Version de la réglementation	**3-0**	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 1.1.2012		

Instruction du groupe relative à la manipulation autorisée du matériel et des logiciels informatiques

1. Généralités

1.1. Situation initiale, objectifs

La présente directive réglemente l'utilisation autorisée du matériel et/ou des logiciels informatiques.

1.2. Champ d'application

Elle s'applique à toute personne physique utilisant le matériel et/ou les logiciels informatiques mis à disposition par les CFF, son partenaire d'externalisation officielle (fournisseur) ou CFF Cargo.

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 30.1 «Manuel de la sûreté des CFF»

2. Mesures de sécurité administratives

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 du groupe et de la directive portant sur l'utilisation autorisée d'Internet, des services et programmes de courrier électronique et sur l'utilisation du matériel et des logiciels informatiques (K 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.

3. Dispositions relatives au matériel

3.1. Principes relatifs à l'utilisation du matériel

3.1.1. Usage autorisé du matériel

Ne peut être utilisé au sein des CFF et de CFF Cargo que du matériel ayant été acquis par les CFF (ou son partenaire d'externalisation) ou CFF Cargo et mis à disposition de l'utilisateur pour l'accomplissement de ses tâches.

Les CFF et CFF Cargo sont habilités à rechercher et à retirer de la circulation le matériel non autorisé au sein des CFF ou de CFF Cargo à l'aide de mesures techniques ou organisationnelles.

Le matériel doit être manipulé avec soin.

3.1.2. Prêt gratuit et à long terme de matériel

Tout prêt de matériel, gratuit et d'une durée supérieure à deux mois, mis à disposition par les CFF ou CFF Cargo par le partenaire d'externalisation des CFF

et devant être utilisé hors des locaux des CFF ou de CFF Cargo, nécessite au préalable l'accord du chef de division compétent. En cas d'accord, un contrat de prêt à usage doit être conclu par écrit avec le tiers concerné, et l'Account Management de CFF IT doit être immédiatement informé du matériel prêté. (Quel matériel a été prêté? À qui? Jusqu'à quand?)

3.1.3. Utilisation des PC, ordinateurs portables ou périphériques informatiques mis à disposition à des fins privées

L'utilisation des PC, ordinateurs portables ou périphériques informatiques (scanners, graveurs de CD, etc.) mis à disposition à usage privé n'est pas autorisée pendant les heures de travail, sauf si le supérieur direct l'a permis pour une brève période de temps.

L'utilisation des PC, ordinateurs portables ou périphériques informatiques mis à disposition à usage privé hors des heures de travail est possible pour un laps de temps limité, dans la mesure où le supérieur direct l'a autorisée.

3.1.4. Utilisation des PC ou ordinateurs portables privés à des fins professionnelles

Les PC/ordinateurs portables privés ne peuvent être raccordés au réseau de communication des données des CFF qu'avec l'accord préalable écrit de l'Operation Management et d'ICT-Security et Risk Management (ci-après «IT-SR») suivant une homologation conformément à K 400.30, sauf dans les cas où une connexion d'accès à distance a été autorisée et où l'accès au réseau ne se fait pas à partir des locaux des CFF ou de CFF Cargo.

3.1.5. Verrouillage du poste de travail

Le PC et l'ordinateur portable doivent automatiquement être verrouillés au plus tard au moment de quitter le poste de travail (p. ex. par un économiseur d'écran protégé par un mot de passe) afin d'empêcher tout accès de personnes non habilitées.

En cas de non utilisation du PC/de l'ordinateur portable pendant une longue période ou à la fin du travail, l'utilisateur doit se déconnecter (log out) et éteindre le PC/l'ordinateur portable.

3.2. Supports de données

Les supports de données (disquettes, CD-ROM, disques durs, bandes magnétiques, impressions) ne doivent pas traîner pour éviter que des personnes non habilitées puissent éventuellement les copier, les consulter ou les voler.

3.3. Dispositions relatives aux appareils informatiques portables sur lesquels des données CFF sont traitées

3.3.1. Dispositions relatives aux appareils informatiques portables mis temporairement à disposition

3.3.1.1. Remise ou reprise des appareils informatiques portables mis à disposition

Les unités d'organisation des CFF et de CFF Cargo prêtant des appareils informatiques portables doivent s'assurer qu'un contrôle approprié des appareils prêtés est effectué.

L'utilisateur de l'appareil informatique portable mis à disposition doit effacer les données qu'il a sauvegardées sur le disque dur avant de rendre ce dernier. En cas de présence de données à usage personnel après la remise de l'appareil, ces dernières doivent être effacées par le Help Desk (Service Desk) ou l'assistance utilisateur.

3.3.1.2. Protection contre le vol d'appareils informatiques portables

L'utilisateur d'un appareil informatique portable doit tout mettre en œuvre pour protéger l'appareil mis à sa disposition contre les éventuels vols.

3.3.1.3. Transport

Les appareils informatiques portables ne doivent être transportés que bien emballés.

3.3.1.4. Perte

En cas de perte ou de vol d'un appareil informatique portable mis à disposition et propriété des CFF, du partenaire d'externalisation ou de CFF Cargo, l'unité d'organisation IT-SR doit être informée immédiatement en raison des pertes de données potentielles pour les CFF et pour que les mesures de protection nécessaires (p. ex. blocage du compte) puissent être prises.

3.4. Sécurité des données, corbeille électronique, dossier de fichiers temporaire, sauvegarde automatique

IT-SR est habilitée à établir des règlements concernant la sécurité et le stockage des données, les dossiers temporaires, la sauvegarde automatique et les mesures de protection antivirus dans la directive se rapportant à la présente instruction.

3.5. Modifications

Les modifications du matériel mis à disposition (y compris des périphériques informatiques) ne doivent être réalisées que par le service de support informatique, sauf autorisations exceptionnelles de l'unité d'organisation IT-SR, celle-ci devant toutefois informer le CISO des autorisations spéciales accordées.

4. Dispositions relatives aux logiciels et aux données

4.1. Utilisation

Ne peuvent être utilisés sur les PC/ordinateurs portables des CFF ou de CFF Cargo que les logiciels autorisés par les CFF ou CFF Cargo. La liste des logiciels autorisés peut être obtenue auprès du service de gestion des licences de CFF IT ou dans le panier d'achat correspondant (p. ex. panier d'achat IT WORKPLACE). Des dispositions complémentaires relatives aux logiciels peuvent figurer dans la directive se rapportant à la présente instruction.

4.2. Tests des mécanismes de protection des interfaces de navigateurs d'applications

Les applications accessibles au moyen d'un navigateur Web doivent être protégées de manière préventive contre les attaques éventuelles. La résistance de l'interface de navigateur de ces applications doit être testée avant la mise en service.

Sont concernées toutes les applications qui peuvent fonctionner avec un navigateur Web et qui se trouvent sur le réseau des CFF.

Cela concerne notamment les applications externalisées sur les systèmes de fournisseurs tiers. Ces applications doivent être protégées conformément aux meilleures pratiques en matière de développement d'attaques.

Les mécanismes de protection de ces applications contre les attaques doivent être testés avant la mise en service.

Les applications productives doivent être testées au moins tous les deux ans en cas de développement de nouvelles versions apportant des modifications en lien avec leur accès au moyen d'un navigateur Web.

4.2.1 Développements propres de CFF Informatique

La TestFactory des CFF est chargée de préparer, d'exécuter et d'évaluer ces tests des mécanismes de protection des interfaces de navigateurs.

La mise en service de l'application ou d'une nouvelle version n'est autorisée que sur présentation d'une attestation de la sûreté opérationnelle des CFF.

4.2.2 Applications développées et exploitées par des fournisseurs tiers

Les fournisseurs tiers qui développent et exploitent ces applications pour les CFF doivent être tenus d'apporter la preuve qu'ils ont analysé et évalué les mécanismes de protection contre les attaques via l'interface de navigateur Web. Ils peuvent également faire analyser les applications par la Testfactory des CFF.

La coordination des preuves incombe à la Testfactory des CFF.

4.2.3 Rapports

La Testfactory des CFF met périodiquement à la disposition d'IT-Security un reporting relatif aux tests des applications.

4.2.4 Réglementation transitoire

Les mécanismes de protection des applications déjà opérationnelles au 1er janvier 2012 doivent être testés ultérieurement.

Ces tests sont planifiés par la Testfactory avec les responsables d'applications concernés conformément à l'ordre de priorité suivant:

1. Les applications accessibles de l'extérieur par Internet ou via un réseau d'entreprise au moyen d'un navigateur Web doivent être testées d'ici au 31 décembre 2012.
2. Les applications intranet traitant des données confidentielles et
3. toutes les autres applications intranet traitant des données internes doivent être testées d'ici au 31 décembre 2013.

4.3. Départ d'un collaborateur

Tout collaborateur quittant les CFF ou CFF Cargo doit, quatre semaines avant son départ et de concert avec son supérieur, déterminer un lieu d'archivage pour la reprise des données et/ou des messages stockés localement et à réutiliser. Les données purement privées ou n'étant plus nécessaires doivent être effacées.

4.4. Effacement des données des collaborateurs licenciés sans préavis, décédés, disparus ou congédiés

Les services du personnel (Human Resources) des CFF et de CFF Cargo informent les proches des collaborateurs décédés/disparus, ainsi que des collaborateurs licenciés sans préavis ou congédiés du fait qu'ils peuvent déposer auprès des CFF ou de CFF de Cargo une requête de remise des données purement privées dans un délai d'un mois après la non-présence au travail du collaborateur concerné. Ils informent à temps le service de support informatique des noms et prénoms des collaborateurs licenciés sans préavis, décédés, disparus ou congédiés, ainsi que du début de la période de préavis d'un mois.

4.5. Traitement de données classifiées et de données du personnel

En cas de traitement sur un appareil informatique de données secrètes, confidentielles ou de données du personnel, ces dernières doivent être protégées par des mesures techniques particulières contre un éventuel accès de personnes non habilitées. Le service de support informatique conseille et assiste sur ce point les utilisateurs concernés.

4.6. Protocolage

Dans le cadre de ce qui est permis par la loi et exclusivement pour des raisons de sécurité technique informatique (c'est-à-dire pas dans le but de surveiller les collaborateurs), l'unité d'organisation IT-SR peut procéder ponctuellement à des contrôles anonymes de l'accès aux programmes et données selon un calendrier déterminé et pour une durée d'utilisation limitée. Ces données sont exclusivement sauvegardées sous forme anonyme et sont immédiatement effacées après leur utilisation.

4.7. Contrôle

IT-SR est habilitée à rechercher systématiquement sur les ordinateurs tout contenu passant dans le système informatique et les réseaux des CFF et pouvant représenter un danger comme les virus, les vers, les surcharges du système, etc. Ces procédures sont entièrement réalisées de façon automatique, conformément aux possibilités techniques actuelles. Ces données sont exclusivement sauvegardées sous forme anonyme et sont immédiatement effacées après leur utilisation.

4.8. Modifications

Les modifications des logiciels mis à disposition ne peuvent être réalisées que par le service de support informatique, sauf autorisations exceptionnelles du CISO ou du CIO compétent, ce dernier devant informer le CISO des autorisations exceptionnelles octroyées.

5. Rapport avec d'autres instructions

Dans le cadre de la compétence qui lui est attribuée par la présente instruction (cf. chiffre 4.1 ci-dessus), IT-SR est habilitée à promulguer des dispositions d'exécution relatives à la manipulation autorisée du matériel et des logiciels informatiques dans la «directive sur 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-SR et découlant d'une norme de délégation prévue dans la présente instruction requièrent un examen juridique préalable.

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
3-0	1.1.2013	Tous	Instruction reprise dans le modèle actuel de la réglementation et actualisation formelle des désignations de fonctions. Changement de K-IT en IT.