



แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ของสำนักงานนโยบายและแผนการขนส่งและจราจร



ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร



สพข www.otp.go.th



แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cyber Security Audit : CSA)
ของสำนักงานนโยบายและแผนการขนส่งและจราจร

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

ประจำปี ครั้งที่

<p>วัตถุประสงค์การตรวจประเมิน (Objective) :</p>	<p>เพื่อตรวจประเมินความสอดคล้องของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีต่อ :</p> <p>๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒</p> <p>๒) ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔</p> <p>๓) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. พ.ศ. ๒๕๖๗</p>
<p>เกณฑ์/มาตรฐานที่ใช้ในการตรวจประเมิน (Audit Criteria) :</p>	<p>๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒</p> <p>๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.</p> <p>๓) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๕</p>
<p>ขอบเขตที่ตรวจประเมิน (Scope of Audit) :</p>	<p>การรักษาความมั่นคงปลอดภัยไซเบอร์ของ สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.)... ซึ่งประกอบไปด้วยขอบเขตบริการที่สำคัญดังต่อไปนี้ (อ้างอิงเอกสารตาม : ผลการวิเคราะห์ความเสี่ยงด้านสารสนเทศ)</p> <p>๑...บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ XXX....</p> <p>๒...บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ XXX....</p> <p>๓...บริการ xxxxx โดยมีหน่วยงานที่รับผิดชอบ ได้แก่ XXX....</p> <p>รวมถึงสิ่งอำนวยความสะดวกพื้นฐาน (Facilities) ระบบเครือข่าย (Network) ที่สนับสนุนการให้บริการดังกล่าวของ สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ติดตั้งที่ ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร อาคาร สนข. ชั้น ๔ เลขที่ ๓๕ ถนนเพชรบุรี แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐</p>

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.
ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
(วันที่ประเมิน)	๐๙.๐๐ - ๐๙.๑๕ น.	Opening Meeting (ประชุมชี้แจงแผนการตรวจ)	All participants	All participants	
(วันที่ประเมิน)	๐๙.๑๕ - ๐๙.๓๐ น.	(ตัวอย่าง เช่น สัมภาษณ์ผู้บริหารระดับสูงขององค์กร - ทิศทางการบริหารจัดการ - วิสัยทัศน์ พันธกิจ กลยุทธ์ และวัตถุประสงค์ ด้านความมั่นคงปลอดภัยไซเบอร์ - บทบาท หน้าที่ และความรับผิดชอบ - การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) - การบริหารความเสี่ยง (Risk Management) - นโยบาย และแนวปฏิบัติ (Policies and Guidelines))	All Auditors	ผู้บริหารสารสนเทศ ระดับสูง (Chief Information Security Officer : CIO) /ผู้บริหาร ระดับสูงด้านบริหาร จัดการความมั่นคง ปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO)	มาตรา ๔๒, ๔๓, ๔๔, ๔๕, ๔๖, ๕๒, ๕๔, ๕๕, ๕๖, ๕๗, ๕๘ ประมวล ข้อ ๑๗, ๑๘, ๑๙ นโยบายข้อ ๑, ๒, ๓

**** จะกำหนดขั้นตอน และรายละเอียดในการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามแบบฟอร์มในแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. หลังจากมีการประกาศใช้ประมวลแนวทางและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. และได้มีผลการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จากแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. เรียบร้อยแล้ว ****

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.

ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
(วันที่ประเมิน)	๐๙.๓๐ - ๑๑.๐๐ น.	<p>(ตัวอย่าง เช่น</p> <p>สอบถามแนวทางปฏิบัติขององค์กร ตาม พรบ.ฯ</p> <p>ตามประมวลฯ และตามนโยบายฯ โดยมีหัวข้อ ดังนี้</p> <p>๑. การจัดทำแผนการตรวจสอบด้านการรักษาความมั่นคง</p> <p>ปลอดภัยไซเบอร์</p> <ul style="list-style-type: none"> - องค์กรมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระ ภายนอก อย่างน้อยปีละ ๑ ครั้งหรือไม่ - องค์กรมีการส่งผลสรุปรายงานการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายใน กำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จหรือไม่ - องค์กรมีการจัดทำแผนดำเนินการแก้ไขอย่างไร - องค์กรมีขั้นตอนการปรับปรุงแผนหรือไม่หากมี การทักท้วงจาก กกก. - องค์กรมีการดำเนินการแก้ไขให้อยู่ในกรอบระยะเวลา อย่างไร และมีการติดตามผลอย่างไร <p>๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย</p> <p>ไซเบอร์</p> <ul style="list-style-type: none"> - องค์กรมีการประเมินความเสี่ยง (Risk Assessment) อย่างไร 	All Auditors	<p>ผู้บริหารสารสนเทศ</p> <p>ระดับสูง (Chief</p> <p>Information Security</p> <p>Officer : CIO) /</p> <p>ผู้บริหารระดับสูง</p> <p>ด้านบริหารจัดการ</p> <p>ความมั่นคงปลอดภัย</p> <p>สารสนเทศ</p> <p>(Chief Information</p> <p>Security Officer :</p> <p>CISO) / ทีมปฏิบัติงาน</p> <p>ด้านไซเบอร์</p>	<p>มาตรา ๔๒,</p> <p>๔๓, ๔๔,</p> <p>๔๕, ๔๖,</p> <p>๕๒, ๕๔,</p> <p>๕๕, ๕๖,</p> <p>๕๗, ๕๘</p> <p>ประมวลข้อ</p> <p>๑๗, ๑๘, ๑๙</p> <p>นโยบายข้อ ๑,</p> <p>๒, ๓</p>

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.

ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
		<ul style="list-style-type: none"> - องค์กรมีการจัดการความเสี่ยง (Risk Treatment) อย่างไร - องค์กรมีการติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) อย่างไร - องค์กรมีการรายงานความเสี่ยง (Risk Reporting) อย่างไร <p>๓. การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์</p> <ul style="list-style-type: none"> - องค์กรมีการจัดทำแผน มีการสื่อสาร และมีการทบทวนแผนการรับมืออย่างไร <p>๔. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)</p> <ul style="list-style-type: none"> - องค์กรมีการกำกับดูแลที่ดี ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างไร <p>๕. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)</p> <ul style="list-style-type: none"> - องค์กรมีการจัดทำ นโยบาย มาตรฐาน และแนวทาง ในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างไร 			

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.

ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
(วันที่ประเมิน)	๑๑.๐๐ - ๑๒.๐๐ น.	(ตัวอย่าง เช่น การระบุความเสี่ยงของหน่วยงาน (Identify) - การจัดการทรัพย์สิน (Asset Management) - การประเมินความเสี่ยงและกลยุทธ์ในการจัดการ ความเสี่ยง (Risk Assessment and Risk Management Strategy) - การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) - การจัดการผู้ให้บริการภายนอก (Third Party Management))	(ชื่อผู้ประเมิน) (Auditor)	ผู้บริหารสารสนเทศ ระดับสูง (Chief Information Security Officer : CIO) / ผู้บริหารระดับสูง ด้านบริหารจัดการ ความมั่นคงปลอดภัย สารสนเทศ (Chief Information Security Officer : CISO) / ทีมปฏิบัติงาน ด้านไซเบอร์	มาตรา ๕๔, ๕๕ ประมวลข้อ ๒๑ นโยบายข้อ ๒
(วันที่ประเมิน)	๑๒.๐๐ - ๑๓.๐๐ น.	<u>พักกลางวัน</u>		-	
(วันที่ประเมิน)	๑๓.๐๐ - ๑๔.๐๐ น.	(ตัวอย่าง เช่น มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้นของ สนช. (Protect) - การควบคุมการเข้าถึง (Access Control) - การทำให้ระบบมีความแข็งแกร่ง (System Hardening) - การเชื่อมต่อระยะไกล (Remote Connection) - สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)	(ชื่อผู้ประเมิน) (Auditor)	ผู้บริหารสารสนเทศ ระดับสูง (Chief Information Security Officer : CIO) / ผู้บริหารระดับสูง ด้านบริหารจัดการ ความมั่นคงปลอดภัย สารสนเทศ (Chief	มาตรา ๕๔, ๕๕ ประมวลข้อ ๒๒ นโยบายข้อ ๓

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.
ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
		<ul style="list-style-type: none"> - การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) - การแบ่งปันข้อมูล (Information Sharing)) 		Information Security Officer : CISO) / ทีมปฏิบัติงานด้านไซเบอร์	
(วันที่ประเมิน)	๑๔.๐๐ – ๑๕.๐๐ น.	(ตัวอย่าง เช่น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ของ สนช. (Detect) <ul style="list-style-type: none"> - การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)) 	(ชื่อผู้ประเมิน) (Auditor)	ผู้บริหารสารสนเทศระดับสูง (Chief Information Security Officer : CIO) / ผู้บริหารระดับสูงด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) / ทีมปฏิบัติงานด้านไซเบอร์	มาตรา ๕๖, ๕๗, ๕๘ ประมวลข้อ ๒๓ นโยบายข้อ ๑

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช.

ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
(วันที่ประเมิน)	๑๕.๐๐ – ๑๖.๐๐ น.	<p>(ตัวอย่าง เช่น มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ ของ สนช. (Respond)</p> <ul style="list-style-type: none"> - แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) - แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) - การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)) 	(ชื่อผู้ประเมิน) (Auditor)	ผู้บริหารสารสนเทศ ระดับสูง (Chief Information Security Officer : CIO) / ผู้บริหารระดับสูง ด้านบริหารจัดการ ความมั่นคงปลอดภัย สารสนเทศ (Chief Information Security Officer : CISO) / ทีมปฏิบัติงาน ด้านไซเบอร์	มาตรา ๕๖, ๕๗, ๕๘ ประมวล ข้อ ๒๔ นโยบายข้อ ๑
(วันที่ประเมิน)	๑๖.๐๐ – ๑๗.๐๐ น.	<p>(ตัวอย่าง เช่น มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคาม ทางไซเบอร์ของ สนช. (Recover)</p> <ul style="list-style-type: none"> - การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทาง ไซเบอร์ (Cybersecurity Resilience and Recovery) - การรายงานผล) 	(ชื่อผู้ประเมิน) (Auditor)	ผู้บริหารสารสนเทศ ระดับสูง (Chief Information Security Officer : CIO) / ผู้บริหารระดับสูง ด้านบริหารจัดการ ความมั่นคงปลอดภัย สารสนเทศ (Chief Information Security	มาตรา ๕๖, ๕๗, ๕๘ ประมวล ข้อ ๒๕ นโยบายข้อ ๑

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.
ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
				Officer : CISO) / ทีมปฏิบัติงาน ด้านไซเบอร์	

แบบการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.

ประจำปี ครั้งที่

วันที่	เวลา	ข้อกำหนดในการตรวจประเมิน (Area of Audit)	ผู้ตรวจประเมิน	ผู้รับการตรวจ ประเมิน	หมายเหตุ
(วันที่ประเมิน)	๑๗.๐๐ - ๑๗.๑๐ น.	Auditor Time ประชุมคณะผู้ตรวจประเมิน	All Auditors	-	
(วันที่ประเมิน)	๑๗.๑๐ - ๑๗.๓๐ น.	สรุปผลการตรวจประเมินภายใน ร่วมกับทีมผู้ตรวจประเมิน และผู้ที่เกี่ยวข้อง	All participants	All participants	

ผู้จัดทำ / ตรวจสอบ	ผู้อนุมัติ
ลงนาม : (.....) หัวหน้าทีมผู้ตรวจสอบภายใน (Lead Internal Auditor)	ลงนาม : (.....) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) / ผู้บริหารด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ประจำ สนข.
วันที่ :	วันที่ :