ผู้รับผิดชอบ
			เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ระดับสูง									
ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ	<ul style="list-style-type: none">- ระบบสารสนเทศไม่ได้รับผลกระทบจากกรณีเกิดเหตุไฟฟ้าขัดข้อง- สามารถแก้ไขสถานการณ์เมื่อเกิดเหตุขัดข้องได้อย่างรวดเร็ว	๑. ตรวจสอบระบบสำรองไฟฟ้า (UPS) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายให้อยู่ในสถานะพร้อมใช้งานเป็นประจำ	←					→	ศทท.
		๒. มีการจัดจ้างผู้เชี่ยวชาญ เพื่อดำเนินการบำรุงรักษา	←					→	
ข้อมูลสำคัญรั่วไหล	<ul style="list-style-type: none">- มีกระบวนการป้องกันเพื่อลดความเสี่ยงของการเกิดเหตุข้อมูลสำคัญของ สนข. รั่วไหลจากการใช้งานระบบคอมพิวเตอร์- มีกระบวนการแก้ไขปัญหากรณีเกิดเหตุได้อย่างรวดเร็ว	๑. มีระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์ ระบบเครือข่ายระบบสารสนเทศ	←					→	ศทท.
		๒. มีกระบวนการทบทวนสิทธิผู้ใช้งานเป็นประจำ	←					→	
		๓. มีการเก็บประวัติการเข้าใช้งานคอมพิวเตอร์	←					→	
		๔. มีกระบวนการบริหารจัดการคอมพิวเตอร์และอุปกรณ์	←					→	
		๕. มีแนวปฏิบัติในการลบหรือทำลายข้อมูลหลังจากไม่ได้ใช้งาน	←					→	

ประเด็นความเสี่ยง/ กิจกรรม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง	แนวทางจัดการ/ กิจกรรม	ปี พ.ศ. ๒๕๖๙						ผู้รับผิดชอบ
			เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
ระดับสูง									
ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	- ผู้ใช้งาน (Users) มีความรู้ ความเข้าใจ และมีทักษะการใช้งาน ระบบเทคโนโลยีสารสนเทศ ได้อย่างถูกต้อง ปลอดภัย	๑. อบรมการใช้งานระบบ			↔				ศทท.
		๒. จัดทำคู่มือสำหรับการใช้งานระบบ	←					→	
		๓. ให้มีเจ้าหน้าที่สำหรับให้คำปรึกษา เกี่ยวกับการใช้งานระบบ และช่วย แก้ไขปัญหาให้ผู้ใช้งาน	←					→	

บทที่ ๔

บทสรุปและข้อเสนอแนะ

ปัจจุบัน สนช. เริ่มปรับเปลี่ยนกระบวนการปฏิบัติงานภายในหน่วยงานไปเป็นรูปแบบดิจิทัล (Digital Transformation) โดยใช้เทคโนโลยีสารสนเทศเข้ามาเป็นกลไกในการขับเคลื่อนมากขึ้น ดังนั้น การดำเนินงานทุกกิจกรรมที่เกิดขึ้นภายในหน่วยงานจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้น ทั้งนี้ ระบบสารสนเทศของหน่วยงานล้วนแล้วแต่มีปัจจัยเสี่ยงซึ่งเป็นต้นเหตุหรือสาเหตุที่ทำให้ระบบสารสนเทศของหน่วยงานเกิดความชะงัก หยุดการทำงาน หรือทำงานได้เพียงบางส่วน ซึ่งส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายของหน่วยงาน

การบริหารความเสี่ยง (Risk Management) คือ เครื่องมือสำหรับใช้ในการบริหารความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศของ สนช. อย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ โดยเริ่มจากการค้นหา ระบุ วิเคราะห์ ประเมิน จัดลำดับความเสี่ยง และกำหนดมาตรการและการตอบสนองต่อความเสี่ยงที่สามารถจัด ลด หรือควบคุมผลกระทบและความเสียหายที่เกิดขึ้นให้อยู่ในระดับที่หน่วยงานยอมรับได้

สนช. จึงได้มีการทบทวนและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ สนช. ใช้งานอยู่ในปัจจุบัน และจัดทำเป็นแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Management) ของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ เพื่อให้ทราบถึงความเสี่ยงที่มีอยู่และแนวทางการบริหารจัดการความเสี่ยง เพื่อให้ความเสี่ยงที่มีอยู่หรือมีโอกาสดังกล่าวจะเกิดขึ้นลดลงอยู่ในระดับที่หน่วยงานยอมรับได้

๔.๑ สรุปความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

จากการประเมินความเสี่ยงและจัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ พบว่า สนช. มีความเสี่ยงที่อยู่ใน ระดับสูงมาก จำนวน ๓ รายการ ระดับสูง จำนวน ๓ รายการ ระดับปานกลาง จำนวน ๑๐ รายการ และ ระดับต่ำ จำนวน ๑๕ รายการ รวมทั้งหมดเป็นจำนวน ๓๑ รายการ ซึ่งได้กำหนดแนวทางและกิจกรรมในการควบคุมความเสี่ยงใน บทที่ ๓ เรียบร้อยแล้ว

๔.๒ บทสรุป

แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Management) ของ สนช. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ได้ดำเนินการจัดทำโดยมีวัตถุประสงค์เพื่อ

๔.๒.๑ เป็นคู่มือในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนช. และติดตามผลการดำเนินงานอย่างถูกต้องและเหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่หน่วยงานสามารถยอมรับได้

๔.๒.๒ เป็นแนวปฏิบัติในการดูแลรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศต่าง ๆ ของ สนช. ให้มีเสถียรภาพ และมีความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

๔.๒.๓ สร้างความเชื่อมั่นและรับประกันว่าระบบสารสนเทศของ สนช. จะยังคงสามารถให้บริการได้อย่างต่อเนื่องทั้งในสถานการณ์ปกติและหรือสถานการณ์ฉุกเฉิน

ซึ่ง สนช. ควรมีการดำเนินการตามแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อช่วยจัดการความเสี่ยงที่ยังคงมีอยู่ หรือมีโอกาสดังกล่าวจะเกิดขึ้น โดยเฉพาะอย่างยิ่งความเสี่ยงที่ยอมรับไม่ได้และต้องเร่งดำเนินการกำจัดความเสี่ยงนั้นออกไป เพื่อให้ระบบเทคโนโลยีสารสนเทศของ สนช. มีความมั่นคงปลอดภัยสูงสุด และทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ สนช. เป็นไปอย่างมีประสิทธิภาพ

๔.๓ ข้อเสนอแนะ

๔.๓.๑ การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสิ่งสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

- (๑) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน
- (๒) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิภาพของการจัดการความเสี่ยงนั้น
- (๓) กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๔.๓.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าวิธีการบริหารความเสี่ยงที่เลือกใช้นั้นมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันทั่วทั้งที่ และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

๔.๓.๑ ควรมีการทบทวนการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง เพื่อนำผลมาพิจารณาปรับปรุงแผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Management) ของ สนข. เพื่อจัดและควบคุมความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ให้สอดคล้องกับปัจจุบันและเกิดประสิทธิผลสูงสุด

ผู้จัดทำร่าง

นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรังรัก ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายณฤทธิ์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๓. นายพิสิฐ ป้อมทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร