

Version réglementation	<b>2-0</b>	Classement de confidentialité	<b>intern</b>
Valable dès le	<b>01.11.2020</b>	Propriétaire	<b>IT-SR</b>
		Processus	-
		Langues disponibles	<b>DE, FR, IT</b>
Divisions	<b>Infrastructure, Voyageurs, Cargo, Immobilier, groupe</b>		
Utilisateurs spécifiques/Destinataires	<b>LIDI-R: A2, A20</b>		
Remplace	<b>Version réglementation 1-0</b>		
Attribution	<b>K 018.4</b>		

## Utilisation des outils IT et des données commerciales

### Table des matières

<b>1.</b>	<b>Généralités .....</b>	<b>2</b>
1.1.	Situation initiale, objectifs.....	2
1.2.	Champ d'application (entreprises, utilisateurs/fonction).....	2
<b>2.</b>	<b>Mes outils .....</b>	<b>2</b>
2.1.	Utilisation des outils IT .....	2
2.2.	Mots de passe.....	2
2.3.	Conditions d'utilisation des outils IT spécifiques .....	2
<b>3.</b>	<b>Traitement de l'information.....</b>	<b>3</b>
3.1.	Classification.....	3
3.2.	Confidentialité et secret .....	4
3.3.	Sauvegarde des données .....	5
3.4.	Envoi de documents .....	5
3.5.	Supports de données mobiles .....	5
<b>4.</b>	<b>Incidents liés à la sécurité .....</b>	<b>5</b>
<b>5.</b>	<b>Logiciels et applis.....</b>	<b>6</b>
<b>6.</b>	<b>Utilisation à des fins privées, droits individuels et surveillance .....</b>	<b>6</b>
6.1.	Utilisation à des fins privées .....	6
6.2.	Droits individuels et surveillance .....	6

### Journal des modifications

Version	Chapitre	Modification
2-0	3.1	Changement des règles de classification en raison du Azure Information Protection
1-0		Première édition, remplacement pour K 400.5, K 400.8, K 400.9, K 400.33, K 400.43, K 400.44

## 1. Généralités

### 1.1. Situation initiale, objectifs

Dans le cadre de la protection des données personnelles et des informations confidentielles, ainsi que des systèmes informatiques et de l'ensemble de l'exploitation, il est crucial de se montrer minutieux dans l'utilisation des outils IT et des données commerciales.

### 1.2. Champ d'application (entreprises, utilisateurs/fonction)

Ces dispositions concernent l'ensemble des collaborateurs qui utilisent les outils IT et les données commerciales au sein de CFF SA ou de CFF Cargo SA.

## 2. Mes outils



Des outils IT sont par principe mis à la disposition des collaborateurs des CFF pour leur permettre de mener à bien leurs tâches. Les collaborateurs et ceux des fournisseurs et partenaires peuvent toutefois utiliser également leurs propres outils IT. Ces outils sont baptisés «Bring your own Device», abrégé «BYOD».

### 2.1. Utilisation des outils IT



Tu te montres minutieux dans l'utilisation des outils IT mis à ta disposition par les CFF, afin de les protéger contre tout dommage ou perte.



Tu ne laisses pas tes outils IT fonctionner sans surveillance. Tu verrouilles tes outils IT avant de quitter ton poste de travail. Tu ne prêtes pas tes outils IT contenant des données commerciales des CFF à des tiers.



Tu peux verrouiller à tout moment ton ordinateur fixe ou portable en utilisant la combinaison de touches **Windows + L** ou (**Control+Alt+Suppr, Entrée**). De même, il t'est possible de verrouiller ta tablette ou ton smartphone avec le bouton d'arrêt.

### 2.2. Mots de passe



**Tu gardes secrets tes mots de passe personnels et ne les partages avec personne. Tu saisis ton mot de passe à l'abri des regards de tiers. Les mots de passe professionnels ne doivent pas être utilisés pour des services privés.**



Un mot de passe long offre une sécurité accrue. Réfléchis ainsi à une suite de caractères au hasard. Choisis une combinaison de mots dont tu te souviendras aisément, qui posera le plus de difficultés possibles pour des hackers.

### 2.3. Conditions d'utilisation des outils IT spécifiques



Des conditions d'utilisation complémentaires peuvent s'appliquer à certains outils et services IT. Les dispositions correspondantes te seront transmises avec l'équipement ou à l'activation du service en question. Les outils IT sont par ailleurs protégés par des mesures techniques. Ces «politiques sur les terminaux» garantissent une protection minimale (avec par exemple un code

à saisir obligatoirement sur smartphone, assorti d'un verrouillage après un certain temps).



**Il est interdit de supprimer ou de contourner les mesures techniques de protection.**

Il t'appartient d'appliquer la protection minimale suivante pour accéder à des données commerciales depuis un terminal privé («BYOD»), qui n'est pas administré par les CFF:

- mot de passe d'accès au terminal d'au moins 4 chiffres,
- verrouillage automatique après 5 minutes,
- cryptage de l'appareil,
- iOS: suppression de toutes les données (rétablissement complet de la configuration d'usine) après dix essais infructueux de saisie du mot de passe du terminal.
- Android: suppression de toutes les données dans l'espace de travail des CFF après dix essais infructueux de saisie du mot de passe du terminal.



Tu trouveras [ici](#) toutes les informations d'accès depuis les terminaux mobiles, en particulier en cas d'entrée en fonction, de mutation ou de départ, de changement de terminal et d'utilisation d'un terminal privé («BYOD»).



Tu trouveras encore [ici](#) de plus amples conditions d'utilisation pour l'accès à Office 365 depuis des terminaux privés («BYOD»).



Les «Mobile Device Services» («MDS») autorisent les collaborateurs des CFF à synchroniser leur calendrier, leurs courriels, contacts, notes et tâches avec des terminaux mobiles validés par le service informatique des CFF et à accéder au réseau d'entreprise des CFF à l'aide des applis adéquates («ICT-Selfcare», «portail des collaborateurs», etc.).



Tu trouveras [ici](#) les conditions d'utilisation pour le service MDS.

### 3. Traitement de l'information

#### 3.1. Classification



Les données commerciales comprennent les données et informations en lien avec les CFF. Il s'agit notamment des données des CFF et des clients, des collaborateurs, fournisseurs et partenaires commerciaux.

Les données peuvent par exemple prendre la forme de documents Office, de courriels, de documents papier, de dossiers personnels et de factures.



**Tu classes obligatoirement les données commerciales confidentielles créées, éditées et enregistrées par tes soins comme «C3 - Confidentiel». Pour les données commerciales publiques et internes, une classification est recommandée, mais n'est pas obligatoire. Néanmoins, elle**

**contribue à éviter tout malentendu et contribue de manière importante au respect de la sécurité de l'information.**



La classification indique dans quelle mesure les données sont précieuses et qui peut les consulter.

Chez les CFF, il existe les niveaux de classification suivants en matière de confidentialité:

1. les données publiques sont celles destinées au grand public. Il s'agit notamment de l'horaire, des prospectus de vente ou des communiqués de presse. Aucune mention relative à la confidentialité ne s'impose;
2. les données internes sont celles destinées à un usage interne et à une sélection d'autres destinataires. Il s'agit notamment des instructions internes, de l'annuaire téléphonique ou de l'adresse de service. Ces informations doivent porter la mention «interne»;
3. les données confidentielles sont des données qui doivent faire l'objet d'une protection particulière. Il s'agit notamment des reportings financiers, des documents relatifs aux technologies critiques, des procès-verbaux de réunions du CA, de la direction du groupe et de la direction de la division, ainsi que des données personnelles imposant une protection particulière. Les documents doivent toujours porter la mention «confidentiel».



Liens utiles:

pour des explications détaillées sur la classification, il convient de consulter [l'instruction sur la classification](#).

### 3.2. Confidentialité et secret



**Tu traites les données commerciales des CFF avec la minutie qui s'impose.** Les données internes ne sont pas non plus destinées au grand public. Au sein des CFF, nous échangeons cependant ouvertement des données dont la classification est «interne» et utilisons des données non confidentielles pour la collaboration intersectorielle, dans l'intérêt des CFF.



L'utilisation minutieuse des données commerciales constitue un élément important du [code de conduite des CFF](#).



**Tu veilles à la protection des discussions, documents papier et supports de données mobiles à caractère commercial et confidentiel, ainsi que des contenus affichés sur ton écran, et tu les protèges contre tout accès non autorisé.**



Tu pourras obtenir un filtre de confidentialité pour ton ordinateur portable sur [l'ICT Service Portal](#). Connecte-toi au portail de commande et saisis le terme «Filtre de confidentialité» dans la recherche. Tu y trouveras une sélection de filtres de confidentialité pour différents modèles d'ordinateurs portables.

Pour les discussions confidentielles, utilise dans la mesure du possible une pièce que tu pourras fermer. Un wagon de train et un restaurant ne sont pas des endroits adaptés aux conversations téléphoniques confidentielles.

Ne laisse pas trainer tes documents papier et supports de données mobiles et prends-en tout particulièrement soin hors de ton lieu de travail.

### 3.3. Sauvegarde des données



**Tu sauvegardes les données commerciales sur les services mis à disposition par les CFF (SharePoint, OneDrive for Business, DMS, Filer, etc.).** Les services de Cloud privé (Dropbox privé ou iCloud) ne sont pas admis pour la sauvegarde des données commerciales. Les données de niveau «confidentiel» peuvent uniquement être enregistrées en local, sur des terminaux gérés par les CFF.



Tu trouveras de plus amples informations sur la sauvegarde de données dans SharePoint, OneDrive for Business et DMS sur la [page ICT Workplace](#).

### 3.4. Envoi de documents



**Pour les échanges de courriels à caractère professionnel, tu utilises les systèmes officiels des CFF (Exchange/Outlook). Tu ne transfères pas de courriels professionnels vers des adresses privées.**



**Par principe, tu envoies les informations confidentielles en format crypté. Elles ne doivent pas être transmises à des interlocuteurs externes sans l'accord de leur auteur.**



Tu trouveras des dispositions complémentaires sur l'utilisation des moyens de communication électroniques et des réseaux sociaux ici: [Principes régissant le comportement à adopter en matière de communication électronique](#) et [Guide médias sociaux](#)

### 3.5. Supports de données mobiles



Les supports de données mobiles ne peuvent être utilisés que pour des données publiques (p. ex. vidéo d'entreprise volumineuse, qui dépasse la capacité de stockage). Les données commerciales appartenant à la catégorie «interne» ou «confidentielle» doivent être sauvegardées dans le dossier d'entreprise dédié (p. ex. SharePoint ou le dossier OneDrive professionnel). La fonction de validation doit être utilisée pour l'échange de données.



SharePoint te permet à la fois de partager les données commerciales en interne aux CFF et avec des tiers. Ce [mode d'emploi](#) sur la page ICT Workplace t'explique comment procéder.

## 4. Incidents liés à la sécurité



Nous te demandons d'informer immédiatement l'ICT Service Desk de la perte ou du vol de terminaux contenant des données commerciales, des incidents pertinents en matière de sécurité de l'information et des violations éventuelles de la protection des données (téléphone **+41 51 220 30 40**).

## 5. Logiciels et applis



Par principe, tu utilises à des fins professionnelles des logiciels acquis et déployés sous licence par les CFF.

Si tu n'utilises pas les logiciels mis à disposition par les CFF à des fins professionnelles (sur les terminaux des CFF et les terminaux BYOD), il t'appartient de veiller à ce que les logiciels que tu utilises puissent servir à des fins professionnelles et qu'ils disposent d'une licence valide.



Des logiciels complémentaires peuvent être commandés sur l'[ICT Service Portal](#).

## 6. Utilisation à des fins privées, droits individuels et surveillance

### 6.1. Utilisation à des fins privées



Les outils informatiques et de communication mis à disposition par les CFF sont principalement destinés à un usage commercial. Les collaborateurs peuvent également les utiliser de façon appropriée et raisonnable dans un cadre privé.



**Tu n'accèdes à aucun site internet diffusant des contenus contraires au droit ou choquants (sexistes, racistes, extrémistes, pornographiques, non éthiques, diffamatoires).** Si tu accèdes à un tel site par erreur, tu le quittes immédiatement.



L'accès peut être restreint ou interdit par des instructions de travail dans le respect du principe de proportionnalité si la personne assume par exemple des fonctions de surveillance.

Ton supérieur hiérarchique direct peut restreindre ou interdire l'utilisation d'Internet dans le respect du principe de proportionnalité s'il existe une suspicion justifiée ou la certitude que l'usage à des fins privées dépasse les limites tolérées ou que l'utilisateur accède à des sites contraires au droit ou choquants.



**Les achats et souscriptions de services par abonnement mobile, notamment par facture mobile, SMS payant ou SMS Pay sont interdits à des fins privées.**



Tu trouveras des informations détaillées sur les paiements par smartphone (par un abonnement mobile des CFF) dans l'article: [Payer avec le smartphone CFF](#).

### 6.2. Droits individuels et surveillance



Une certaine surveillance des outils de travail informatiques des CFF est nécessaire pour garantir l'exploitation.

Les mesures de surveillance et d'évaluation correspondantes veillent à ce que toutes les dispositions légales et internes soient respectées, au même

titre que les accords avec les partenaires sociaux. Elles garantissent par ailleurs que les mesures limitent autant que possible l'atteinte aux droits individuels.

Pour leurs mesures de surveillance, les CFF respectent le principe de proportionnalité et utilisent uniquement des mesures de surveillance et d'évaluation limitant autant que possible l'atteinte aux droits individuels au regard des finalités visées.



Tu trouveras des informations complémentaires dans l'[instruction K 155.1](#).

IT-SR-L

sig. Marcus Griesser

CISO

IT-SR

sig. Daniel Wild

Security and Risk Manager