



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Roads Office FEDRO

POLITIQUE DU SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION RELATIF AU REGISTRE DES CARTES DE TACHYGRAPHE

(POLITIQUE SMSI RCT)

V.1.0

IMPRESSUM

Date de création / Date de révision :	27.3.2020
Auteur :	Gerhard Schuwerk (Shg, RSSI SMSI RCT)
Répertoire / Nom du fichier :	ISMS-FKR_Policy_v[X.X]_fr.docx
Nombre de pages :	7
Approuvé le :	05.11.2020
Approuvé par :	Comité de pilotage RCT (PAS FKR)

Liste des modifications

Version	Date	Auteur	Remarques
0.1	27.03.2020	Shg	Version initiale
0.2	06.04.2020	Shg	Ajouts après définition du périmètre du SMSI RCT
0.9	08.04.2020	Shg	Version pour l'étape 1
0.9.1	04.05.2020	Shg	Version après corrections lors de la révision de l'étape 1
0.9.2	28.05.2020	Shg	Adaptations après l'étape 2
0.9.3	12.10.2020	Shg	Adaptations liées au projet de certification SMSI des services chargés de l'exploitation à l'OFIT
1.0	05.11.2020	Shg	Approbation par le comité de pilotage

TABLE DES MATIÈRES

1.	Contexte et champ d'application	4
2.	Objectifs de la sécurité des informations	4
3.	Le SMSI RCT de l'OFROU	5
4.	Amélioration permanente	5
5.	Organisation et responsabilités	5
5.1.	Direction	5
5.2.	Collaborateurs internes / Généralités	5
5.3.	RSSI (responsable de la sécurité du système d'information)	5
5.4.	Propriétaires d'actifs	5
5.5.	Propriétaires de risques	5
5.6.	Collaborateurs externes / Collaborateurs de tiers	6
6.	Contrôles	6
7.	Sanctions	6
8.	Définitions	6
8.1.	Sécurité de l'information	6
8.2.	Système de management de la sécurité de l'information (SMSI)	6
8.3.	RSSI	6

1. Contexte et champ d'application

L'Office fédéral des routes (OFROU) a obtenu une certification en matière de système de management de la sécurité de l'information relatif au registre des cartes de tachygraphe (SMSI RCT) selon la norme ISO 27001:2013 et s'engage à satisfaire les exigences applicables.

La certification s'applique à l'autorité suisse d'émission de cartes (*Swiss Card Issuing Authority* ; CH-CIA) chargée de la délivrance des cartes de tachygraphe (CT) sur la base de l'application métier Registre des cartes de tachygraphe (RCT), dans le système global du « tachygraphe intelligent » (TI).

En vertu de l'art. 21 de l'accord sur la circulation routière entre la Confédération suisse et la Principauté de Liechtenstein (RS 0.741.531.951.4), la délivrance de cartes de tachygraphe pour la Principauté de Liechtenstein (Liechtenstein Member State Authority / FL-MSA) est du ressort de l'OFROU, autrement dit de la Suisse (Swiss Member State Authority / CH-MSA).

Le SMSI RCT inclut explicitement :

- l'accès des collaborateurs de la douane (AFD) au RCT.

Le SMSI RCT inclut explicitement les prestataires suivants qui présentent un SMSI :

- le fournisseur du logiciel pour le RCT ;
- le personnalisateur de cartes (CH-CP) ;
- le développeur et l'exploitant de l'ICP (Infrastructure à clés publiques) ;
- le prestataire proposant les solutions de paiement.

Le SMSI RCT inclut explicitement les prestataires suivants qui présentent un projet de SMSI :

- l'exploitant du logiciel.

Le SMSI RCT exclut :

- les processus externes à la CH-CIA ainsi que le matériel et les logiciels des entreprises et des chauffeurs (tachygraphe dans le véhicule), des fabricants de tachygraphes, des ateliers et des autorités de contrôle.

2. Objectifs de la sécurité des informations

L'OFROU a fixé les objectifs suivants :

- Utiliser un système approprié de management de la sécurité de l'information (SMSI) garantissant durablement la sécurité informatique de toutes les activités utiles à l'accomplissement de ses tâches.
- Protéger les informations de façon adéquate pour garantir leur disponibilité, leur confidentialité et leur intégrité.
- Satisfaire les exigences légales, contractuelles et internes dans le domaine de la sécurité de l'information.
- Utiliser la norme ISO 27001 comme un instrument du quotidien pour garantir la qualité et un développement constant au sein de l'organisation.
- Satisfaire l'exigence de l'UE concernant l'audit du RCT (audit de conformité).

3. Le SMSI RCT de l'OFROU

Le système de management de la sécurité de l'information relatif au registre des cartes de tachygraphe (SMSI RCT) documente l'ensemble des procédures et règles qui servent à garantir la sécurité des informations de l'OFROU vis-à-vis des groupes d'interlocuteurs de ce dernier. Le SMSI RCT fait l'objet de communications régulières et des formations en la matière sont dispensées à chaque niveau. L'application de ces règles est obligatoire et contraignante.

4. Amélioration permanente

Le SMSI RCT est régulièrement contrôlé et adapté à la situation. Dans un souci d'amélioration permanente, toutes les parties prenantes développent régulièrement leurs compétences.

5. Organisation et responsabilités

5.1. Direction

La direction est le premier organe décisionnel de l'entreprise au niveau opérationnel. Elle délègue au RSSI les tâches, les responsabilités et les compétences en matière de sécurité de l'information du RCT.

5.2. Collaborateurs internes / Généralités

Tous les collaborateurs de l'OFROU qui exercent des activités dans le champ d'application du SMSI RCT sont responsables de la sécurité de l'information dans leur domaine de spécialité. Quel que soit leur niveau, les supérieurs hiérarchiques sont tenus non seulement de mettre à la disposition de leurs collaborateurs les ressources et les compétences nécessaires, mais également de mettre en œuvre durablement toutes les mesures de sécurité indispensables dans leur domaine de responsabilité. Ils guident leurs collaborateurs et les forment en fonction des besoins.

5.3. RSSI (responsable de la sécurité du système d'information)

Le RSSI est chargé d'élaborer, de définir, de surveiller, de piloter, d'exploiter et d'améliorer continuellement le SMSI RCT. Il rend compte de ses travaux à la direction.

5.4. Propriétaires d'actifs

Les propriétaires d'actifs définissent des règles concernant l'usage licite des informations et des valeurs qui leur sont confiées, les documentent et les appliquent.

5.5. Propriétaires de risques

Les propriétaires de risques gèrent le processus d'évaluation et de traitement des risques en matière de sécurité de l'information pour les risques qui leur sont attribués. Ils analysent et évaluent les risques, et définissent des mesures ad hoc.

5.6. Collaborateurs externes / Collaborateurs de tiers

Les personnes exerçant en qualité d'externes ou de collaborateurs de tiers des activités entrant dans le champ d'application du SMSI RCT sont également soumises aux règles de l'OFROU en matière de sécurité des informations et doivent les respecter.

6. Contrôles

L'OFROU contrôle la sécurité des informations du RCT à intervalles réguliers et planifiés au moyen d'audits internes et externes. Les résultats de ces contrôles contribuent à l'amélioration permanente.

7. Sanctions

L'OFROU convient avec les tiers de peines conventionnelles pouvant être exigées en cas d'infractions graves isolées ou répétées contre les prescriptions et les instructions en matière de sécurité. Si les collaborateurs internes commettent de tels actes, les sanctions applicables seront celles prévues par le droit du travail.

8. Définitions

8.1. Sécurité de l'information

Par « sécurité de l'information », on entend l'ensemble des mesures qui sont ordonnées, exécutées, contrôlées et améliorées en permanence dans le but de préserver la confidentialité, l'intégrité et la disponibilité des informations. Ces mesures peuvent notamment revêtir un caractère organisationnel ou technique voire prendre la forme d'aménagements.

- Confidentialité : garantir l'accès aux informations aux seules personnes habilitées.
- Intégrité : garantir l'inaltération et l'exhaustivité des informations et de leurs méthodes de traitement.
- Disponibilité : garantir aux utilisateurs habilités l'accès aux informations et aux valeurs y relatives.

8.2. Système de management de la sécurité de l'information (SMSI)

Par « SMSI », on entend :

- l'ensemble des règles, procédures et processus au sein du champ d'application, qui définissent, pilotent, assurent, contrôlent, préservent et améliorent en permanence la sécurité de l'information.
- Le cadre SMSI, les mesures de sécurité de la déclaration d'applicabilité de même que les politiques en la matière, les vues d'ensemble des processus et d'autres pièces justificatives constituent la documentation du système.

8.3. RSSI

Le RSSI est responsable de la sécurité de l'information dans le domaine de compétences qui lui est assigné.

