GUIDE

# CHARTE DE L'UTILISATEUR POUR L'USAGE DU SYSTÈME D'INFORMATION DE LA SNCF

**Direction de la Sûreté**
34 rue du Commandant Mouchotte
75699 PARIS CEDEX 14
(CRT PARIS SIEGE)

Les Éditions du Petit Matin - 01 44 61 00 98 - septembre 2006

# Préface

*Le système d'information de la SNCF fait partie de son patrimoine et son importance grandissante en fait une « colonne vertébrale » de notre fonctionnement. La protection de cet outil indispensable est plus que jamais essentielle et s'avère en cela un objectif majeur.*

*L'intégrité et le bon fonctionnement de notre système d'information nous sont indispensables pour développer notre capital d'innovation et pour que la SNCF devienne l'entreprise publique de service public leader du transport en Europe.*

*Comme la qualité, la sécurité ne peut être obtenue dans la durée que par une action à la fois collective et individuelle. Si la mise en œuvre des organisations et des techniques permettant d'assurer la sécurité du système d'information est l'affaire de quelques experts, leur application au quotidien est l'affaire de tous, dans l'intérêt de chacun. Protéger le système d'information de la SNCF, c'est aussi se protéger de certaines dérives comportementales qui pourraient résulter, entre autres, de la méconnaissance de la législation, de l'ignorance des risques encourus ou d'une mauvaise application des règles parfois simples et de bon sens, mais toujours essentielles.*

*Chacun doit être conscient des exigences qui s'imposent à lui pour prévenir les risques et, pour cela, disposer de l'information et de la formation indispensables pour être un acteur de la sécurité conscient de ses droits et de ses devoirs comme des responsabilités qui sont les siennes envers lui-même et envers l'entreprise.*

*Cette charte est là pour nous conseiller lorsque nous avons une incertitude sur notre comportement. Chacun d'entre nous doit percevoir la nécessité des principes qu'elle rappelle et qui s'imposent à tous.*

*La Présidente*



*Anne-Marie IDRAC*

# Qu'est-ce que c'est ?
# Pourquoi ?
# Pour qui ?

## Qu'est-ce que c'est ?

Cette charte est avant tout un **code de bonne conduite**. Elle décrit des pratiques comportementales **essentielles** devant être connues et appliquées par l'ensemble du personnel afin d'assurer les conditions d'un usage correct et sécurisé du système d'information de l'Entreprise. A cette fin, elle a pour objet de préciser les droits, les devoirs et les responsabilités de chacun, en accord avec la législation en vigueur, le code de déontologie de la SNCF et le règlement du personnel RH-0006.

Les principes énoncés ne sont pas exclusifs des règles normales de courtoisie et de respect d'autrui.

## Pourquoi ?

L'Entreprise fonctionne en réseau, son système d'information également. Tous les composants du réseau sont **dépendants les uns des autres**. La défaillance de l'un d'entre eux a des conséquences qui peuvent dépasser largement le composant lui-même. Dans tous ces réseaux, le maillon le plus fragile et le moins contrôlable reste l'humain.


## Pour qui ?

La présente charte s'applique à l'ensemble des collaborateurs de la SNCF, permanents ou temporaires, tous statuts confondus, ayant accès aux ressources du système d'information de l'Entreprise. Elle sera notamment jointe, à titre d'information, au contrat de travail.

***La charte s'adresse à l'ensemble des agents (contractuels ou au cadre permanent) de l'entreprise mais également aux personnels sous contrats avec la SNCF (prestataires, stagiaires, intérimaires).***

# Définitions

**Système d'information :** ensemble des moyens humains, techniques et organisationnels permettant, en support à l'activité, de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et externes de l'entreprise, quelle que soit la forme sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image …).

**Utilisateur du système d'information :** toute personne autorisée à accéder, utiliser ou traiter des ressources du système d'information de la SNCF dans le cadre de son activité professionnelle.

**Ressource du système d'information :** le terme « ressource » désigne l'information et ses différents moyens de partage, de traitement, d'échange et de stockage.

**Patrimoine d'information de la SNCF :** il constitue l'un de ses actifs les plus importants, sur lequel reposent sa performance, sa pérennité, sa sécurité et sa capacité à maintenir et développer ses activités et ses résultats ; il recouvre :

- les systèmes d'information de commercialisation, de production et de gestion, nécessaires au plein exercice de ses métiers ;
- le patrimoine intellectuel, composé de toutes les informations concourant à son savoir et son savoir-faire, par exemple, ses recherches, ses brevets en cours, ses retours d'expérience ;
- les informations relatives à ses clients ou aux tiers avec lesquels elle est en relation, dont l'altération ou la divulgation pourrait porter atteinte à son image de marque, celle de ses clients ou des tiers concernés, voire entraîner des poursuites judiciaires ;
- les informations relatives à son personnel, telles que les dossiers administratifs ou médicaux, dont la divulgation constituerait une violation de la vie privée.

# Accès aux ressources

L'utilisation des ressources du système d'information de la SNCF n'est possible que dans le **cadre de l'activité professionnelle** des personnels, défini par leur fonction et dans les limites des **délégations** qui leur sont accordées.

Un usage personnel **ponctuel et raisonnable** de la messagerie et de l'Internet est néanmoins toléré en aide à la vie pratique ou familiale dès lors qu'il n'est pas susceptible d'affecter la qualité du service associé. Les informations à caractère privé doivent être clairement identifiées comme telles (option « Privé » dans les critères OUTLOOK, notamment). Il en est de même des supports recevant ces informations (répertoire « PRIVÉ »).

Cette utilisation est soumise à une autorisation **strictement personnelle** qui ne peut, en aucune manière, être cédée, même temporairement, à un tiers sans engager la responsabilité du titulaire. Elle peut être révoquée à tout instant et prend fin en cas de suspension momentanée ou définitive de l'activité professionnelle qui l'a justifiée.

# Bon usage des ressources

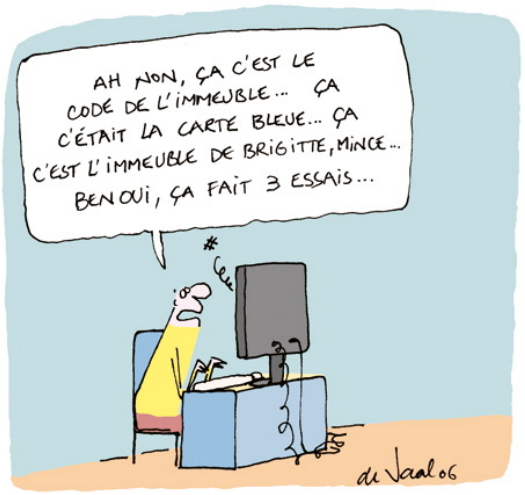
Chaque collaborateur est responsable de l'usage des ressources du système d'information auxquelles il accède. Contribuant, à son niveau, à la sécurité générale, il doit les utiliser de **façon rationnelle** et **loyale** afin d'en éviter la saturation ou le détournement à des fins personnelles.

## Il doit :

- **Protéger** ses accès au système d'information en utilisant les moyens de contrôle imposés ;

  *Exemple : Pendant mes absences temporaires, je mets un mot de passe de veille sur mon poste de travail*

- **Choisir des mots de passe robustes** et ne jamais les communiquer à des tiers :




*Des astuces pour constituer des mots de passe sont fournies sur le site Intranet «Sécurité des systèmes d'information» : (http://www.securitesi.sncf.fr/sections/public)*

## Il ne doit pas :

- **Faciliter l'intrusion** dans le système d'information en introduisant des failles de sécurité dans l'architecture réseau, notamment par l'usage de **modems** connectés directement aux réseaux publics ;

  *Exemple : Je ne tente pas de charger un logiciel personnel, une nouvelle carte graphique...*

- **Contourner les dispositifs de sécurité** de son poste de travail, notamment les antivirus ;

  *Exemple : Je ne tente pas de suspendre, même temporairement, l'antivirus de mon poste de travail,*

- **Tenter de s'approprier** ou déchiffrer le **mot de passe** d'un autre utilisateur.

# Bon usage des ressources *(suite)*

## Il doit :

- **Appliquer les règles de sécurité** en vigueur dans l'Entreprise, éventuellement complétées dans l'entité à laquelle il appartient :
(voir http://www.securitesi.sncf.fr/sections/public)

  *Exemples : Je porte mon badge, je ne communique pas les codes de la porte, je ne confie pas la clef des locaux.*

- **Être vigilant** et signaler tout constat, tentative ou soupçon de **violation** d'une ressource du système d'information à sa hiérarchie ou au responsable de la sécurité des systèmes d'information de son entité, et, de façon générale, toute anomalie qu'il peut constater.

  *Exemple : Je signale à mon service informatique tout message à caractère commercial non sollicité (vente par correspondance, transactions financières...)*

## Il ne doit pas :

- **Exploiter ni tenter d'exploiter** une éventuelle faille de sécurité du système d'information, ni en faire la publicité ;
- **Usurper une identité** ou masquer la sienne ;

  *Exemple : je n'utilise pas le compte d'un autre utilisateur.*

- **Quitter son poste de travail** sans s'être déconnecté, laissant ainsi des ressources accessibles.

  *Exemple : Je ne finis pas ma journée sans verrouiller la session de mon poste de travail, ou sans l'éteindre.*

# Protection de l'information

La protection du patrimoine d'information de l'Entreprise vise avant tout à assurer sa **disponibilité**, son **intégrité** et sa **confidentialité** (communication aux seules personnes « habilitées à en connaître »). Même si des dispositions organisationnelles et techniques sont prises au niveau de l'Entreprise, elles ne constituent qu'un premier niveau de protection. Chaque utilisateur a un rôle individuel essentiel à jouer.

## Il doit :

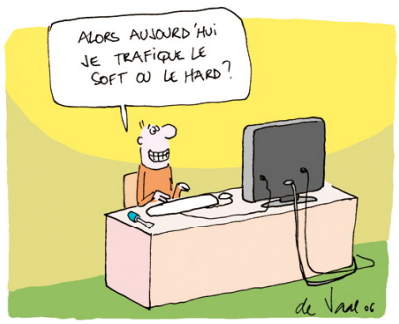
- **Assurer la protection et la confidentialité des informations** qui lui sont confiées ou dont il a connaissance, dans le respect des règles en vigueur au sein de l'Entreprise ;

  *Exemples : Lors de mes déplacements je fais preuve de discrétion lorsque j'échange des informations à usage interne.*

  *Je contacte le service de la communication avant toute prise de parole ou communication en externe.*

- **Respecter l'intégrité des configurations qui lui sont fournies** : l'installation de logiciels ou de matériels ou la modification du paramétrage des ressources auxquelles il accède sont interdites ;

  *Exemple : Je ne connecte aucun accessoire personnel sur mon poste de travail.*




- **Assurer la pérennité des informations** gérées au niveau de son environnement de travail en utilisant les différents moyens de sauvegarde et de duplication mis à sa disposition.

  *Exemple : Je sauvegarde régulièrement mes dossiers et je conserve les sauvegardes dans une pièce distincte.*

## Il ne doit pas :

- **Utiliser** des informations mises à la disposition d'autres utilisateurs, quand bien même celles-ci ne seraient pas explicitement protégées ;

  *Exemple : Je ne copie pas ou je n'utilise pas de document dont je ne suis pas destinataire.*

- **Transmettre d'informations sensibles** à l'extérieur de l'Entreprise, par le biais de la messagerie ou de tout autre support, sans protection et sans autorisation ;

  *Exemple : Je ne diffuse à l'extérieur de l'entreprise que des documents explicitement identifiés comme diffusables.*

- **Apporter volontairement des perturbations** au bon fonctionnement du système d'information, que ce soit par des manipulations anormales des ressources matérielles et/ou logicielles ou par l'introduction de programmes malveillants tels que virus, logiciels espion… ;

  *Exemple : Je ne réponds pas "à tous" les destinataires d'un mail envoyé à plusieurs centaines d'utilisateurs.*

- **Contourner les restrictions** d'utilisation des ressources mises à sa disposition par les services de l'Entreprise.

# Législation

**« Nul n'est censé ignorer la loi ».**

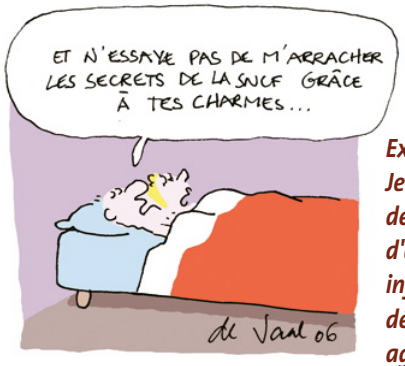
Ainsi, chaque collaborateur peut être tenu pour responsable civilement et/ou pénalement dans sa mission au quotidien, en cas de manquement à ses obligations légales et/ou régle mentaires. En être conscient permet de mieux assumer ses responsabilités.

## Il doit :

- **S'interdire**, en dehors de sa propre activité professionnelle, **tout usage ou toute communication d'information** sur l'Entreprise, ses filiales, ses partenaires, ses clients et ses personnels ;
- **Protéger les droits de propriété** de l'Entreprise pour l'ensemble de ses savoirs et savoir-faire et, notamment, pour tous les logiciels qu'elle a fait développer ;

*Exemple : Je ne copie pas la disquette ou le CD des horaires SNCF pour les donner à des tiers.*

- **Respecter strictement le secret professionnel** lors du traitement des informations médicales ou juridiques concernant des personnels ;




*Exemple : Je ne laisse jamais à des tiers la possibilité d'accéder aux informations que je détiens sur les autres agents.*

## Il ne doit pas :

- **Chercher à porter** atteinte directement ou indirectement au droit des personnes, à leur honneur et considération ainsi qu'à leur vie privée ;

*Exemple : Je ne publie pas de clichés, vidéos... sans avoir obtenu l'accord écrit des personnes représentées, je ne publie pas leurs propos sans leur accord.*

- **Se rendre coupable**, directement ou indirectement, notamment par le biais des moyens informatiques, de **délits dits « de presse »** (diffamation, injure …) ou à procéder au stockage de documents proscrits par la loi (détention d'images ou de textes à caractère pédophile et/ou raciste, …) ;

*Exemple : Je n'utilise pas mon adresse e-mail professionnelle pour participer à des forums externes.*

# Législation

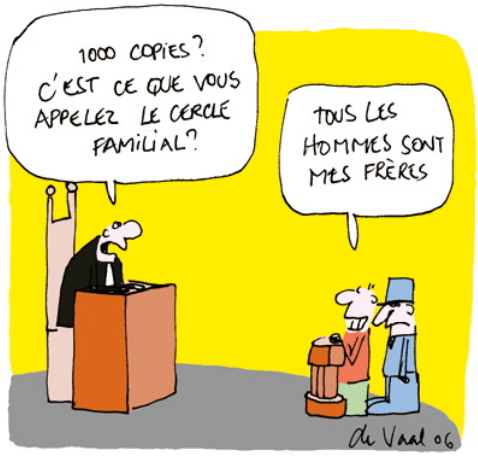
*(suite)*

## Il doit :

**N'utiliser pour la protection des informations que les seuls moyens de chiffrement** mis à sa disposition par l'Entreprise dans le respect des contraintes associées ;

*Exemple : Je m'assure qu'au moins une autre personne de mon service possède les codes d'accès aux documents professionnels protégés par chiffrement.*

**S'interdire de porter atteinte** au droit d'auteur ou de se rendre coupable de contrefaçon, en particulier en faisant une **copie d'un logiciel commercial** pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.




*Exemple : Je ne télécharge ni musique, ni vidéos, ni logiciels.*

## Il ne doit pas :

**Utiliser ou détourner à son profit** ou à celui d'un tiers tout ou partie du système d'information auquel il a accès, que ce soit ou non dans l'exercice de ses missions ;


*Exemple : Je ne peux utiliser mon poste de travail à des fins privées qu'avec modération. Au-delà de 30 courriels par mois ou 5% de capacité du disque dur, il y a abus.*

**Porter atteinte**, directement ou indirectement, aux systèmes de traitement automatisés des données, aux bases de données et aux logiciels : intrusion ou utilisation sans autorisation… ;

*Exemple : Je ne détruis pas de fichier dont je ne suis pas l'auteur ou le responsable.*

**Intercepter ou écouter des communications** ou se livrer à la surveillance des autres postes de travail.

*Exemple : Je n'enregistre pas les conversations et je ne consulte pas le courrier de mes collègues.*

# Usage de l'internet (Web, messagerie, forum...)

L'usage des services offerts par INTERNET devient un élément prépondérant du système d'information de l'Entreprise. Ses spécificités génèrent de nouveaux risques auxquels il faut être particulièrement vigilant, eu égard à la mondialisation de son étendue. La loi et les règlements évoluent régulièrement et varient en fonction des États ; chaque collaborateur a le devoir de se tenir informé des nouvelles clauses ou restrictions d'usage.

## Il doit :

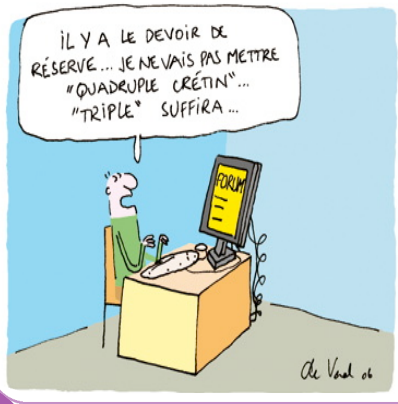
**Utiliser** les services Internet dans le cadre strict des droits accordés et des accès autorisés dans le respect des principes et règles propres aux divers sites concernés ;

*Exemple : Je ne consulte pas de sites inapropriés (pornographie, jeux, piratage...) même s'ils sont accessibles.*

**Faire preuve** de la plus grande correction à l'égard de ses interlocuteurs dans le cadre des échanges électroniques (courrier, forums de discussion …) ;

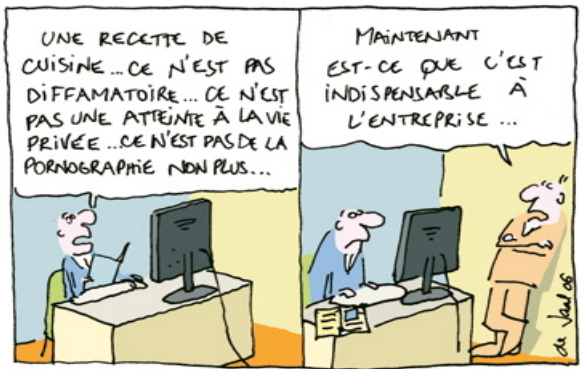
*Exemple : Je m'identifie, je respecte mes interlocuteurs, je ne sature pas les forums internes, je ne me livre pas à des attaques personnelles dans ces forums.*

**Observer un devoir de réserve** et se garder d'émettre une opinion personnelle étrangère à son activité professionnelle, susceptible de porter atteinte à l'Entreprise ;




## Il ne doit pas :

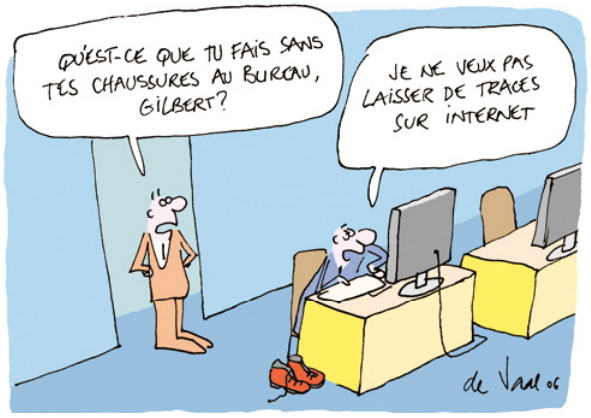
**Consulter ou télécharger** des données (textes, images, sons) ayant un caractère explicitement indécent, contraire à l'ordre public, portant atteinte à la dignité ou à la vie privée, à caractère injurieux, raciste, pornographique, diffamatoire ou en rapport avec une secte ;




**Transgresser** les autorisations d'accès à Internet ; de façon dissimulée ou non, **porter ou proférer des propos** à caractère injurieux, raciste, pornographique ou diffamatoire.

## Contrôle de l'usage des ressources

L'Entreprise doit pouvoir répondre aux requêtes émanant des tribunaux ou des organismes de police relatives au comportement de ses collaborateurs, notamment lors de l'usage des ressources de son système d'information. A ces fins, elle met en œuvre des **moyens d'enregistrement** et d'**analyse**. Les informations associées jouissent d'une protection particulière contre tout risque de divulgation.




Par ailleurs et dans le respect des dispositions législatives et réglementaires, notamment par référence à la Loi « informatique et libertés », l'entreprise met en œuvre des moyens de contrôle et d'investigation utiles à la sauvegarde de ses intérêts. Ces contrôles sont limités aux mesures quantitatives en ce qui concerne les informations à caractère « privé » explicite.

Lorsque les circonstances l'exigent, l'Entreprise peut être amenée à **restreindre**, voire **fermer**, sans préavis tout accès avec l'extérieur.



## Pour tout renseignement complémentaire

### Notes :

**Notez ici vos contacts utiles :**

- Votre service informatique local :

  .....

- Le responsable de la sécurité du système d'information de votre entité :

  .....

- Le portail Sécurité du système d'information de la SNCF
  **http://www.securitesi.sncf.fr/sections/public**