Version de la réglementation	**2-0**	Classement de confidentialité	**interne**
Valable dès le	**1.1.2013**	Propriétaire	**IT-SR**
Dernière révision		Processus	**Gestion informatique**
Prochaine révision		Langues	**DE, FR, IT**
Divisions concernées	**Infrastructure, Voyageurs, Cargo, Immobilier, groupe**		
Utilisateurs spécifiques/Distribution			
Remplace	Version de la réglementation du 1.5.2010		

Directive relative à l'utilisation autorisée d'Internet, des services et programmes de courrier électronique ainsi qu'à l'utilisation du matériel et des logiciels informatiques

1. Généralités

1.1 Situation initiale, objectifs

La présente directive décrit les situations qu'ICT Security et Risk Management est en droit de réglementer conformément à une règle de délégation expresse formulée dans les instructions du groupe relatives, d'une part, à l'utilisation autorisée d'Internet, ainsi que des services et programmes de courrier électronique (K 400.8) et, d'autre part, à la manipulation autorisée du matériel et des logiciels informatiques (K 400.9).

1.2 Champ d'application

Elle s'applique à toute personne physique utilisant le matériel et/ou les logiciels informatiques ou Internet, les services et programmes de courrier électronique mis à disposition par CFF SA, son partenaire d'externalisation officielle (fournisseur) ou CFF Cargo SA au moyen d'un accès local ou à distance.

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.

1.2 Documents de référence et documents annexés

K 400.8 «Instruction du groupe relative à l'utilisation autorisée d'Internet, ainsi que des services et programmes de courrier électronique»

K 400.9 «Instruction du groupe relative à la manipulation autorisée du matériel et des logiciels informatiques»

1.3 Termes et abréviations

La présente directive utilise la terminologie suivante:

Terme	Description
Compte	Compte utilisateur
Pièce jointe	Fichier joint au message électronique
Utilisateur	Utilisateur de matériel et/ou logiciels informatiques, d'Internet et/ou de services et/ou de programmes de courrier électronique
CISO	Chief Information Security Officer des CFF
NSM	Gestionnaire de la sécurité réseau (Network Security Manager)
Dossier	Emplacement de stockage de fichiers
Appareil nomade	Ordinateur de poche (p. ex. Psion, Communicator)
Matériel informatique	Tous les appareils et composants techniques d'une installation de traitement des données
Hachage	Somme de contrôle cryptographique d'un document permettant d'en garantir l'intégrité
Canular	Message électronique contenant des informations erronées (principalement des alertes de virus), fréquemment assorti de demande de transmission à des tiers
IT	Technologie de l'information; appareils électroniques de traitement, d'enregistrement et de sauvegarde des données
JavaScript/ActiveX	Applications Internet permettant d'afficher des éléments Internet spéciaux
Connexion/déconnexion	Message de connexion/déconnexion destiné au système informatique

Instruction relative à l'utilisation d'Internet	Instruction du groupe sur l'utilisation autorisée d'Internet, ainsi que des services et programmes de courrier électronique (R Z 400.8).
Instruction relative à la manipulation du matériel et des logiciels informatiques	Instruction du groupe relative à la manipulation autorisée du matériel et des logiciels informatiques (R Z 400.9)
Logiciel	Désignation commune des programmes pouvant être exécutés sur un ordinateur
CISO	Responsable de la sécurité des systèmes d'information (Chief Information Security Officer)

2. Dispositions relatives aux logiciels

2.1 Utilisation de logiciels privés sur les PC/ordinateurs portables (ch. 4.1 K 400.9)

L'utilisation de logiciels privés sur les PC/ordinateurs portables mis à disposition par les CFF, leur partenaire d'externalisation (cf. ch. 1, al. 1 Z 400.9) ou CFF Cargo est interdite, sauf si le supérieur hiérarchique l'autorise, après avoir obtenu l'accord du service de support informatique et du CISO des CFF.

2.2 Installation/désinstallation de logiciels (ch. 4.1 K 400.9)

Seuls les services de support informatique sont habilités à installer et désinstaller des logiciels.

L'installation de logiciels autres que ceux fournis par les CFF ou CFF Cargo est interdite.

2.3 Logiciels mis à disposition (ch. 4.1 K 400.9)

Les logiciels éventuellement fournis par les CFF ou CFF Cargo à des fins d'installation sur un PC ou un ordinateur portable privé ne peuvent être utilisés que pour le compte des CFF ou de CFF Cargo. À la fin du contrat de travail ou du mandat conclu avec les CFF ou CFF Cargo, les logiciels susmentionnés doivent être supprimés du PC ou de l'ordinateur portable privé et ne plus être utilisés.

2.4 Demande de nouveaux logiciels ou de logiciels supplémentaires (ch. 4.1 K 400.9)

Les demandes de nouveaux logiciels ou de logiciels supplémentaires doivent être adressées au service de support informatique après consultation du supérieur hiérarchique.

2.5 Modification des paramètres de configuration (ch. 4.1 K 400.9)

L'utilisateur n'est pas autorisé à modifier les paramètres de configuration des logiciels (p. ex. niveau de sécurité du navigateur ou paramètres de contrôle du programme antivirus). Si une configuration particulière est souhaitée, le supérieur hiérarchique doit en faire la demande auprès du responsable du logiciel concerné (s'il s'agit de paramètres de sécurité, la demande doit être adressée au CISO).

2.6 Copie et octroi des droits d'utilisation de logiciels (ch. 4.1 K 400.9)

La copie de logiciels n'est pas permise, sauf pour les cas autorisés par la loi (p. ex. à des fins de sécurité) et approuvés préalablement par le responsable du Centre de solutions compétent.

L'octroi à des personnes physiques ou morales de droits d'utilisation et de sous-licences de logiciels, pour lesquels les CFF ou CFF Cargo ne disposent pas des droits de propriété intellectuelle ni ne sont autorisés (notamment par contrat) à céder de tels droits, est interdit. En cas de doute, il convient de demander une évaluation préalable de la recevabilité légale auprès du service juridique compétent de CFF IT.

2.7 Principes relatifs à l'utilisation des mots de passe (ch. 4.1 K 400.9)

Les mots de passe permettent aux utilisateurs de faire authentifier leur identification par le système informatique et d'accéder aux composants et informations informatiques (données) qui leur sont destinés.

La saisie par les utilisateurs d'un identifiant et d'un mot de passe secret prévient l'obtention de leurs droits d'accès par des tiers via une identification inconnue et ainsi l'accès non autorisé à leurs composants informatiques.

Il est interdit de craquer ou d'essayer de craquer les mots de passe de tiers.

Tout mot de passe doit être tenu secret et ne peut être communiqué qu'à l'utilisateur autorisé. Dès qu'un mot de passe est porté à la connaissance d'une personne non autorisée, il doit être modifié.

Les mots de passe doivent être saisis à l'abri des regards. Pour ce faire, le système et les applications doivent permettre la saisie masquée du mot de passe.

Le mot de passe doit être composé au minimum de huit caractères, dont un de chacune des trois catégories suivantes:

Majuscule

Minuscule

Chiffre

Caractère spécial

Les mots de passe ne doivent pas être aisés à deviner ni avoir de lien avec l'entreprise, une application informatique ou l'utilisateur (nom, prénom, plaque d'immatriculation du véhicule ou numéro de téléphone, etc.). Il convient d'éviter d'utiliser des mots de passe triviaux (p. ex. AAAAAAAA, 12345678, répétition de l'identification de l'utilisateur). Les dérogations à cette règle motivées par des raisons techniques doivent être validées par IT-SR.

Les mots de passe prédéfinis doivent être immédiatement modifiés et les mots de passe initiaux utilisés lors de l'inscription à un système doivent être remplacés par des mots de passe individuels après la première utilisation.

Les mots de passe personnels doivent être régulièrement modifiés (une fois par mois en général).

Si deux systèmes du réseau des CFF communiquent via un utilisateur, le service de coordination peut attribuer au mot de passe les attributs «never expires» et «user cannot change password».

Les mots de passe ne doivent pas être enregistrés sur des touches de fonction programmables.

Les mots de passe des utilisateurs privilégiés doivent être conservés sous scellés en lieu sûr afin de garantir l'accès aux systèmes et aux applications en cas d'urgence ou d'absence des utilisateurs en question. Les mots de passe déposés doivent être systématiquement actualisés par les utilisateurs concernés. Les règles relatives à l'accès aux droits d'administrateur en cas d'urgence sont définies au point A.1.8.

2.8 Principes relatifs à la gestion des comptes d'administrateur

Ni les administrateurs ni les utilisateurs ne peuvent travailler avec des comptes d'administrateur. Les administrateurs doivent travailler avec les identifiants personnels assortis des droits d'administrateur correspondants afin de garantir la traçabilité de leurs activités.

Le recours aux comptes d'administrateur est limité aux cas d'urgence, lorsqu'aucun des administrateurs ne peut être mobilisé.

Les autres règlements relatifs à la gestion des comptes privilégiés figurent dans l'instruction K 400.11 «Comptes privilégiés».

3 Dispositions relatives au matériel informatique

3.1 Champ d'application

Les réglementations décrites ci-après concernent l'ordinateur personnel (PC) et les terminaux portables, tels que les ordinateurs portables, les téléphones portables et les appareils du même genre, dans la mesure où les prescriptions individuelles ne visent pas explicitement un type précis d'appareil.

3.2 Emplacement (chiffre 3 K 400.9)

Le changement d'emplacement de l'ordinateur personnel (PC) requiert l'autorisation préalable du service de support informatique.

Les terminaux portables allumés ne doivent pas être laissés sans surveillance.

3.3 Connexions au réseau (chiffre 3 K 400.9)

Seul le service de support informatique est autorisé à modifier la configuration du réseau.

3.4 Modem (chiffre 3 K 400.9)

Les utilisateurs ne sont pas autorisés à installer des modems, sauf dans les cas où le supérieur hiérarchique direct en fait la demande auprès du CISO et que ladite demande est approuvée par le CISO et le DIO compétent. Si la demande est validée, le modem doit être installé par I-TC.

3.5 Accès à distance via IPSec VPN depuis les PC/ordinateurs portables privés (ch. 4.4 K 400.9)

L'IPSec VPN est utilisé pour les opérations de maintenance au niveau du système et de sa configuration, pour les développeurs (source code repositories, environnements de test/d'intégration) et pour les analyses en cas d'incident. La règle applicable est la suivante.

La création d'une connexion IPSEC VPN à l'aide d'un service d'accès à distance (RAS) depuis des PC ou des ordinateurs portables privés (c'est-à-dire non fournis par les CFF) n'est pas permise, sauf pour les appareils approuvés par le NSM et le CISO des CFF, qui sont assortis de logiciels spéciaux nécessaires à la réalisation des opérations de maintenance (p. ex. des composants du réseau ou des systèmes de serveurs informatiques).

L'accès de tiers via IT WORKPLACE RAS/IT WORKPLACE RAS depuis des PC ou des ordinateurs portables privés non fournis par les CFF est autorisé.

3.6 Sécurité et stockage des données (chiffres 3.4 et 4.1 K 400.9)

Les données saisies depuis un PC doivent être enregistrées dans le domaine de serveur attribué. Les données saisies depuis un ordinateur portable peuvent être enregistrées sur le disque dur de l'appareil.

Tout utilisateur qui saisit des données nécessaires à d'autres utilisateurs est tenu de les transférer, dans la mesure du possible, vers le serveur. (Ainsi ces données sont automatiquement enregistrées dans le cadre de la sauvegarde du serveur.)

Si l'utilisateur ne transfère pas quotidiennement les données de son appareil informatique vers le serveur, il doit réaliser une sauvegarde périodique de ses données sur des supports de mémoire portables dûment étiquetés et conservés en lieu sûr. L'utilisateur est informé de la marche à suivre par le service de support informatique.

Dans la mesure du possible, il convient de procéder à une analyse antivirus des données provenant de supports externes (p. ex. clés USB, disques durs externes). Le

Help Desk (n° de tél. 166) et le service de support informatique soutiennent et conseillent les utilisateurs en la matière.

L'utilisateur doit s'informer au préalable du niveau de classification des données et gérer l'appareil en conséquence.

Les données classées «confidentielles» doivent être cryptées avant leur enregistrement, dès que l'infrastructure correspondante est disponible. Les données non cryptées ne doivent pas être enregistrées sur des appareils portables.

Les tiers non autorisés n'ont pas le droit de consulter les données personnelles ou classées «confidentielles».

Le stockage des données auprès d'entreprises tierces n'est permis que sous réserve du respect du processus RfA (Request for Architecture) et de l'approbation du comité RfA en raison des répercussions possibles sur la sécurité.

3.7 Protection antivirus (ch. 3.4 et 4.1 K 400.9)

Seuls les PC et ordinateurs portables dotés d'un système de mise à jour automatique de la protection antivirale peuvent être utilisés dans les locaux des CFF ou de CFF Cargo. Si l'utilisateur constate l'absence d'un tel système sur son PC ou sur son ordinateur portable, il doit en informer l'assistance utilisateur dont il dépend.

L'utilisateur doit s'assurer de disposer des versions en vigueur du système d'exploitation et du correctif de sécurité des CFF.

Le Help Desk et l'assistance utilisateur doivent être immédiatement informés de la présence réelle ou supposée de virus. L'ordinateur doit être déconnecté du réseau. Le Help Desk et l'assistance utilisateur déterminent la marche à suivre.

L'utilisateur ne doit pas interrompre l'exécution du programme de recherche de virus.

L'antivirus installé ne doit pas être désactivé et l'appareil doit être régulièrement connecté au réseau afin de garantir la mise à jour des tableaux de protection antivirus.

L'utilisateur d'un appareil informatique portable peut connecter celui-ci au réseau local ou installer un logiciel récent de protection antivirus afin d'accroître son niveau de protection.

3.8 Protection antivirus des connexions d'accès à distance (ch. 3.4 et 4.1 K 400.9)

Toute personne qui utilise le réseau de communication des données des CFF via une connexion d'accès à distance (hors IT WORKPLACE–RAS) doit disposer d'un programme actualisé de protection antivirus afin de s'assurer avant chaque connexion au réseau de communication en question que le PC/l'ordinateur portable qu'elle utilise ne contient aucun virus, ver ou autre élément indésirable.

Si l'utilisateur du réseau de communication des données des CFF présume avoir transmis un virus/ver ou autre élément indésirable audit réseau de communication des CFF depuis son PC/ordinateur portable, il doit l'annoncer immédiatement à l'unité d'organisation IT-SR des CFF.

IT-SR conseille les utilisateurs actuels et futurs du réseau de communication des données des CFF au sujet de l'utilisation d'un programme de protection antivirus efficace.

3.9 Communication via des réseaux publics sans fil (Public GSM, Public WLAN) – ch. 3 et 4.1 K 400.9

Dans la mesure où un système de cryptage est disponible, seules les données cryptées peuvent être transférées. Le système de cryptage installé ne doit être en aucun cas désactivé.

3.10 Connexion à des réseaux non contrôlés par les CFF (p. ex. Internet, WLAN privé) – ch. 3 et 4 K 400.9

Les réseaux non contrôlés par les CFF sont les réseaux d'organisations tierces, telles que les fournisseurs, les clients et organisations du même genre.

Il est interdit de connecter des appareils des CFF à des réseaux de ce type afin d'éviter le transfert involontaire de données depuis les appareils des CFF vers un environnement réseau tiers, ainsi que l'échange de logiciels malveillants entre le réseau tiers et les appareils des CFF.

La connexion à Internet d'un appareil IT WORKPLACE en vue d'une utilisation pour IT WORKPLACE-RAS est expressément permise.

Les autorisations exceptionnelles du CISO des CFF restent réservées.

3.11 Perte et vol (ch. 3 et 4.1 K 400.9)

La perte/le vol de terminaux des CFF doivent être immédiatement annoncés aux services compétents. La perte d'appareils de téléphonie mobile doit être signalée au centre de support correspondant. La perte des autres appareils doit être annoncée à la coordination du service informatique, conformément au processus défini.

3.12 Annonce des événements et risques concernant la sécurité (ch. 3 et 4.1 K 400.9)

Les utilisateurs de terminaux CFF sont tenus d'annoncer immédiatement au responsable d'objet compétent les événements importants en matière de sécurité et/ou les risques identifiés (pour les projets: chef de projet/pour les appareils acquis via IT WORKPLACE: Fachbus IT WORKPLACE – IT-OM-WUS-WDM).

4 Utilisation autorisée d'Internet

4.1 Utilisations à risque (ch. 3.1.3 K 400.8)

Les commandes et octrois de commandes avec saisie du numéro de carte de crédit, ainsi que les transactions financières (p. ex. commerce de valeurs en ligne, télébanque) réalisées sur Internet sont, dans la mesure du possible, à éviter et sont déconseillées par les CFF ainsi que CFF Cargo. L'utilisateur reconnaît effectuer ce type d'opérations à ses risques et périls et admet que ni les CFF (y c. leurs filiales, les associations et fondations auxquelles ils sont liés, etc.) ni CFF Cargo (y c. leurs filiales, les associations et fondations auxquelles ils sont liés, etc.) ne sauraient être tenus responsables des éventuels dommages subséquents.

4.2 Diffusion de données sensibles (ch. 3.1.3 K 400.8)

Les identifiants utilisateur et les mots de passe internes à l'entreprise ne doivent pas être publiés sur Internet ni être utilisés pour se connecter à des services Internet externes (p. ex. comptes privés de messagerie électronique ou connexion de membre).

Les CFF et CFF Cargo ne peuvent pas garantir que les mots de passe, les noms d'utilisateur ou les informations secrètes/confidentielles transmis via Internet sans avoir été préalablement cryptés à l'aide de programmes de technologie récente ou de manière adéquate ne puissent pas être lus par des tiers non autorisés.

Dans la mesure du possible, il convient de ne pas divulguer sur Internet l'adresse de son lieu de travail, son adresse électronique professionnelle, ainsi que le nom de son employeur.

5 Utilisation autorisée de services et de programmes de courrier électronique

5.1 Information et soutien (ch. 4.4 K 400.8)

Pour tout problème relatif à l'utilisation des services de courrier électronique, les utilisateurs peuvent s'adresser au Help Desk ou au service de support informatique compétent. Les questions concernant la sécurité des informations transférées doivent être adressées au service de support informatique, division «Poste de travail et courrier électronique» (IT-OM-WUS-WDM) des CFF ou directement au CISO en cas de problèmes de sécurité majeurs.

5.2 Utilisation des systèmes de courrier électronique (clients) – ch. 4.4 K 400.8

L'échange de messages électroniques professionnels doit s'effectuer uniquement au moyen des systèmes et programmes de courrier électronique prévus à cet effet et autorisés (p. ex. Exchange/Outlook). Toute dérogation à cette règle doit faire l'objet d'une demande auprès du CISO, avec l'accord du supérieur hiérarchique.

CFF SA est autorisée à empêcher par des moyens techniques l'utilisation de systèmes de courrier électronique généralement accessibles (p. ex. Hotmail, GMX, Yahoo) depuis les PC, les ordinateurs portables ou les PDA fournis par CFF SA ou ses filiales à des fins professionnelles; elle a également le droit d'interdire partiellement ou totalement l'utilisation desdits systèmes dans le contexte commercial.

5.3 Indication de l'adresse e-mail en cas de risque de courrier indésirable (ch. 4.4 K 400.8)

L'indication de l'adresse e-mail professionnelle dans le cadre p. ex. de forums ou de listes de diffusion, susceptibles de déclencher un envoi massif de courrier à caractère purement publicitaire, est interdite.

5.4 E-mails privés (ch. 4.4 K 400.8)

Dans la mesure du possible, il convient de distinguer les e-mails aux contenus privés de ceux aux contenus professionnels. À cet effet, les messages aux contenus privés doivent être assortis de la mention «privé», si possible dans l'objet, le texte ou l'attribut du courrier, ou doivent être signalés comme tels. Tous les utilisateurs doivent s'assurer que les e-mails privés entrants sont également, dans la mesure du possible, marqués de manière adéquate. Il convient d'éviter d'enregistrer/d'archiver localement les e-mails privés.

5.5 Pièces jointes (ch. 4.4 K 400.8)

Pour des raisons de sécurité et de ressources, la taille maximum des documents/fichiers joints envoyés et réceptionnés est respectivement limitée à 5 et 10 mégaoctets.

L'envoi par e-mail de fichiers contenant des plaisanteries, des animations ou de la musique, ainsi que l'envoi de gratuiciels et/ou partagiciels et de jeux est interdit.

5.6 Envoi d'e-mails (ch. 4.4 K 400.8)

L'envoi par e-mail de programmes exécutables n'est pas permis, sauf s'il s'agit d'envois nécessaires à des fins professionnelles et validés par le CISO.

Les e-mails envoyés à des adresses électroniques internes ne peuvent être transférés vers des adresses électroniques externes qu'après vérification de leur contenu. De manière générale, il est interdit de transférer des e-mails aux contenus confidentiels vers des adresses électroniques externes.

Le transfert automatique des e-mails vers des adresses électroniques externes est interdit.

5.7 Confidentialité/cryptage (ch. 4.4 K 400.8)

Aucune information classifiée (notamment confidentielle) ne doit être envoyée (sous forme d'e-mail et/ou de pièce jointe) sans protection à des adresses électroniques externes (hors du réseau des CFF).

Seules les procédures validées par le CISO des CFF peuvent être utilisées pour le cryptage. Pour toute question sur les techniques de cryptage, l'utilisateur peut s'adresser aux services de support informatique.

5.8 Signature numérique (ch. 4.4 K 400.8)

Il est possible d'avoir recours aux signatures numériques afin de garantir l'authenticité des informations transmises, conformément à la loi en vigueur.

5.9 Réception d'e-mails (ch. 4.4 K 400.8)

L'utilisateur doit vérifier au moins une fois par jour la réception d'e-mails dans sa boîte de réception (appelée également «boîte aux lettres»). Par ailleurs, la réglementation concernant les suppléants s'applique, conformément à B.2.16. Les e-mails qui ne sont plus nécessaires doivent être supprimés. Les utilisateurs qui reçoivent des e-mails envoyés par des salariés des CFF ou de CFF Cargo dont les contenus sont illicites ou choquants doivent le signaler à leur supérieur hiérarchique et lui fournir une version imprimée des e-mails en question.

5.10 E-mail et conclusion de contrats (ch. 4.4 K 400.8)

La conclusion de contrats par courrier électronique doit s'effectuer, dans la mesure des possibilités et conformément à la loi en vigueur, à l'aide d'une signature numérique.

5.11 Pièces jointes (ch. 4.4 Z 400.8 et ch. 5.1 K 400.8)

Il est interdit d'ouvrir des pièces jointes envoyées par des expéditeurs non identifiables ou des sources douteuses (risque de virus). Le service de support informatique doit être informé le plus rapidement possible de la pièce jointe suspecte.

5.12 Programmes reçus par courrier électronique (ch. 4.4 K 400.8)

Les utilisateurs peuvent réceptionner des programmes envoyés en pièce jointe par un expéditeur connu, mais ne sont pas autorisés à les exécuter ni à les installer sur le matériel informatique fourni par les CFF, CFF Cargo ou leurs partenaires d'externalisation, sauf autorisation exceptionnelle accordée par le CISO et le DIO compétent.

5.13 Canulars reçus par courrier électronique (ch. 4.4 K 400.8)

Les utilisateurs sont tenus d'ignorer les e-mails contenant des avertissements erronés (portant principalement sur des virus) et des demandes de transmission à des tiers. Le service de support informatique doit être informé de la réception de canulars.

5.14 Réglementation concernant les suppléants (ch. 4.4 K 400.8)

Le supérieur hiérarchique désigne les personnes habilitées à lire et à supprimer le courrier entrant des utilisateurs absents sur une longue durée.

L'utilisateur doit autoriser le suppléant à accéder à sa boite aux lettres et à son courrier électronique pour la durée de son absence.

5.15 Enregistrement/archivage (ch. 4.4 K 400.8)

Pour des raisons de sécurité, les e-mails et leurs pièces jointes ne doivent pas être enregistrés ni archivés localement à l'aide du programme de courrier électronique (p. ex. Outlook).

5.16 Contrôle (ch. 4.4 K 400.8)

IT-SR peut procéder ponctuellement à des contrôles anonymes du courrier électronique selon une fréquence déterminée et pour une durée d'utilisation limitée afin de vérifier le respect des dispositions prévues au chiffre 4.1 de l'instruction «Utilisation d'Internet».

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 et à la transparence (PFPDT).

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-SR au supérieur hiérarchique de l'auteur de l'infraction. Le supérieur 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.

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).

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

6. Entrée en vigueur

La présente instruction entre en vigueur le 1er janvier 2013.

IT IT-SR

Sig. Peter Kummer
CIO

Sig. Marcus Griesser
CISO

Suivi des modifications

Version	Valable dès le	Chapitre	Modification
2-0	1.1.2013	Tous	Instruction reprise dans le modèle actuel de la réglementation; adaptations formelles. Changement de K-IT en IT.