Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Roads Office FEDRO

POLICY

SISTEMA DI GESTIONE SICUREZZA INFORMAZIONI

REGISTRO CARTE TACHIGRAFICHE

(POLICY ISMS FKR)

V1.0

COLOPHON

Data di redazione:	27.3.2020
Autore:	Gerhard Schuwerk (Shg, CISO ISMS FKR)
Directory/Nome del file:	ISMS-FKR_Policy_v[X.X]_it.docx
Numero di pagine:	7
Data di approvazione:	05.11.2020
Approvato da:	Comitato direttivo FKR (PAS FKR)

Cronologia redazionale

Versione	Data	Autore	Osservazioni
0.1	27.03.2020	Shg	Prima bozza
0.2	06.04.2020	Shg	Bozza ampliata, dopo la definizione del campo di azione ISMS FKR
0.9	08.04.2020	Shg	Versione 1ª tappa
0.9.1	04.05.2020	Shg	Versione con correzioni 1ª tappa
0.9.2	28.05.2020	Shg	Adeguamenti 2ª tappa
0.9.3	12.10.2020	Shg	Adeguamenti UFIT (Operazioni) (obiettivi ISMS)
1.0	05.11.2020	Shg	Approvazione PAS

SOMMARIO

1. Riferimenti e campo di applicazione 4
2. Scopo della sicurezza informazioni 4
3. L'ISMS FKR dell'USTRA 5
4. Ottimizzazione continua 5
5. Organizzazione e responsabilità 5
5.1. Direzione 5
5.2. Personale interno - aspetti generali 5
5.3. CISO (chief information security officer) 5
5.4. Asset owner 5
5.5. Risk owner 5
5.6. Personale esterno / di terzi 6
6. Controlli 6
7. Sanzioni 6
8. Definizioni 6
8.1. Sicurezza informazioni 6
8.2. Sistema di gestione sicurezza informazioni (ISMS) 6
8.3. CISO 6

1. Riferimenti e campo di applicazione

L'Ufficio federale delle strade (USTRA) è certificato secondo la norma ISO 27001:2013, di cui si impegna a rispettare i requisiti, per il sistema di gestione della sicurezza informazioni del registro carte tachigrafiche (ISMS FKR).

La certificazione vale per la Swiss Card Issuing Authority (CH-CIA) relativamente all'emissione di schede tachigrafiche tramite l'applicazione FKR (registro carte tachigrafiche) nel sistema integrale iDFS (tachigrafo intelligente).

Il rilascio di carte tachigrafiche per il Principato del Liechtenstein (Liechtenstein Member State Authority / FL-MSA) è di competenza dell'USTRA ovvero della Svizzera (Swiss Member State Authority / CH-MSA) ai sensi dell'articolo 21 dell'Accordo tra la Confederazione Svizzera e il Principato del Liechtenstein relativo alla circolazione stradale (*SR* 0.741.531.951.4).

L'ISMS FKR prevede esplicitamente:

- l'accesso a FKR per i dipendenti dell'Amministrazione federale delle dogane (ADF)

L'ISMS FKR comprende esplicitamente i seguenti interlocutori, che dispongono di un sistema di gestione sicurezza informazioni:

- il fornitore del software di FKR
- il personalizzatore di schede (CH-CP)
- lo sviluppatore e l'operatore PKI (infrastruttura a chiave pubblica)
- il fornitore delle soluzioni di pagamento

L'ISMS FKR comprende esplicitamente anche il seguente interlocutore, che prevede di implementare un sistema di gestione sicurezza informazioni:

- l'operatore del software

Sono invece esclusi:

- processi esterni a CH-CIA nonché hardware e software di imprese e autisti (di veicoli muniti di tachigrafo), produttori di tachigrafi, officine e autorità preposte al controllo.

2. Scopo della sicurezza informazioni

L'USTRA si è posto i seguenti obiettivi:

- utilizzare un sistema di gestione della sicurezza IT (ISMS) adeguato, che garantisca durevolmente la sicurezza tecnica dei dati legati a tutte le attività rilevanti per l'Ufficio;
- tutelare adeguatamente le informazioni, garantendone disponibilità, riservatezza e integrità;
- rispettare le disposizioni legali, contrattuali e interne in ambito di sicurezza delle informazioni;
- applicare la norma ISO 27001 quale strumento quotidiano per garantire la qualità e uno sviluppo continuo all'interno dell'Ufficio;
- soddisfare i requisiti UE per l'auditing di FKR (audit di conformità).

3. L’ISMS FKR dell’USTRA

Il Sistema di gestione sicurezza informazioni Registro carte tachigrafiche (ISMS FKR) documenta tutte le regole e procedure che servono a garantire la sicurezza dei dati USTRA nei confronti delle diverse categorie di interlocutori. Queste norme sono obbligatorie e vincolanti. Vengono forniti periodicamente informazioni e corsi modulati secondo i livelli inerenti ai diritti di accesso.

4. Ottimizzazione continua

L’ISMS FKR è costantemente verificato e adeguato alle circostanze. Nel quadro di un processo di ottimizzazione continua, vengono costantemente sviluppate le competenze di tutti i soggetti coinvolti.

5. Organizzazione e responsabilità

5.1. Direzione

La Direzione è l’istanza decisionale superiore dell’Ufficio e delega al CISO (chief information security officer) attività, responsabilità e competenze in materia di sicurezza informazioni del registro carte tachigrafiche.

5.2. Personale interno - aspetti generali

Tutti i collaboratori USTRA che svolgono attività nel campo di applicazione di ISMS FKR sono responsabili per la sicurezza dei dati attinenti al loro ambito specifico. I superiori di qualsiasi livello gerarichico sono tenuti a mettere a disposizione le risorse e skill richieste; hanno inoltre l’obbligo di attuare durevolmente le misure di sicurezza necessarie nel loro ambito di responsabilità. Guidano i propri collaboratori e si occupano della loro formazione a seconda delle esigenze.

5.3. CISO (chief information security officer)

Il CISO è incaricato delle attività di sviluppo e concezione, monitoraggio, gestione, esercizio e ottimizzazione continua di ISMS FKR. Risponde alla Direzione.

5.4. Asset owner

I proprietari degli attivi (asset owner) definiscono le regole circa l’uso autorizzato di informazioni e dati a cui hanno accesso, le documentano e le applicano.

5.5. Risk owner

I responsabili operativi (risk owner) gestiscono i rischi di loro competenza relativi alla sicurezza informazioni, predisponendo misure adeguate sulla base dell’analisi e valutazione di tali rischi.

5.6. Personale esterno / di terzi

Le disposizioni dell'USTRA in materia di sicurezza informazioni valgono con effetto vincolante anche per il personale esterno che svolge attività legate all'ambito ISMS FKR, per conto sia dell'Ufficio sia di terzi.

6. Controlli

L'USTRA verifica la sicurezza informazioni del registro carte tachigrafiche a cadenza regolare programmata mediante audit esterni e interni. I risultati di tali controlli confluiscono nel processo di ottimizzazione continua.

7. Sanzioni

L'USTRA conviene con terzi pene convenzionali applicabili in caso di grave violazione una tantum o reiterata delle prescrizioni e istruzioni legate alla sicurezza. Quando il contravventore invece è un collaboratore interno valgono le norme del diritto del lavoro.

8. Definizioni

8.1. Sicurezza informazioni

Per *sicurezza (delle) informazioni* si intendono tutte le misure predisposte, attuate, verificate e continuamente ottimizzate con il fine di salvaguardare riservatezza, integrità e disponibilità dei dati. Tali misure possono essere di carattere organizzativo, tecnico o materiale.

- Riservatezza: accesso alle informazioni solo per gli aventi diritto
- Integrità: garanzia di inviolabilità e integrità delle informazioni nonché della metodologia di trattamento
- Disponibilità: accesso alle informazioni adeguato alle esigenze e al livello di diritti dell'utente.

8.2. Sistema di gestione sicurezza informazioni (ISMS)

Per ISMS si intende l'insieme di regole, procedure e processi del campo di applicazione, che definiscono, impostano, attuano, verificano, mantengono e ottimizzano la sicurezza delle informazioni.

La documentazione è costituita da framework ISMS, controlli della SOA (dichiarazione di applicabilità) e relative policy, controlli delle procedure e altre attestazioni.

8.3. CISO

Il CISO è responsabile per la sicurezza informazioni nel suo ambito di competenza.