Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Roads Office FEDRO

INFORMATIONS-SICHERHEITS-MANAGEMENT-SYSTEM FAHRTSCHREIBER-KARTEN POLICY

(ISMS FKR POLICY)

V1.0

IMPRESSUM

Erstelldatum / Revisionsdatum:	27.3.2020
Ersteller/in:	Gerhard Schuwerk (Shg, CISO ISMS FKR)
Verzeichnis / Dateiname:	ISMS-FKR_Policy_v[X.X]_de.docx
Anzahl Seiten:	7
Genehmigt am:	05.11.2020
Genehmigt von:	PAS FKR

Änderungsverzeichnis

Version	Datum	Ersteller	Bemerkungen
0.1	27.03.2020	Shg	Initiale Version
0.2	06.04.2020	Shg	Erweiterung nach Definition des Scope ISMS FKR
0.9	08.04.2020	Shg	Version für MS1
0.9.1	04.05.2020	Shg	Version nach Korrekturen Review MS1
0.9.2	28.05.2020	Shg	Anpassungen nach MS2
0.9.3	12.10.2020	Shg	Anpassungen BIT Betrieb (Vorhaben ISMS)
0.9.4	16.12.2020	Shg	Kleinkorrekturen aus der Übersetzung
1.0	05.11.2020	Shg	Genehmigung PAS

INHALTSVERZEICHNIS

1. Ausgangslage und Geltungsbereich

Das Bundesamt für Strassen (ASTRA) zertifiziert sich im Informationssicherheitsmanagementsystem Fahrtschreiberkartenregister (ISMS FKR) nach der ISO Norm 27001:2013 und verpflichtet sich zur Erfüllung dieser Anforderungen.

Dabei umfasst der Geltungsbereich der Zertifizierung die Swiss Card Issuing Authority (CH-CIA) zur Ausstellung der Fahrtschreiberkarten (FSK) auf Basis der Fachanwendung Fahrtschreiberkartenregister (FKR) im Gesamtsystem des «Intelligenten Fahrtschreibers» (iDFS).

Die Zuständigkeit für die Ausgabe von Fahrtschreiberkarten für das Fürstentum Liechtenstein (Liechtenstein Member State Authority / FL-MSA) liegt gemäss Artikel 21 des Abkommens über den Strassenverkehr zwischen der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein (SR 0.741.531.951.4) beim ASTRA bzw. der Schweiz (Swiss Member State Authority / CH-MSA).

Im ISMS FKR explizit eingeschlossen sind:

- Der Zugriff der Mitarbeitenden des Zolls (EZV) auf FKR

Im ISMS FKR explizit eingeschlossen sind folgende Bereiche, welche ein ISMS vorweisen:

- Der Softwarelieferant für FKR
- Der Kartenpersonalisierer (CH-CP)
- Der Entwickler und Betreiber der PKI
- Der Anbieter mit den Bezahllösungen

Im ISMS FKR explizit eingeschlossen sind folgende Bereiche, welche ein ISMS-Vorhaben vorweisen:

- Der Betreiber der Software

Aus dem ISMS FKR ausgeschlossen sind:

- Die Prozesse ausserhalb der CH-CIA sowie die Hard- und Software der Unternehmen und der Fahrer (Fahrtschreiber im Fahrzeug), der Fahrtschreiber-Hersteller, der Werkstätten und der Kontrollbehörden.

2. Ziele der Informationssicherheit

Das ASTRA hat sich folgende Ziele gesetzt:

- Anwendung eines geeigneten IT-Sicherheitsmanagement-Systems (ISMS), durch das die informationstechnische Sicherheit aller für seine Aufgaben relevanten Tätigkeiten dauerhaft gewährleistet ist.
- Angemessener Schutz von Informationen in Bezug auf Verfügbarkeit, Vertraulichkeit sowie Integrität.
- Erfüllung der gesetzlichen, vertraglichen und internen Vorgaben im Bereich der Informationssicherheit.
- ISO 27001 als Alltagswerkzeug zur Qualitätssicherung und konstanten Weiterentwicklung in der Organisation nutzen.
- Erfüllung der Anforderung der EU zur Auditierung von FKR (Konformitätsaudit).

3. Das ISMS FKR des ASTRA

Im Informationssicherheits-Managementsystem Fahrtschreiberkarten (ISMS FKR) werden alle Verfahren und Regeln dokumentiert, welche dazu dienen, die Informationssicherheit des ASTRA gegenüber ihren Anspruchsgruppen zu gewährleisten. Das ISMS FKR wird laufend kommuniziert und stufengerecht geschult. Die Anwendung dieser Regelungen ist zwingend und verbindlich.

4. Kontinuierliche Verbesserung

Das ISMS FKR wird laufend überprüft und den aktuellen Gegebenheiten angepasst. Im Sinn einer kontinuierlichen Verbesserung werden die Kompetenzen aller beteiligten Stellen laufend weiterentwickelt.

5. Organisation und Verantwortlichkeiten

5.1. Geschäftsleitung

Die Geschäftsleitung ist das oberste operative Entscheidungsorgan der Firma und delegiert Aufgaben, Verantwortung und Kompetenzen in der Informationssicherheit des Fahrtschreiberkartenregisters FKR an den CISO.

5.2. Interne Mitarbeitende / Generell

Alle Mitarbeitenden des ASTRA, welche Tätigkeiten im Geltungsbereich des ISMS FKR verrichten sind für die Informationssicherheit in ihrem Fachbereich verantwortlich. Die Vorgesetzten aller Hierarchiestufen sind verpflichtet, die dafür nötigen Ressourcen und Skills zur Verfügung zu stellen. Sie sind verpflichtet, sämtliche notwendigen Sicherheitsmassnahmen im Rahmen ihres Verantwortungsbereiches nachhaltig umzusetzen. Sie leiten ihre Mitarbeitenden an und schulen sie bedarfsgerecht.

5.3. CISO (chief information security officer)

Der CISO ist verantwortlich für die Erarbeitung und Definition, Überwachung, Steuerung und Betrieb und kontinuierliche Verbesserung des ISMS FKR. Er rapportiert an die Geschäftsleitung.

5.4. Asset Owner

Asset Owner legen Regeln für den zulässigen Gebrauch von ihnen zugeteilten Informationen und Werten fest, dokumentieren diese und wenden sie an.

5.5. Risk Owner

Risk Owner führen den Prozess zur Informationssicherheitsrisikobeurteilung und –Behandlung für ihre zugeteilten Risiken. Sie analysieren und bewerten die Risiken und legen entsprechende Massnahmen fest.

5.6. Externe Mitarbeitende / Mitarbeitende von Dritten

Die Regelungen des ASTRA im Kontext Informationssicherheit gelten entsprechend auch für Personen, welche als Externe oder Mitarbeitende von Dritten im Geltungsbereich des ISMS FKR Tätigkeiten verrichten und sind durch diese einzuhalten.

6. Kontrollen

Das ASTRA überprüft die Informationssicherheit des Fahrtschreiberkartenregisters FKR in geplanten und regelmässigen Abständen mit internen und externen Audits. Die Ergebnisse dieser Kontrollen fliessen in die kontinuierliche Verbesserung ein.

7. Sanktionen

Das ASTRA vereinbart mit Dritten Konventionalstrafen, welche bei wiederholten oder einzelnen schwerwiegenden Verstössen gegen die Sicherheitsvorschriften und –Weisungen eingefordert werden können. Bei den internen Mitarbeitenden kommen in solchen Fällen die arbeitsrechtlichen Sanktionen zur Anwendung.

8. Begriffsdefinitionen

8.1. Informationssicherheit

Unter der Informationssicherheit werden alle Massnahmen verstanden, die zur Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen angeordnet, durchgeführt, überprüft und kontinuierlich verbessert werden. Diese Massnahmen können u. a. organisatorischer, technischer oder baulicher Natur sein.

- Vertraulichkeit: Gewährleistung des Zugangs zu Informationen nur für die Zugangsberechtigten.
- Integrität: Sicherstellen der Unversehrtheit und Vollständigkeit von Informationen und deren Verarbeitungsmethoden.
- Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und den zugehörigen Werten für berechtigte Benutzer.

8.2. Informationssicherheits-Managementsystem (ISMS)

Unter einem ISMS wird verstanden:

- Sämtliche Regeln, Verfahren und Prozesse innerhalb des Anwendungsbereichs, welche die Informationssicherheit definieren, steuern, durchführen, überprüfen, aufrechterhalten und kontinuierlich verbessern.
- Die Dokumentation erfolgt mittels ISMS Framework, den Controls der SOA (Anwendbarkeitserklärung) und mit entsprechenden Policies, Prozessübersichten und weiteren Nachweisdokumenten.

8.3. CISO

Der CISO ist verantwortlich für die Informationssicherheit in seinem zugewiesenen Geltungsbereich.