

Exemple pédagogique de Charte Informatique pour une Entreprise

en date du 15 juin 2004

Note préliminaire : Ce document est utilisé dans le cadre de la **formation à la Sécurité Informatique**, il constitue une compilation mettant en lumière les différents aspects de la sécurité informatique **dans un but pédagogique**.

Son usage direct n'est donc pas possible.

Cependant ce texte peut permettre une sélection et une adaptation en fonction de VOTRE environnement et de VOS besoins.

Les notes additives soulignent certains aspects pratiques et de droit.

Ni la société, ni le formateur, ne pourront être tenus pour responsable de l'usage et des conséquences qui pourraient résulter de ce texte.

Faisant office de règlement intérieur

1. Généralités

1.1. But de cette charte

Cette charte a pour but d'établir un code de déontologie pour régir l'utilisation des ressources informatiques mises à la disposition des adhérents par l'association. Elle sert également à faire prendre conscience aux adhérents de certains risques qu'ils pourraient encourir et des conséquences de tels risques.

1.2. Définitions

1.2.1. Utilisateurs

On entend par utilisateur une personne faisant partie du personnel de l'Entreprise et ayant accepté les termes de la présente charte par sa signature.

1.2.2. Invités

On entend par invité toute personne ayant été dûment autorisée à utiliser une ressource informatique de l'Entreprise. Cette autorisation est écrite (voir Annexe) et limitée dans le temps. Elle est signée par l'invité en même temps que cette charte. Il est invité par un utilisateur nommément désigné sur cette autorisation et qui fait partie du personnel de l'Entreprise. L'acceptation d'un invité dans l'Entreprise implique en particulier et expressément la signature de cette charte, sans préjuger d'autres conditions liées à l'usage des matériels informatiques de l'Entreprise. Dans le cadre de l'usage des ressources informatiques de l'Entreprise les droits et obligations d'un invité sont identiques à ceux d'un utilisateur.

1.2.3. Opérateurs

On entend par opérateurs les membres du Service Informatique. Ils signent cette charte au même titre que les autres usagers. Leurs droits sont plus étendus en terme de d'utilisation

1.2.4. Matériels et logiciels

L'Entreprise n'est responsable que des matériels et des logiciels inclus dans l'enceinte de ses locaux, soit dans les postes de travail, soit dans les serveurs, ainsi que des matériels associés permettant en particulier les impressions papier et la numérisation et du matériel permettant le fonctionnement du réseau interne. Les matériels multimédia tels que graveurs de CD ou DVD sont inclus expressément dans la mise en application de cette charte.

1.2.5. Opérateurs externes

Des opérateurs externes à l'Entreprise sont habilités par la direction informatique à travailler sur ces matériels et logiciels dans le cadre strict de missions définies par une commande qui précise les objectifs et les moyens mis en œuvre. Il

1.2.6. Ressources informatiques

On entend par ressources informatiques tous les moyens mis à la disposition des utilisateurs (serveurs, postes locaux, imprimantes, matériels liés au réseau, câbles, etc.) par l'Entreprise. Cela inclut notamment les moyens d'accès aux ressources extérieures à l'Entreprise fournis par toute Entreprise extérieure, telle que France Telecom ou le prestataire fournisseur d'Accès à Internet.

2. Droits et devoirs

2.1. Droits et devoirs des adhérents

Les adhérents de l'association ont des droits sur lesquels veillent les opérateurs (accès aux ressources, confidentialité), mais ils ont également des devoirs :

2.1.1. Informations à fournir

Les adhérents sont tenus de fournir aux opérateurs des informations valides, notamment concernant des indications comme leur adresse familiale et leur adresse sur le campus de l'Entreprise.

2.1.2. Conditions d'accès à une ressource

Les adhérents ont le droit d'accéder aux ressources partagées par l'association. Ce droit d'accès peut être modifié ou retiré si l'adhérent a eu un comportement en désaccord avec cette charte.

L'adhérent est tenu responsable personnellement de l'utilisation faite des ressources informatiques à partir de son poste de travail. L'utilisateur ou l'invité est seul responsable de la sécurité sur son poste de travail (il est notamment important de ne jamais communiquer son mot de passe à quiconque), ainsi que de son administration.

2.1.3. Respect de la confidentialité

Les fichiers d'un utilisateur sont sa propriété privée, même s'ils sont physiquement accessibles. Partant de ce principe, la possibilité de lire un fichier n'équivaut pas à l'autorisation de le lire. L'interception des données d'un utilisateur sur le réseau est également une atteinte à la confidentialité de l'utilisateur.

Cependant, en ce qui concerne les droits d'auteurs, il est à noter que rendre une oeuvre accessible est une communication : il y a acte de représentation.

2.1.4. Respect des individus

Ce postulat est vrai dans tous les terrains de la vie quotidienne, y compris dans l'utilisation des outils informatiques.

Tout harcèlement ou injures par le biais de forums électroniques ou de messagerie électronique est une atteinte flagrante à ce noble principe.

2.2. Droits et devoirs des opérateurs

Les opérateurs sont garants de l'application rigoureuse des recommandations de cette charte. Ces personnes ont des

privileges qui leur sont indispensables pour le bon fonctionnement du réseau INTERNE, mais sont bien sur également soumises

à la loi française. Les opérateurs se doivent de :

- fournir à chaque adhérent un accès physique au réseau de la résidence de l'Entreprise, dans la limite des moyens humains et matériels disponibles, et dans la mesure où l'adhérent respecte strictement cette charte.
- respecter la confidentialité,
- informer, sur demande de sa part, la direction de l'Entreprise de toute violation de cette charte.

Pour cela, ils peuvent notamment :

- interrompre certains services,
- imposer des limitations (débits réseau, impressions...) aux utilisateurs,
- stopper brutalement tout acte suspect qui viole les règles d'utilisation du système.

3. Utilisation des ressources communes

Les ressources communes sont en général des ressources onéreuses. Leur partage a pour but d'en faire profiter plusieurs utilisateurs et d'amortir au maximum l'investissement qui a été fait.

Voici les principales règles qui doivent régir l'utilisation de ces ressources.

3.1. Principe d'équité

L'utilisation d'une ressource commune doit se faire de manière équitable si l'on ne veut pas aller à l'encontre du

respect mutuel que se doivent les adhérents. Aucun utilisateur n'a le droit de monopoliser cette ressource pour son propre

travail de façon abusive. Voici quelques points importants à respecter :

- Éviter d'exécuter des programmes occasionnant un ralentissement excessif du réseau interne ou des matériels qui y sont connectés.
- Libérer les matériels prêtés (dont les logiciels) ou mis en partage par l'association dès que l'on estime ne plus en avoir besoin.
- Éviter de transférer des fichiers de taille importante depuis ou vers l'extérieur du réseau interne pendant les heures de pointe.
- Éviter d'envoyer à une imprimante des fichiers de taille importante aux heures de pointe.

3.2. Règles d'utilisation des matériels

Les matériels mis à la disposition des utilisateurs ou des invités fonctionnent avec des logiciels qui ne doivent en aucun cas être :

- désinstallés
- reconfigurés

Tout dysfonctionnement doit être signalé à un opérateur qui lui seul décide des actions à entreprendre. Par dérogation certaines manipulations pourront être effectuées par l'utilisateur :

- soit sous couvert de l'opérateur, soit à distance (aide de la Hot-line),
- soit à l'aide de procédures écrites contenues soit dans les Fiches techniques, soit dans les Livrets de formation.

Il est précisé que chaque matériel est référencé par une étiquette apposée de façon visible sur tous les matériels de l'Entreprise. L'usage de tout autre matériel est strictement interdit. La présence de tels matériels doit être immédiatement signalée à un opérateur.

3.3. Règles d'utilisation du réseau

L'interconnexion actuelle du monde de l'Entreprise à travers des réseaux comme Internet met à la disposition des utilisateurs ou des invités d'innombrables ressources d'informations. Mais l'utilisation de ces réseaux est régie par des règles de bonne conduite sous peine de se voir exclure de cette communauté.

Voici une liste non exhaustive d'actes non tolérés, pouvant entraîner la déconnexion de la machine d'un utilisateur ou d'un invité et la prise de sanctions disciplinaires, voire conduire à des sanctions pénales :

- interruption volontaire du fonctionnement normal du réseau ou de l'une des ressources connectées,
- utilisation de logiciels de lecture ou d'analyse du trafic sur le réseau,
- accès à des informations privées d'autres utilisateurs du réseau,
- intrusion dans un système connecté au réseau,
- modification ou destruction d'informations sur un système connecté au réseau,
- connexion sur une machine sans autorisation préalable de son opérateur.

3.4. Nature des programmes exécutés

Les programmes exécutés sur les machines ne doivent pas, notamment :

- harceler d'autres utilisateurs (messages d'insultes, perturbations sonores, etc.),
- essayer de contourner les barrières de sécurité,
- saturer les ressources communes,
- propager des virus informatiques,
- contourner les protections des logiciels.

4. Respect des restrictions légales

Certaines restrictions d'utilisation des ressources informatiques logicielles ou matérielles sont imposées dans le cadre de l'Entreprise ou dans un cadre plus large prévu par la loi. Chaque utilisateur ou invité est tenu de respecter ces restrictions. En voici les principales :

4.1. Utilisation universitaire de certaines ressources

Certains logiciels ou matériels sont destinés à des fins strictement pédagogiques. L'utilisation de certaines ressources pour des fins commerciales est soumise à une autorisation préalable.

4.2. Droits d'auteur

L'utilisateur est tenu par la législation en vigueur de respecter les droits d'auteurs des oeuvres intellectuelles. L'utilisation qu'il fait des ressources informatiques ne fait pas exception à ce principe.

Il lui est donc notamment interdit de télécharger des contenus multimédias (MP3, films, ...) non libres de droits et/ou de les mettre à disposition par quelque moyen que ce soit sur le réseau sans le consentement de l'auteur.

En plus des sanctions légales encourues par les contrevenants, pouvant aller jusqu'à deux ans d'emprisonnement et 150 000 euros d'amende, ceux-ci s'exposent à des sanctions disciplinaires pouvant aller jusqu'au renvoi pour faute lourde avec mise à pied à effet immédiat. Voir le chapitre 5 "Sanctions".

4.3. Protection du logiciel

Le logiciel bénéficie des mêmes protections légales que toute oeuvre intellectuelle. Seule une copie de sauvegarde est autorisée pour un logiciel officiellement acheté. Toute autre copie illicite est assimilée à un acte de contrefaçon. Le code source d'une application ne peut être inclus dans une application qui va être utilisée ailleurs. Le contournement des restrictions d'utilisation d'un logiciel est considéré comme un délit dont la sanction peut aller jusqu'à deux ans de prison ferme.

Tout acte de piratage de logiciel constaté sur une machine du réseau interne par un opérateur conduira à des sanctions, dont la déconnexion de cette machine. Voir le chapitre 5 "Sanctions".

4.4. La fraude informatique

La loi Godefrain du 5/01/1988 (cf § I.G) considère comme délits les actes suivants :

- accès ou maintien frauduleux dans un système informatique,
- l'atteinte volontaire au fonctionnement du système informatique,
- la tentative de ces délits,
- l'association ou l'entente en vue de commettre ces délits.

5. Sanctions

Les infractions aux principes énoncés dans cette charte peuvent conduire à des sanctions.

Les sanctions internes sont prises par les opérateurs qui jugeront de la gravité de l'acte et prendront les sanctions qui leur semblent adéquates (déconnexion par exemple). Ils suivront alors la procédure prévue qui consiste :

- à consigner les faits,
- à consigner les actions conservatoires qu'il entreprend à ce premier stade
- à en référer dans les délais les plus brefs au Responsable Informatique.

Les opérateurs peuvent également être amenés à remettre le cas entre les mains de la direction de l'Entreprise soit de leur propre initiative, soit sur ordre du Responsable Informatique, soit à la demande de la Direction.

6. Annexes

Les lois énoncées dans ce document sont données à titre purement indicatif, à la date d'édition du présent document et de manière non exhaustive.

6.1. Délits informatiques

La loi française reconnaît certaines actions sur les systèmes informatiques comme étant des délits et prévoit de les

sanctionner. A titre d'exemple (la liste est loin d'être exhaustive) :

- l'intrusion sur un ordinateur à travers un réseau, cf. loi du 5 janvier 1988, article 462 (peines d'amende et de prison)
- en cas d'introduction dans un système informatique, avec ou sans intervention sur le système).
- la copie illicite de logiciels, cf. loi du 3 juillet 1985, article 47 (toute reproduction autre qu'une copie de sauvegarde)
- est une contrefaçon, la copie privée n'est pas autorisée)
- l'emprunt de l'identité d'un tiers, (comprenant l'envoi d'un courrier électronique sous une fausse identité)
- le vandalisme informatique (destruction de fichiers sans en avoir l'autorisation par exemple)

6.2. Sanctions pénales

L'Entreprise est tenue par la loi de signaler toute violation constatée des lois. Les sanctions pénales peuvent aller de 1 mois à plusieurs années de prison et de 300 euros à plusieurs centaines de milliers d'Euros d'amende. Les principales lois françaises et européennes sont :

- le code de propriété intellectuelle,
- la loi du 6/01/1978 sur l'informatique, la sécurité et les libertés,
- la loi du 3/07/1985 sur la protection des logiciels,
- la loi du 5/01/1988 (Godefrain) sur la fraude informatique,
- les articles 462-2 à 462-9 du code pénal,
- la convention européenne du 28/01/1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel,
- la directive de la CEE du 21/12/1988 sur l'harmonisation juridique de la protection des logiciels.

6.3. Extraits du code de propriété intellectuelle

Art. L335-2 - Toute édition d'écrits, de composition musicale, de dessin, de peinture, ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon ; et toute contrefaçon est un délit. La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de deux ans d'emprisonnement et de 150 000 euros d'amende. Seront punis des mêmes peines le débit, l'exportation et l'importation des ouvrages contrefaits.

Art. L335-3 - Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une oeuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.

Art. L335-9 - En cas de récidive des infractions définies aux articles L 335-2 à L.335-4 ou si le délinquant est ou a été lié par convention avec la partie lésée, les peines encourues sont portées au double.

6.4. Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique

Article unique. - Dans le titre II du livre II du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé :

Chapitre III De certaines infractions en matière informatique :

- Article 462-2. Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement d'un mois à un an et d'une amende de 300 euros
- à 7500 euros ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 1500 euros à 15 000 euros.
- Article 462-3. Quiconque aura intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1500 euros à 15 000 euros ou de l'une de ces deux peines.
- Article 462-4. Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatique ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 300 euros à 75 000 euros ou de l'une de ces deux peines.
- Article 462-5. Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3000 euros à 300 000 euros.
- Article 462-6. Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 3000 euros à 300 000 euros ou de l'une de ces deux peines.
- Article 462-7. La tentative des délits prévus par les articles 462-2 à 642-6 est punie des mêmes peines que le délit lui-même.
- Article 462-8. Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.
- Article 462-9. Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.

Document rédigé en deux exemplaires originaux ne comportant aucune modification manuscrite, paraphés sur chaque page et signés avec la mention manuscrite suivante :

Fait à
Le

Nota : les mentions en italiques ne sont applicables qu'aux intervenants externes

« Je soussigné "Nom, prénom", agissant en qualité de "...", pour le compte de la société "...", ai lu et déclare me conformer à la présente charte de Sécurité informatique, Bon pour acceptation, Signature, lieu et date.»