Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Office fédéral des routes OFROU**

INSTRUCTIONS

# OT SECURITY GOVERNANCE

*Sécurité des systèmes EES*

*Édition 2022 V1.00*
*ASTRA 73006*

# Impressum

**Auteurs**

| | |
|---|---|
| Schnetz Jean-Paul | OFROU DS-DTI, présidence |
| Martin Wyss | OFROU I-B |
| Markus Eisenlohr | OFROU I-FU |
| Manfred Jungo | OFROU DS |
| Wolfgang Hoffmann | OFROU DS-GOV |
| Bruno Frey | OFROU DS-GOV |
| Daniel Gähwiler | CSI Consulting, Zurich |

**Groupe de suivi**

| | |
|---|---|
| Bernard Crausaz | OFROU DS-UARS |
| Mario Pfammatter | OFROU DS-UARS |

**Traduction**
François Jamme, la version originale en allemand fait foi.

**Éditeur**
Office fédéral des routes OFROU
Division réseaux routiers N
Standards et sécurité de l'infrastructure SSI
3003 Berne

**Sources**
Le document peut être téléchargé gratuitement sur le site www.ofrou.admin.ch.

© OFROU 2022
Reproduction - hors utilisation commerciale - autorisée sous réserve de mention de la source.

# Avant-propos

Les progrès de la technique et les exigences croissantes en matière d'infrastructures routières nécessitent des prescriptions uniformisées y compris en ce qui concerne la sécurité. Sur le réseau routier, cette dernière, notamment dans le domaine des possibles nouveaux points d'attaque, est une de nos priorités.

Les présentes instructions définissent l'OT Security Governance d'ordre supérieur dans le domaine des EES ainsi que les systèmes OT (Operational Technology) y afférents. La différence entre les systèmes IT et OT est également mise en lumière, de pair avec leurs domaines d'application et leurs spécificités.

Cette OT Security Governance fournit une structure d'ordre supérieur permettant de soutenir les objectifs commerciaux liés à l'OT-Security aux niveaux stratégique, fonctionnel et opérationnel.

**Office fédéral des routes**

Jürg Röthlisberger
Directeur

# Table des matières

**Impressum** ..... **2**
**Avant-propos** ..... **3**

**1 Introduction** ..... **7**
1.1 But ..... 7
1.2 Champ d'application ..... 7
1.3 Bases légales, normes et standards déterminants ..... 7
1.4 Destinataires ..... 7
1.5 Entrée en vigueur et modifications ..... 7

**2 Sécurité au sein de l'administration fédérale** ..... **8**
2.1 Aperçu des bases légales au sein de la Confédération ..... 8
2.2 Niveaux organisationnels au sein de l'administration fédérale ..... 8
2.3 Mise en œuvre au sein de l'OFROU, domaine EES ..... 9

**3 Différenciation technologies de l'information et opérationnelles** ..... **10**
3.1 La sécurité OT en lien avec les EES expliquée en bref ..... 10
3.2 Points clés IT et OT ..... 10

**4 OT Security Governance** ..... **11**
4.1 Objectifs spécifiques de l'OT Security Governance ..... 11

**5 Cadre et fondement** ..... **12**
5.1 Éléments de l'OT-SMS ..... 12
5.1.1 Bases : normes, lois, directives informatiques de la Confédération ..... 12
5.1.2 Audit et controlling ..... 12
5.1.3 Analyse / Évaluation des risques ..... 12
5.2 Éléments de base de l'OT-SMS ..... 13
5.2.1 Règles : processus, rôles et organisation ..... 13
5.2.2 Personnes : qualification et formation des collaborateurs ..... 13
5.2.3 Technologie : prescriptions techniques ..... 13
5.3 Cadre ..... 13
5.4 Structures organisationnelles OT Security Governance (responsabilités) ..... 14
5.4.1 Pilotage ..... 14
5.4.2 Mise en œuvre ..... 14
5.4.3 Exploitation ..... 15

**Glossaire** ..... **17**
**Bibliographie** ..... **19**
**Liste des modifications** ..... **20**

# 1 Introduction

## 1.1 But

Les présentes instructions couvrent le cadre réglementaire pour l'OT Security Governance de la technique de pilotage et de commande des EES (systèmes OT). Elles couvrent :

- les objectifs de l'OT Security Governance (voir chap. 4.1) ;
- les différents éléments constitutifs permettant de soutenir les niveaux stratégique, fonctionnel et opérationnel ;
  - les règles : processus, rôles et organisation ;
  - les personnes : qualification et formation des collaborateurs ;
  - la technologie : prescriptions techniques ;
- la différenciation entre IT et OT sur les routes nationales (voir chap. 3) ;
- les principaux organes de l'organisation de sécurité OT (voir chap. 5.4).

## 1.2 Champ d'application

Les présentes instructions valent pour la planification, l'élaboration, la réalisation et l'exploitation de tous les systèmes OT des routes nationales. Elles sont contraignantes et doivent être impérativement respectées lors de l'intégration des installations sur le réseau IP EES.

Les systèmes OT des routes nationales font partie intégrante des routes nationales et sont de ce fait soumis à l'ordonnance sur les routes nationales (ORN). Partant, ils ne sont pas concernés par les directives W007 (Directives du Conseil fédéral concernant les projets informatiques de l'administration fédérale et le portefeuille informatique de la Confédération).

## 1.3 Bases légales, normes et standards déterminants

L'élaboration, l'exploitation et l'utilisation d'installations EES, domaines de l'Operational Technology compris, ne peuvent se faire que conformément aux dispositions légales en vigueur. Il incombe aux maîtres d'ouvrage, planificateurs, fournisseurs et exploitants de respecter les prescriptions et les normes applicables à leur domaine (voir bibliographie).

## 1.4 Destinataires

Les présentes instructions s'adressent en premier lieu aux collaborateurs de l'OFROU et aux exploitants des systèmes OT. Dans un deuxième temps, elles fournissent aux maîtres d'ouvrage, concepteurs de projet et planificateurs des informations importantes sur l'organisation de sécurité OT des routes nationales.

## 1.5 Entrée en vigueur et modifications

Les présentes instructions entrent en vigueur le 31.10.2022. Le « liste des modifications » est documenté en page 20.

# 2 Sécurité au sein de l'administration fédérale

## 2.1 Aperçu des bases légales au sein de la Confédération

La figure suivante donne un aperçu des bases légales devant être respectées. Il existe des exceptions aux prescriptions en matière de sécurité de l'information et de protection des données pour les EES (équipements d'exploitation et de sécurité) spécifiques. Celles-ci sont mises en œuvre de manière ciblée.

*Fig. 2.1 Prescriptions en matière de sécurité de l'information et de protection des données*

## 2.2 Niveaux organisationnels au sein de l'administration fédérale

Le Centre national pour la cybersécurité (National Cyber Security Centre – NCSC) est le centre de compétences de la Confédération en matière de cybersécurité. Service spécialisé de la Confédération en matière de sécurité informatique, le NCSC édicte des prescriptions relatives à la cybersécurité au sein de l'administration fédérale (autoprotection), vérifie leur respect et aide les prestataires de services à supprimer les points faibles. Le SG du DETEC ventile les prescriptions fédérales d'ordre supérieur sur le département et ses offices. L'OFROU définit les prescriptions spéciales pour le réseau de routes nationales dans le domaine des EES et reprend ce faisant par analogie les prescriptions applicables aux systèmes OT.

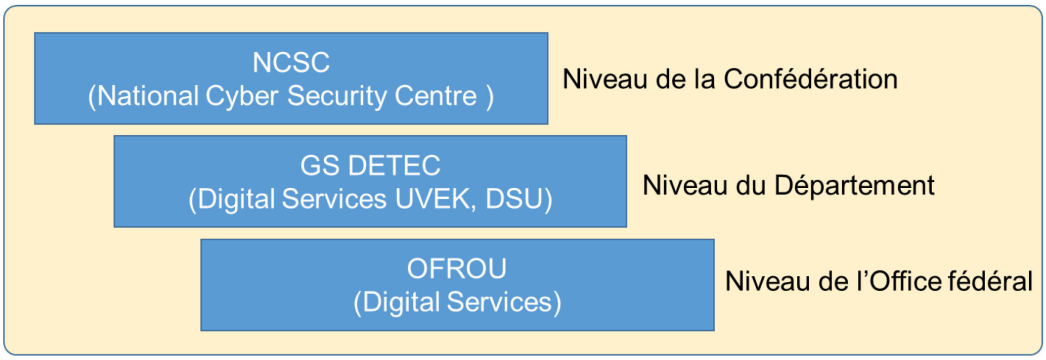


*Fig. 2.2 Niveaux organisationnels au sein de l'administration fédérale*

Les prescriptions suivantes sont en particulier déterminantes en ce qui concerne la sécurité OT de l'OFROU :

- loi fédérale sur la protection des données et ordonnance y afférente (LPD et OLPD) [1], [4] ;
- ordonnance concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations, OPrI) [5] ;
- ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy) [6] ;
- ordonnance sur la transformation numérique et l'informatique (OTNI) [7] ;
- stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) [9] ;
- Si001 - Protection informatique de base dans l'administration fédérale (Chancellerie fédérale ChF, Centre national pour la Cybersécurité NCSC) [15].

## 2.3 Mise en œuvre au sein de l'OFROU, domaine EES

S'agissant des EES, il existe quelques autorisations spéciales visant à garantir la sécurité sur les routes nationales. Elles permettent une mise en œuvre, adaptée aux besoins, des bases légales existant du fait de la différenciation IT/OT (voir chapitre 3).

Les chapitres suivants donnent une description des prescriptions propres à l'OFROU en ce qui concerne les routes nationales.

# 3 Différenciation technologies de l'information et opérationnelles

## 3.1 La sécurité OT en lien avec les EES expliquée en bref

OT fait référence à Operational Technology (technologie opérationnelle) et correspond à l'utilisation de systèmes composés de matériels et de logiciels permettant de piloter les installations.

Les équipements d'exploitation et de sécurité (EES) comprennent des installations électromécaniques ainsi que de pilotage et de commande utilisées pour assurer l'exploitation et la sécurité des routes nationales.

Les OT couvrent ainsi les techniques de pilotage et de commande des EES, l'infrastructure nécessaire à cette fin (p. ex. réseau IP EES), les systèmes OT ainsi que les applications et services. Les systèmes et agrégats OT font partie des EES.

## 3.2 Points clés IT et OT

Ci-après une description de l'importance des différences entre les problématiques IT et OT, ce qui permet de comprendre pourquoi il convient de les traiter séparément.

*Fig. 3.3 Différenciation entre les problématiques IT et OT*

| **Champs d'application** | **IT** | **OT** |
|---|---|---|
| Principaux points d'utilisation | Bureautique / Automatisation / Applications spécialisées sans fonction opérationnelle. | Pilotage et régulations fiables, surveillance et contrôle des machines, installations et processus / Applications spécialisées et applications avec fonction opérationnelle (p. ex. pilotage d'installations). |
| Type de l'activité | Focalisation sur l'interaction transactionnelle entre l'homme et l'application. | Interactions basées sur les résultats entre les conditions et le système de processus. |
| **Thèmes de sécurité** | **IT** | **OT** |
| Objectifs en termes de sécurité | Confidentialité<br>Intégrité<br>Disponibilité | Sécurité fonctionnelle<br>Fiabilité<br>Disponibilité |
| Données / Informations critiques | Données commerciales (y. c. données financières)<br>Données personnelles | Données du système de commande (signaux de pilotage des capteurs de données) |
| Intégrité | Critique selon le contexte | Intégrité critique selon le contexte, possibles effets sur la vie, le corps et l'environnement |
| Disponibilité | En règle générale, pendant les heures de travail / Des applications telles que le SIAC, ETC et d'autres constituent des exceptions au sein de l'OFROU. | Élevée, temps réel (365 jours / an, 24h sur 24) |
| Durée de vie de la technologie | 3 à 5 ans ; grand nombre de prestataires ; élargissements très nombreux / Gestion permanente du cycle de vie des technologies employées. | 10 à 20 ans ; normalement, même fournisseur dans le temps ; la fin de vie du produit donne naissance à de nouvelles questions de sécurité. |
| Gestion des modifications | Régulière et planifiée ; coordonnée avec les durées minimales d'utilisation. | Planification stratégique ; pas un simple processus basé sur les effets sur la production. |
| Sécurité physique et liée à l'environnement | Va de faible (systèmes de bureautique) à excellente (systèmes informatiques critiques). | Normalement excellente pour les domaines critiques ; maturité variable dépendant du caractère critique / de la culture. |

# 4 OT Security Governance

L'OT-Security Governance (en abrégé OT Sec Gov) règle la sécurité des systèmes OT et garantit une disponibilité, une intégrité et une fiabilité élevées des techniques de pilotage et de commande des EES des routes nationales. Elle permet également une coordination des stratégies de sécurité OT et des objectifs commerciaux dans le domaine des EES et vient les soutenir. Elle doit en outre de veiller à ce que ces stratégies respectent les lois et prescriptions en vigueur grâce à un suivi scrupuleux des directives et à la réalisation de contrôles internes et à ce que les responsabilités et compétences pour ce faire soient clairement définies. La gouvernance doit par conséquent préciser qui est autorisé à prendre des décisions, elle doit fixer le cadre nécessaire à la reddition des comptes et permettre une surveillance garantissant une réduction des risques à un niveau approprié.

## 4.1 Objectifs spécifiques de l'OT Security Governance

Élaboration, suivi et surveillance du cadre de l'OT Security Governance, notamment :

- définition, prescription et surveillance de standards et de « best practices » selon un équilibre optimal entre performance et conformité pour toutes les disciplines de la prestation de services (projet OT sur toutes les phases mais aussi exploitation OT des applications spécialisées ou des applications dotées d'une fonction opérationnelle) ainsi que pour l'évaluation des risques ;
- définition, prescription et vérification du respect des prescriptions ; garantie d'un accompagnement adéquat des projets OT et des applications spécialisées ou des applications dotées d'une fonction opérationnelle grâce à l'exercice d'un rôle d'architecture directrice ;
- examen par le PSIO de la pertinence d'une mise en œuvre des directives informatiques pour les routes nationales ;
- garantie du respect des prescriptions légales, de portée fédérale et de portée départementale liées à l'OT et aux systèmes d'intégration.

# 5 Cadre et fondement

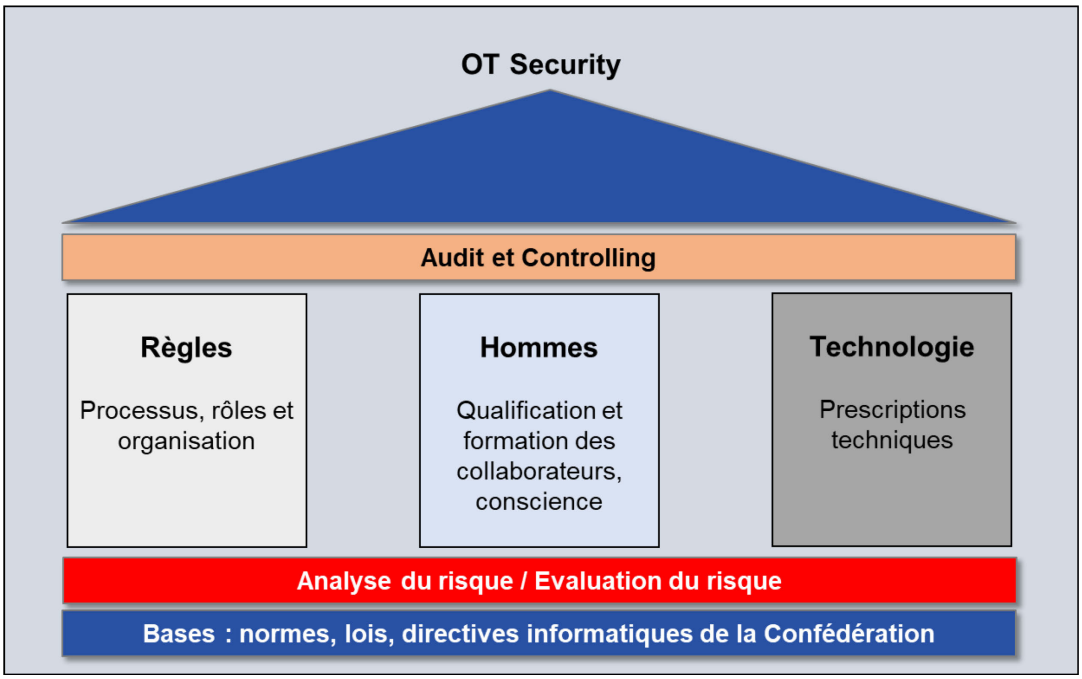


*Fig. 5.4 OT Security Management System (OT-SMS)*

## 5.1 Éléments de l'OT-SMS

Les trois éléments de base sont intégrés dans trois éléments d'importance mis en lumière dans les sous-chapitres qui suivent.

### 5.1.1 Bases : normes, lois, directives informatiques de la Confédération

Dispositions d'exécution portant sur l'utilisation des documents de base, notamment sur l'application des directives informatiques de la Confédération (transformation numérique et gouvernance de l'informatique), l'applicabilité à l'infrastructure des routes nationales devant être étudiée de manière séparée.

### 5.1.2 Audit et controlling

Prescriptions et dispositions relatives aux audits ou au contrôle régulier de l'OT-SMS et de sa mise en œuvre. Il existe des plans d'examen, des listes de contrôle et des protocoles de réception pour ce qui est des tâches d'audit et de controlling mais aussi des activités d'assurance qualité.

### 5.1.3 Analyse / Évaluation des risques

L'analyse et l'évaluation des risques indique ce contre quoi il convient de se prémunir et selon quelle priorité. La gestion du risque est exploitée de manière centralisée, en fonction des projets et dans une optique d'exploitation.

L'analyse des risques consiste en l'analyse des risques déterminés sur la base de l'identification des risques liés à différentes configurations et situations de danger.

L'évaluation des risques consiste en l'évaluation des risques individuels ou des risques généraux effectuée par le preneur des risques ou par des tiers et auxquels le preneur des risques est exposé.

## 5.2 Éléments de base de l'OT-SMS

Les sous-chapitres suivants donnent un aperçu des éléments constitutifs que sont les règles, les hommes et la technologie.

### 5.2.1 Règles : processus, rôles et organisation

Prescriptions et dispositions relatives aux rôles, tâches, compétences et responsabilité, par exemple :

- SPoC (Single Point of Contact) ;
- Processus de remontée ;
- Règles d'entrée et d'accès.

### 5.2.2 Personnes : qualification et formation des collaborateurs

Prescriptions et dispositions relatives aux qualifications et à la formation des collaborateurs, par exemple :

- formations à la sécurité et activités de sensibilisation ;
- garantie de savoir-faire.

### 5.2.3 Technologie : prescriptions techniques

Prescriptions et dispositions relatives aux systèmes techniques et à la façon de les utiliser, par exemple :

- Security Monitoring (récolte et analyse d'informations en provenance de sources [de connexion] des plus variées afin de détecter sur le réseau les évènements concernant la sécurité, en d'autres termes les comportements douteux ou les modifications non autorisées du système).
- IAM EES (Identity und Access Management des EES)
- Log Management (définition, réception, stockage et suppression des données de protocole transmises au Security Monitoring).

## 5.3 Cadre

Le cadre est arrêté dans les directives, standards, manuels spécialisés, mémos techniques, guides et autres documentations.

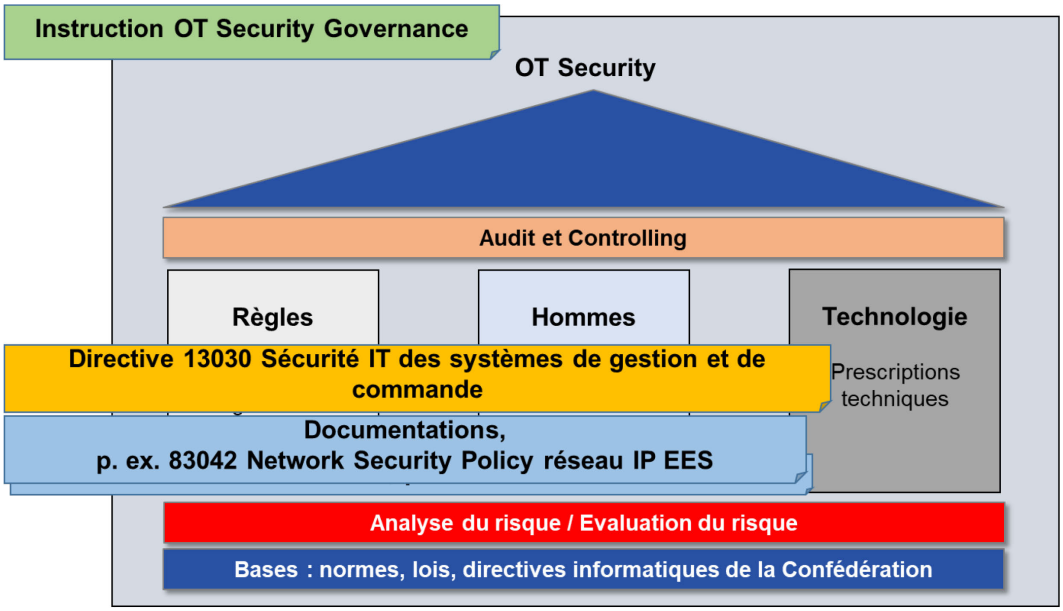


*Fig. 5.5 Documents de l'OT-SMS*

Le cadre est défini au travers des documents suivants :

- **Instructions 73006 OT Security Governance**

  Instructions constituant le cadre réglementaire pour l'OT Security Governance de la technique de pilotage et de commande des EES.

- **Directive 13030 « Sécurité IT des systèmes de gestion et de commande des équipements d'exploitation et de sécurité »**

  Directive décrivant le QUOI ainsi que les concepts de sécurité sous-jacents afin de minimiser les risques identifiés.

- **Documentations**

  Les documentations décrivent le COMMENT et définissent des mesures concrètes de mise en œuvre ainsi que les systèmes de sécurité, par exemple l'IAM EES ou la Network Security Policy réseau IP EES.

## 5.4 Structures organisationnelles OT Security Governance (responsabilités)

Les questions organisationnelles sont définies dans plusieurs domaines.

- Pilotage : adapter, planifier et organiser ;
- Mise en œuvre : constituer, acquérir et mettre en service ;
- Exploitation : mettre à disposition, exploiter et apporter un soutien.

### 5.4.1 Pilotage

Le pilotage d'ordre supérieur se fait au travers du **Change Advisory Board OT-Security (CAB-OT-Sec)**. Le Change Advisory Board est un groupe de personnes chargé d'évaluer les changements dans l'environnement OT. En sont membres des représentants de l'OFROU (gestionnaires produits, centraux, réseau IP EES Security, exploitation de l'infrastructure et filiale) ainsi que l'unité territoriale.

Ci-après les principaux aspects :

- s'assure que tous les documents de sécurité, instructions et directives nécessaires soient élaborés, actualisés si nécessaires et mis en œuvre de manière conséquente ;
- veille à ce que le processus de sécurité soit imbriqué dans le processus de gestion des risques de l'entreprise, à ce qu'il soit méthodiquement intégré et à ce que les prescriptions en provenance du processus de gestion des risques soient respectées.

### 5.4.2 Mise en œuvre

La mise en œuvre est du ressort des gestionnaires de produits, de l'organisation d'exploitation réseau IP EES d'ordre supérieur et des chefs de projets des filiales, mais aussi de l'Information Security Officer (EES) des unités territoriales.

Ci-après les principaux aspects :

- assure la direction technique de la sécurité des informations pour ce qui a trait aux OT et fixe les priorités en matière d'activités en fonction de la situation ;
- veille à ce que les nouvelles thématiques importantes pour la sécurité soient identifiées, analysées et, le cas échéant, traitées ;
- s'assure que les rapports destinés à la direction commerciale soient corrects en termes de contenu, de délais, de niveau hiérarchique et qu'ils soient faits de manière systématique.

### 5.4.3 Exploitation

L'exploitation est du ressort des unités territoriales et de l'organisation de l'exploitation d'ordre supérieur réseau IP EES Security ainsi que I-B.

Ci-après les principaux aspects :

- s'assure que le savoir-faire et les ressources correspondants soient bien disponibles au sein de la gestion globale de la sécurité ;
- veille à ce que les examens périodiques, audits et tests de pénétration (analyses de vulnérabilité) soient bien réalisés ;
- fournit les informations obligatoires lors des incidents relevant de la sécurité.

# Glossaire

| Terme | Signification |
|---|---|
| ChF | Chancellerie fédérale |
| BSA<br>*EES* | Betriebs- und Sicherheitsausrüstungen<br>*Équipements d'exploitation et de sécurité* |
| CAB | Change Advisory Board |
| OPCy | Ordonnance sur les cyberrisques |
| LPD | Loi sur la protection des données |
| ETC | Easy Way for Traffic Control |
| GOV | Governance |
| SG | Secrétariat général du DETEC |
| IAM BSA | Identité et Access Management BSA |
| I-B | Domaine dans le département infrastructure, domaine spécialisé Exploitation |
| PSIDCF | Préposé à la sécurité informatique des départements et de la Chancellerie fédérale |
| PSIO | Préposé à la sécurité informatique de l'organisation |
| TIC | Technique d'information et de communication |
| IdO | Internet des objets |
| IP | Internet protocol |
| IT | Information Technology |
| SIAC | Système d'information d'admission à la circulation |
| OPrI | Ordonnance concernant la protection des informations |
| Coll | Collaborateur |
| SNPC | Stratégie nationale de protection de la Suisse contre les cyberrisques |
| NCSC | Centre national pour la cybersécurité (National Cyber Security Centre) |
| OT | Operational Technology |
| OT-SMS | Operational Technology Security Management System |
| SPOC | Single Point of Contact |
| DETEC | Département fédéral de l'environnement, des transports, de l'énergie et de la communication |
| OLPD | Ordonnance relative à la loi fédérale sur la protection des données |
| OTNI | Ordonnance sur la transformation numérique et l'informatique |

# Bibliographie


**Lois fédérales**

[1] Confédération suisse (1992), **« loi fédérale sur la protection des données (LPD) »**, *RS 235.1*, www.admin.ch.

[2] Confédération suisse (1960), **« loi fédérale les routes nationales » (LRN) »**, *RS 725.11*, www.admin.ch.

[3] Confédération suisse (1958), **« loi fédérale sur la circulation routière (LCR) »**, *RS 741.01*, www.admin.ch.

**Ordonnances**

[4] Confédération suisse (1993), **« ordonnance relative à la loi fédérale sur la protection des données (OLPD) »**, *RS 235.11*, www.admin.ch.

[5] Confédération suisse (2007), **« ordonnance concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations, OPrI) »**, *RS 510.411*, www.admin.ch.

[6] Confédération suisse (2020), **« ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy) »**, *RS 120.73*, www.admin.ch.

[7] Confédération suisse (2020), **« ordonnance sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (ordonnance sur la transformation numérique et l'informatique, OTNI) »**, *RS 172.010.58*, www.admin.ch.

[8] Confédération suisse (2007), **« ordonnance sur les routes nationales (ORN) »**, *RS 725.111*, www.admin.ch.

**Directives et documents stratégiques**

[9] Confédération suisse, **« Stratégie nationale de protection de la Suisse contre les cyberrisques »** (SNPC 2018-2022)

[10] Confédération suisse, **« Stratégie Réseaux de la Confédération »** de novembre 2018

[11] Confédération suisse, **« Directive relative aux décisions concernant les exploitants et l'approvisionnement informatiques au DETEC »** du 01/01/2022.

[12] Confédération suisse, **« Directive concernant l'utilisation des moyens informatiques au DETEC »** du 01/01/2022

[13] Confédération suisse, **« Directive relative au pilotage, à la gestion et au contrôle de l'informatique et de la numérisation au DETEC »** du 01/01/2022

[14] Confédération suisse, **« Directive concernant l'architecture d'entreprise du DETEC »** du 01/01/2022

[15] Confédération suisse, **« Directive Si001 – Protection informatique de base dans l'administration fédérale – version 5.0 »** du NCSC du 23/02/2022

# Liste des modifications

| Édition | Version | Date | Modifications |
|---|---|---|---|
| 2022 | 1.00 | 31.10.2022 | Entrée en vigueur de l'édition 2022 (version originale en allemand). |