Version de la réglementation	**3-0**	Classement de confidentialité	**Interne**
Valable dès le	**1.8.2018**	Propriétaire	**IT-SR**
		Processus	**Gestion informatique**
		Langues	**DE, FR, IT**

Divisions concernées	**Infrastructure, Voyageurs, Cargo, Immobilier, groupe**
Utilisateurs spécifiques/Distribution	**LIDI-R A2**
Remplace	**Version de la réglementation 2-0**
Attribution	**K 030.1**

Instruction du groupe relative à l'ut-ilisation autorisée d'Internet, ainsi que des services et programmes de courrier électronique

Suivi des modifications **1**

1. Généralités **2**
1.1. Situation initiale, objectifs 2
1.2. Champ d'application 2
1.3. Documents de référence et documents annexés 2
1.4. Termes et abréviations 2

2. Mesures de sécurité administratives **2**

3. Utilisation d'Internet à des fins professionnelles ou privées **3**
3.1. Accès à Internet à des fins professionnelles 3
3.2. Accès à Internet à des fins privées 3
3.3. Contrôle de l'utilisation autorisée d'Internet 4
3.4. Impossibilité technique d'accéder à certains contenus Internet 4
3.5. Téléchargement de logiciels à partir d'Internet et installation en local 5
3.6. Forcement des liaisons https cryptés (SSL Interception) 5

4. Utilisation de services et de programmes de courrier électronique **5**

5. Sanctions **6**

6. Rapport avec la directive et les autres instructions **6**

Suivi des modifications

Version	Chapitre	Modification
3-0	3.6	Description thème SSL-Interception
2-0	Tous	Reprise de l'instruction dans le modèle actuel de la réglementation. Changement de K-IT en IT.

1. Généralités

1.1. Situation initiale, objectifs

La présente instruction réglemente l'utilisation autorisée d'Internet, des services et programmes de courrier électronique (notamment Outlook/Exchange, services e-mail gratuits, services de messagerie ou Outlook) par les personnes physiques pouvant utiliser Internet, les services et/ou les programmes de courrier électronique au moyen d'un accès à distance ou local au réseau de communication des CFF.

1.2. Champ d'application

La présente instruction a caractère obligatoire pour les collaborateurs des CFF et de CFF Cargo. Elle est également contraignante pour les collaborateurs d'autres personnes morales dans la mesure où ces dernières mettent à la disposition de leurs collaborateurs les possibilités techniques mentionnées dans le précédent paragraphe, ainsi que pour les collaborateurs externes des CFF, de CFF Cargo et toute autre personne morale disposant également des possibilités techniques susmentionnées.

Toutes les personnes physiques soumises aux dispositions de la présente instruction sont désignées par le terme «utilisateurs». Afin de faciliter la lecture, seule la forme masculine est utilisée dans le présent document pour désigner les personnes des deux sexes.

1.3. Documents de référence et documents annexés

K 030.1 «Manuel de la sûreté des CFF»

1.4. Termes et abréviations

2. Mesures de sécurité administratives

2.1 Le supérieur direct s'assure que l'utilisateur qui lui est subordonné est informé de l'existence, ainsi que des dispositions fondamentales de la présente instruction et de la directive correspondante portant sur l'utilisation autorisée d'Internet, des services et programmes de courrier électronique et sur l'utilisation du matériel et des logiciels informatiques (R Z 400.5, ci-après la «directive»). Il attire son attention sur le fait que la présente instruction et la directive correspondante peuvent être consultées et téléchargées à partir de la réglementation CFF disponible dans l'intranet des CFF.

2.2. Par le biais de mesures appropriées, les autres personnes morales au sens du ch. 1, al. 2 de la présente instruction (Securitrans, etc.) sont tenues d'appliquer les dispositions de la présente instruction à leurs propres collaborateurs.

3. Utilisation d'Internet à des fins professionnelles ou privées

3.1. Accès à Internet à des fins professionnelles

3.1.1 L'utilisation professionnelle d'Internet par les utilisateurs est autorisée sous réserve des dispositions du chiffre 3.1.2.

3.1.2 Il est toutefois interdit

aux utilisateurs d'ouvrir les sites Internet dont ils savent ou devraient du moins savoir qu'ils présentent des contenus illicites ou choquants (sites aux contenus notamment sexistes, racistes, extrémistes, pornographiques, contraires à l'éthique ou diffamatoires). Ces contenus ne doivent être ni sauvegardés (de quelque façon que ce soit) ni communiqués à des tiers. Si un site de ce type est ouvert par erreur, il doit être aussitôt refermé (sans que le contenu soit enregistré ou transmis).

3.1.3 La directive correspondant à la présente instruction peut réglementer l'utilisation d'Internet pour des transactions financières, ainsi que les commandes/octrois de commandes par cartes de crédit. Elle peut également contenir des dispositions relatives à la diffusion de certaines données sensibles via Internet.

3.2. Accès à Internet à des fins privées

3.2.1 L'utilisation privée d'Internet par les utilisateurs est autorisée dans la mesure où elle est limitée dans le temps. Sont toutefois réservées les dispositions du chiffre 3.1.2. de la présente instruction, qui s'appliquent également à l'utilisation d'Internet à des fins privées.

Si l'accès aux sites Internet autorisés entrave la disponibilité du réseau CFF, le CISO peut ordonner le blocage des liens Internet correspondants.

3.2.2 Néanmoins, si le supérieur direct de l'utilisateur soupçonne à juste titre ou est même certain que l'accès aux sites Internet autorisés dépasse les limites de tolérance ou que son subordonné consulte ou consultera des sites ne devant pas être ouverts (cf. chiffre 3.1.2), il est habilité à restreindre voire supprimer l'accès à Internet privé de l'utilisateur en question. Cette mesure doit être proportionnelle à la situation. Les sanctions prévues au chiffre 5 de la présente instruction demeurent réservées.

Dans le cadre d'instructions de travail internes aux services, l'accès à Internet peut être interdit si cela s'avère une mesure proportionnée.

Le principe de proportionnalité s'applique, par exemple, dans les cas où l'accès à Internet n'est pas nécessaire à des fins professionnelles et/ou si les personnes exercent des fonctions de surveillance.

3.3. Contrôle de l'utilisation autorisée d'Internet

3.3.1. L'unité d'organisation IT-Security et Risk Management des CFF (ci-après «IT-SR») procède ponctuellement à des contrôles anonymes des fichiers journaux Internet selon une fréquence déterminée et pour une durée d'utilisation limitée afin de vérifier le respect des dispositions prévues au chiffre 3.1.2 de la présente instruction du groupe.

Si un abus est constaté, il est possible de procéder à une évaluation des fichiers journaux de la personne concernée. Le résultat de cette évaluation personnelle est transmis par IT-Security et Risk Management au supérieur direct du fautif, ainsi qu'à la direction Human Resources de la division/de l'unité centrale pour laquelle cette personne travaille. Le supérieur direct prend les mesures de conduite qui s'imposent. Les responsables du personnel concernés se tiennent à la disposition des supérieurs pour les assister et les conseiller.

3.3.2 Dans le cadre de ses contrôles, IT-SR est tenue de respecter les dispositions actuelles du «Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail» élaboré par le Préposé fédéral à la protection des données.

Il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail. Lorsque des systèmes de surveillance ou de contrôle sont nécessaires pour d'autres raisons, ils doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs (art. 26 de l'ordonnance 3 relative à la loi sur le travail).

3.3.3. En cas de doute sur la légalité d'un tel contrôle, IT-Security et Risk Management doit au préalable consulter les services juridiques internes des CFF.

3.4. Impossibilité technique d'accéder à certains contenus Internet

Afin de limiter les dommages techniques (p. ex. intrusion de virus), IT-Security et Risk Management a le droit et le devoir d'utiliser des mesures techniques de protection autorisées par la loi. Ces mesures de protection sont régulièrement adaptées aux dernières avancées techniques. IT-Security et Risk Management peut à tout moment verrouiller l'accès à des sites Internet qui vont à l'encontre des dispositions du chiffre 3.1.2 ou pourraient nuire à la bonne réputation du groupe CFF.

3.5. Téléchargement de logiciels à partir d'Internet et installation en local

Le téléchargement de logiciels sur Internet et leur installation ultérieure en local ne sont pas permis, exception faite des cas autorisés à titre exceptionnel par le CISO des CFF pour des raisons professionnelles de force majeure.

D'autres dispositions d'exécution se rapportant à ce point de règlement, ainsi qu'au téléchargement de codes logiciels sont contenues dans la directive correspondant à la présente instruction.

3.6. Forcement des liaisons https cryptés (SSL Interception)

Afin d'identifier et d'arrêter les virus et les Malware en trafic de données cryptés (https), les liaisons cryptées sont forcées par une Forward Proxi et son consultés par une Software. Ensuite, le traffic de données est de nouveau crypté et renvoyé à son destinataire. L'accès au internet décrypté ne sera pas sauvegardé ou évalué. Sont également bloqués les sites Web indésirables, les applications et les contenues (violence, racisme, pornographie, services de diffusion)

La communication cryptée avec la fédération, les banques et autres fournisseurs, dans lequel une norme de sécurité accrue est supposée (Banques, hôpitaux et assurance maladie).

Ces règles s'appliquent également aux utilisateurs mobiles qui accèdent à Internet sur la route ou à la maison.

4. Utilisation de services et de programmes de courrier électronique

4.1. L'envoi de messages (avec ou sans pièce jointe) dont les contenus sont illicites ou choquants est interdit – indépendamment du service ou du programme de courrier électronique utilisé (p. ex. services de courrier électronique sur Internet ou Outlook) et de la nature du message (privé ou professionnel).

4.2. L'usage privé de services vocaux et de messagerie, qui ne sont pas mis à disposition par les CFF (p. ex. MSN Messenger, Skype), ainsi que les envois publicitaires électroniques de masse à des fins privées sont également interdits.

4.3. La réception d'e-mails provenant d'envois publicitaires électroniques de masse peut être communiquée au service de support informatique (166) afin d'en verrouiller la réception future.

4.4. Des dispositions complémentaires relatives à l'utilisation des services et des programmes de courrier électronique sont contenues dans la directive correspondant à la présente instruction.

5. Sanctions

5.1. En cas d'inobservation des dispositions de la présente instruction – notamment du chiffre 3.1.2 ou 4.1 – par des collaborateurs des CFF, de CFF Cargo ou d'autres personnes morales (cf. chiffre 1, al. 2), les sanctions découlent des relations juridiques définies par le contrat de travail conclu avec l'employeur. (Un manquement grave au chiffre 3.1.2 ou 4.1 peut engendrer un licenciement sans préavis.)

5.2. Les sanctions ne peuvent être prononcées que lorsque l'identité du collaborateur fautif est connue avec certitude. Ces sanctions doivent rester proportionnelles à l'infraction. En cas de comportement criminel, le service juridique compétent doit décider, d'entente avec le chef de l'unité d'organisation de la personne incriminée, si une plainte doit être déposée.

5.3. Si un collaborateur d'une autre personne morale (au sens du chiffre 1, al. 2, de la présente instruction) ou un collaborateur externe des CFF, de CFF Cargo ou d'une autre personne morale viole les dispositions de la présente instruction (et de la directive y relative), le commanditaire ou l'employeur applique à l'encontre de la personne en faute les sanctions qu'il juge proportionnelles et adaptées.

5.4. Si la personne fautive est économiquement congruente avec l'entreprise ayant signé un contrat (p. ex. de services informatiques) avec les CFF, CFF Cargo ou toute autre personne morale au sens du chiffre 1, al. de la présente instruction (p. ex. société individuelle ou SA unipersonnelle) ou si l'entreprise refuse d'appliquer à l'encontre de son employé fautif ou du collaborateur mandaté des sanctions proportionnelles au préjudice conformément au ch. 1, al. 2 de la présente instruction reconsidérera sa politique d'adjudication vis-à-vis de cette entreprise et en tirera les conséquences légales autorisées.

6. Rapport avec la directive et les autres instructions

Dans le cadre de la compétence qui lui est attribuée par la présente instruction (cf. chiffres 3.1.3, 3.5, etc. de la présente instruction), IT-Security et Risk Management est habilitée à promulguer des dispositions d'exécution relatives à l'utilisation autorisée d'Internet et des services et programmes de courrier électronique dans la «directive relative à l'utilisation autorisée d'Internet, des services et programmes de courrier électronique et sur la manipulation du matériel et des logiciels informatiques».

Les dispositions de cette directive ne peuvent toutefois aller à l'encontre des dispositions de la présente instruction. Les modifications de la directive souhaitées

par IT-Security et Risk Management et découlant d'une norme de délégation prévue dans la présente instruction requièrent un examen juridique préalable.

IT	IT-SR
Sig. Peter Kummer	Sig. Marcus Griesser
CIO	CISO