
DIRECTION DES RESSOURCES HUMAINES

CHARTE INFORMATIQUE

POURQUOI UNE TELLE DEMARCHE ?

Nous sommes passés en quelques années d'une époque où les micro-ordinateurs ne dialoguaient presque pas (rappelez-vous quand il n'y avait pas de messagerie), sans ouverture vers l'extérieur, à une situation où le micro est devenu un outil de travail au quotidien et en groupe, toujours plus ouvert sur les bases de données de l'entreprise et sur le monde extérieur.

Dans le même temps, se sont développés le piratage et la malveillance informatique. Cette situation rend l'entreprise plus vulnérable, d'autant que certains incidents de sécurité peuvent venir de l'intérieur même de l'entreprise (défaut de protection, erreur humaine, malveillance,...).

La diffusion des accès Internet à partir des postes de travail ouvre des possibilités d'utilisation de cet outil à des fins autres que professionnelles. Il faut que cet usage privé soit protégé mais strictement réglementé afin qu'il ne porte pas préjudice aux conditions d'accès professionnel et ne remette pas en cause la productivité de l'entreprise. Cofiroute doit s'assurer que le personnel n'utilise pas de façon abusive sans lien direct avec l'activité professionnelle les postes de travail mis à sa disposition.

Cofiroute souhaite que chaque personne de l'entreprise bénéficie des évolutions informatiques pour optimiser son travail tant individuel que de groupe dans un souci permanent de sécurité et de responsabilité. L'atteinte de cet objectif repose concrètement sur l'association de la technique, de mesures de sécurité et du bon comportement de chacun. La mise en place de mesures de sécurité est maintenant une nécessité pour éviter ou repérer l'origine d'intrusions ou d'attaques et pour protéger les informations confidentielles de l'entreprise.

Les obligations d'information et de transparence imposent à l'entreprise d'informer les salariés sur les règles d'utilisation, les moyens de contrôle et de protection qui sont ou seront mis en place pour vérifier l'application de ces règles et ainsi assurer la sécurité du système informatique de Cofiroute.

Les nouvelles pratiques doivent s'intégrer dans le cadre juridique entourant les nouvelles technologies en terme de responsabilité collective et individuelle. Cofiroute veut informer et sensibiliser ses salariés aux exigences de sécurité, attirer leur attention sur certains comportements propres à porter préjudice à l'intérêt collectif de l'entreprise. C'est le but de la présente charte informatique qui constitue un code de bonne conduite sur la route des nouvelles technologies.

Jean-Marc CHAROUD
Directeur Général Délégué

TABLE DES MATIERES

1.	OBJET DE LA CHARTE INFORMATIQUE	3
2.	GENERALITES	3
2.1	Champ d'application de la charte	3
2.2	Responsabilité des utilisateurs.....	3
3.	ACCES AU SYSTEME D'INFORMATION DE COFIROUTE.....	3
3.1	Compte utilisateur	3
3.2	Mots de passe	3
4.	AFFECTATION DES OUTILS.....	3
5.	DEVELOPPEMENT INTERNE.....	4
6.	SECURITE DE L'ENVIRONNEMENT DE TRAVAIL ET ACCES RESEAU	4
7.	UTILISATION DES SERVEURS DE FICHIERS	4
8.	UTILISATION DE LA MESSAGERIE	5
9.	UTILISATION D'INTERNET.....	5
10.	LES VIRUS.....	5
11.	LES PORTABLES.....	6
12.	EN CAS D'INCIDENT.....	6
13.	CONTROLES	6
14.	MODALITES DE DIFFUSION DE LA CHARTE	6

ANNEXE : Dispositions spécifiques concernant l'accès des institutions représentatives du personnel aux nouvelles technologies de l'information et de la communication

1. OBJET DE LA CHARTE INFORMATIQUE

La présente charte a pour objet d'informer les utilisateurs des règles à observer dans l'utilisation des postes informatiques et du matériel mis à leur disposition en vue d'une plus grande sécurité et d'une plus grande fiabilité.

Par ce document, l'utilisateur sera informé des moyens de contrôle et de protection qui seront mis en place par la Direction des Ressources Humaines et la Direction des Systèmes Opérationnels pour vérifier l'application de ces règles.

2. GENERALITES

2.1 Champ d'application de la charte

Les règles définies dans cette charte s'appliquent à tout utilisateur d'un poste de travail susceptible d'accéder au réseau informatique de Cofiroute.

On appelle "utilisateur" toute personne appartenant ou non à l'entreprise, appelée à utiliser les ressources informatiques et les réseaux de la société.

2.2 Responsabilité des utilisateurs

Le poste de travail informatique est attribué à un utilisateur par Cofiroute mais reste la propriété de l'entreprise. Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques.

3. ACCES AU SYSTEME D'INFORMATION DE COFIROUTE

3.1 Compte utilisateur

Un contrôle d'accès est réalisé pour accéder au système informatique de Cofiroute. Des couples "compte utilisateur" et "mot de passe" de connexion sont fournis à chaque utilisateur. Ces codes d'accès sont strictement personnels.

3.2 Mots de passe

Les mots de passe sont un des moyens usuels de validation de l'identité d'utilisateurs qui accèdent à un système ou à un service informatique. Les mots de passe protègent l'accès aux comptes attribués aux utilisateurs, ils valident l'identité de tous les utilisateurs et établissent ainsi les droits d'accès aux équipements ou services informatiques.

Les mots de passe sont personnels et confidentiels. Ils ne doivent être divulgués sous quelle que forme que ce soit et doivent être changés régulièrement.

Le mot de passe choisi par l'utilisateur devra comporter au minimum 6 caractères et être changé au moins tous les 60 jours.

Chaque utilisateur est responsable de l'utilisation des ressources informatiques faites à partir de ses codes d'accès.

4. AFFECTATION DES OUTILS

La Direction des Ressources Humaines est responsable de la gestion du parc micro-informatique.

Seul le matériel fourni par la Direction des Ressources Humaines peut être connecté au réseau ou au matériel de l'entreprise.

Seul le personnel appartenant au Département Entreprise Communicante et Organisation Bureautique (DECOB)¹ ou travaillant pour le compte de celui-ci est habilité à installer une application sur un poste de travail. En aucun cas, l'utilisateur ne doit installer de logiciels de quel que type que ce soit (Software², Shareware³, Freeware⁴) de type ludique ou non sur son poste de travail.

¹ Le DECOB est un département de la Direction des Ressources Humaines.

² Software : Logiciel "professionnel" dont l'installation et l'utilisation impliquent l'achat d'une licence.

La connexion physique d'un matériel sur le réseau informatique, le déplacement ou la réaffectation d'un poste bureautique fixe ou d'un périphérique ne peuvent être réalisés que par une personne appartenant au DECOB ou à la Direction des systèmes Opérationnels (DSO) ou travaillant pour le compte de ceux-ci. Les droits d'accès aux ressources de l'entreprise par les ordinateurs portables (interne ou externe) sont attribués et configurés par le DECOB.

Le DECOB peut supprimer sans préavis tout logiciel non référencé.

Aucune copie de logiciel sous licence ne doit être réalisée et ce quel que soit le support (disquettes ou CD-ROM via graveur).

5. DEVELOPPEMENT INTERNE

Les développements de type bureautique (macro, base file Maker, Access, etc) sont placés sous l'entière responsabilité des utilisateurs (y compris la maintenance).

Les applications partagées dont la disponibilité peut s'avérer sensible doivent répondre aux normes et être qualifiées par le DECOB et la Direction des Systèmes Opérationnels (DSO) qui en assureront alors la maintenance.

Hors bureautique, seul le personnel appartenant ou travaillant pour le compte du DECOB ou de la DSO est autorisé à effectuer des développements informatiques.

6. SECURITE DE L'ENVIRONNEMENT DE TRAVAIL ET ACCES RESEAU

Les documents et médias informatiques sensibles doivent être mis sous clé dans des tiroirs, armoires ou tout autre meuble, lorsqu'ils ne sont pas utilisés.

En cas d'absence de son bureau, l'utilisateur doit protéger l'accès à son poste et au réseau en procédant au verrouillage de celui-ci par l'intermédiaire d'une veille écran avec mot de passe ou en fermant la session de travail en cours.

En dehors du ou des utilisateurs déclarés, les seules personnes autorisées à intervenir sur le poste de travail doivent appartenir au DECOB ou travailler pour le compte de celui-ci.

Les postes doivent être accessibles au personnel habilité par le DECOB. Si une personne ainsi habilitée est amenée à utiliser le mot de passe de l'utilisateur, ce dernier devra modifier son mot de passe après l'intervention.

L'utilisation d'un mot de passe au "set up" est interdite.

Les tentatives d'intrusion ou toutes anomalies suspectées ou constatées doivent être signalées à la Direction des Ressources Humaines par le biais du SVP.

7. UTILISATION DES SERVEURS DE FICHIERS

La sauvegarde des documents se trouvant sur le disque dur local du poste de travail est à la charge de l'utilisateur.

La Direction des Systèmes Opérationnels assure la sauvegarde et la disponibilité des données stockées sur les serveurs.

L'utilisateur est responsable du stockage de ses documents sur le serveur de fichiers.

³ Shareware : Petit programme qui est libre d'installation et d'utilisation pendant une durée déterminée puis payant à terme.

⁴ Freeware : Logiciel entièrement libre d'installation et d'utilisation.

8. UTILISATION DE LA MESSAGERIE

En cas d'absence prolongée, les règles de gestion de la messagerie doivent être utilisées afin de ne pas divulguer le mot de passe personnel.

L'ouverture d'un fichier joint dont l'origine est inconnue présente un risque important d'infection du poste par un virus. L'utilisateur doit détruire sans les ouvrir les messages avec fichier joint dont il ignore la provenance.

En principe, les fichiers exécutables⁵ ne doivent pas être envoyés par la messagerie. En cas de réception d'un tel fichier dont l'origine est inconnue, le message devra être supprimé sans être ouvert.

Pour l'envoi par messagerie de documents confidentiels, la protection du document par un mot de passe s'impose, celui-ci étant alors communiqué par transmission distincte.

Un usage raisonnable de la messagerie dans le cadre des nécessités de la vie courante et familiale est toléré, à condition qu'il n'affecte pas le trafic normal des messages professionnels (en nombre et en volume).

La boîte aux lettres de messagerie et les messages envoyés ou reçus depuis le poste de travail revêtent un caractère professionnel. Il ne peut en être autrement qu'en cas d'indication manifeste du caractère personnel d'un message dans son objet ou dans le nom du fichier dans lequel il est archivé. En cas de nécessité, Cofiroute pourra s'adresser au juge des référés pour mettre le poste sous scellé.

9. UTILISATION D'INTERNET

La connexion à Internet doit être réalisée via le réseau Cofiroute. Les abonnements personnels accessibles via Modem sont interdits.

En principe, seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.

Néanmoins, une consultation ponctuelle et raisonnable, pour un motif personnel, des sites Internet dont le contenu n'est pas contraire à l'ordre public, aux bonnes mœurs et ne mettant pas en cause l'intérêt et la réputation de l'entreprise est tolérée.

L'entreprise se réserve néanmoins le droit d'interdire l'accès à certains sites.

il est interdit de télécharger des logiciels, à l'exception des personnes travaillant pour le compte de la DSO ou du DECOB.

10. LES VIRUS

Chaque utilisateur est responsable des documents utilisés et stockés sur son poste bureautique. Il doit être conscient des risques qu'il fait courir à l'entreprise en ne respectant pas les règles élémentaires de précaution vis-à-vis des risques de contamination par un virus informatique (destruction de la totalité des données de son disque dur, paralysie du système informatique de l'entreprise...).

L'ouverture d'un fichier dont la provenance est inconnue présente un risque d'infection du poste par un virus. L'utilisateur détruira les fichiers dont il ignore l'origine.

En cas d'alerte de l'antivirus lors de l'ouverture d'un document, l'utilisateur doit se renseigner auprès du SVP et ne pas le diffuser.

⁵ Un fichier exécutable est un fichier de type ".exe" dont le lancement génère une action au niveau du poste de travail

11. LES PORTABLES

La sécurité des postes portables doit faire l'objet d'une attention toute particulière. En effet, la présence de données locales sur le disque dur ainsi que la possibilité de connexion distante au système informatique de Cofiroute rendent sensible ce type de matériel.

L'utilisateur doit s'efforcer de protéger le portable du vol et de toute dégradation.

12. EN CAS D'INCIDENT

Lors d'un incident ou de la suspicion d'un incident, l'ordinateur doit, si possible, être déconnecté des réseaux informatique et électrique et toute utilisation de la machine doit être arrêtée. Le SVP doit être averti immédiatement et l'utilisateur doit s'abstenir de toute intervention.

13. CONTROLES

Cofiroute se réserve le droit de procéder à des contrôles réguliers des logiciels et des données des systèmes serveurs et postes de travail.

Les données illicites ou dangereuses (par exemple, tout fichier non approuvé sur un serveur de fichier : exécutable, ...) seront supprimées par la DSO. Les données entraînant une gêne à la productivité seront isolées par la DSO (déplacement des données concernées sur un support inaccessible) puis supprimées après avoir averti les personnes concernées.

Concernant l'usage de la messagerie, un dispositif de traçabilité est mis en place. Par traçabilité, on entend écriture dans un fichier "trace" d'information concernant les émetteurs et destinataires de messages, leur objet (titre du message), le nom des pièces jointes ainsi que la date et l'heure des envois, à l'exclusion de toute autre information. Les données ainsi collectées sont conservées pendant une durée de 7 mois maximum.

Concernant la connexion Internet, un dispositif de suivi individuel de chaque compte utilisateur est mis en place, produisant un relevé des dates et heures de connexion et des sites et pages visités, à l'exclusion de toute autre information. Les données ainsi collectées sont conservées pendant une durée de 7 mois maximum.

Ces dispositifs de traitement automatisé d'informations nominatives ont fait l'objet d'une consultation du Comité d'Hygiène, de Sécurité et des Conditions de Travail le 10 avril 2003 et du Comité d'Entreprise le 25 mars 2003. Ils ont par ailleurs fait l'objet d'une demande d'avis à la Commission Nationale de l'Informatique et des Libertés qui a été enregistrée le 6 mai 2003 sous le numéro 854659 et pour laquelle la CNIL a rendu un avis favorable.

Conformément à la loi, chaque utilisateur dispose d'un droit d'accès aux informations le concernant. Ce droit d'accès s'exerce directement auprès du Directeur des Ressources Humaines qui remet à l'utilisateur sur sa demande et sous huitaine un relevé des informations enregistrées à partir de son identifiant. Celui-ci pourra demander la rectification des données qui se révéleraient inexacts dans le support informatique en cours. Le cas échéant, un nouveau relevé corrigé serait remis au demandeur sous huitaine.

14. MODALITES DE DIFFUSION DE LA CHARTE

La présente charte est remise à chaque utilisateur et affichée dans l'entreprise. Un exemplaire est par ailleurs remis au secrétaire du Comité d'Entreprise, au secrétaire du CHSCT ainsi qu'aux délégués syndicaux. Un exemplaire est également transmis à l'inspecteur du travail pour information.

CHARTRE INFORMATIQUE : ANNEXE

Dispositions spécifiques concernant l'accès des institutions représentatives du personnel aux nouvelles technologies de l'information et de la communication

La Direction, consciente de l'intérêt, pour le développement et la bonne qualité du dialogue social, de l'accès des partenaires sociaux aux Nouvelles Technologies d'Information et de Communication (NTIC), décide d'attribuer des moyens en ce sens aux organisations syndicales représentatives, au CHSCT et au Comité d'Entreprise et d'encadrer leur utilisation. Les conditions d'utilisation sont les suivantes :

TABLE DES MATIERES

1.	MISE A DISPOSITION DE MOYENS MATERIELS INFORMATIQUES.....	8
2.	ACCES A L'INTRANET	8
3.	ACCES A LA MESSAGERIE ELECTRONIQUE	9
4.	ENCADREMENT ET SANCTIONS	9

1. MISE A DISPOSITION DE MOYENS MATERIELS INFORMATIQUES

L'entreprise met à la disposition de chaque organisation syndicale représentative le matériel utile pour l'accès aux NTIC.

Le matériel informatique attribué dans ce cadre se compose d'un micro-ordinateur, d'une imprimante, de logiciels bureautiques.

Par ailleurs, l'entreprise met en œuvre les moyens nécessaires pour l'accès à l'intranet (Cofiweb), à Internet et à la messagerie électronique.

L'entreprise assure l'entretien et la mise à jour des matériels mis à disposition des organisations syndicales. Les produits consommables seront à la charge de l'organisation syndicale.

Les matériels définis ci-dessus sont placés sous l'entière responsabilité de l'organisation syndicale utilisatrice qui doit s'assurer de leur bonne conservation et des conditions d'utilisation qui en sont faites. Ces matériels restent la propriété de l'entreprise et ne peuvent être déplacés hors du local attribué à l'organisation syndicale.

Un dispositif identique est mis en place pour le Comité d'Entreprise.

Un ordinateur portable équipé de logiciels bureautiques sera mis à la disposition du secrétaire du CHSCT dont la connexion au réseau interne pourra se faire dans les locaux de l'entreprise, tout comme les impressions nécessaires à son activité.

2. ACCES A L'INTRANET

La Direction décide de mettre à disposition des organisations syndicales représentatives, à titre d'expérimentation pendant une période d'un an à partir de la date de mise en application, un espace d'expression dédié sur l'intranet de l'entreprise : Cofiweb. Cet espace respecte le format et l'organisation générale du site intranet de l'entreprise. Il est mis en place par l'entreprise en fonction des rubriques souhaitées par les organisations syndicales qui sont responsables du contenu et de la mise à jour.

Cet espace est soumis aux règles qui concernent l'affichage sur les panneaux syndicaux. Les informations contenues dans l'espace intranet relèvent de la responsabilité d'un rédacteur désigné par les délégués syndicaux et doivent revêtir un caractère exclusivement syndical. Le contenu des pages intranet doit respecter les dispositions sur le droit de la presse et ne doivent à ce titre contenir ni injure, ni diffamation. De même, elles doivent respecter la dignité des personnes, la vie privée et le droit à l'image.

Chaque communication syndicale est transmise automatiquement, à l'identique, au Directeur des Ressources Humaines, simultanément à sa publication sur le Cofiweb.

Des espaces intranet sont également réservés au Comité d'Entreprise et au CHSCT. Ils ne doivent contenir que des informations ayant un lien direct avec les attributions de l'instance concernée. De même que les espaces syndicaux, ces informations doivent respecter les dispositions sur le droit de la presse et ne doivent contenir ni injure, ni diffamation et respecter la dignité des personnes, la vie privée et le droit à l'image.

Conformément au droit de la propriété intellectuelle, les logos de l'entreprise ou de ses produits et services ne peuvent être utilisés ou modifiés sans l'autorisation formelle préalable de celle-ci.

Les espaces intranet attribués à chaque organisation syndicale, au Comité d'Entreprise et au CHSCT ne doivent contenir ni fichier audio, ni fichier vidéo, ni lien hypertexte vers l'extérieur.

Chaque espace syndical doit être identifiable dès son ouverture par l'affichage du nom et du logo de l'organisation syndicale.

Les espaces réservés au Comité d'Entreprise et au CHSCT doivent eux aussi pouvoir être clairement identifiés dès leur ouverture.

La date de mise à jour doit être indiquée pour chaque information publiée.

Pour assurer une utilisation optimale du matériel mis à disposition des organisations syndicales, du Comité d'Entreprise et du CHSCT, une formation sera proposée au rédacteur désigné par chaque organisation, au secrétaire du Comité d'Entreprise et au secrétaire du CHSCT (ou un autre membre de ces instances désigné par eux) sur demande formulée auprès du Directeur des Ressources Humaines. Le temps consacré à la formation du rédacteur désigné, du secrétaire du Comité d'Entreprise et du secrétaire du CHSCT (ou d'un autre élu de ces instances) n'est pas pris en charge par l'entreprise.

Les documents accessibles sur le Cofiweb, à l'exclusion des documents accessibles sur les espaces réservés aux instances représentatives du Personnel qui restent leur propriété respective, sont la propriété de l'entreprise et ne peuvent être diffusés à l'extérieur sans accord exprès préalable de l'entreprise, leur contenu ne peut être divulgué.

3. ACCES A LA MESSAGERIE ELECTRONIQUE

Une adresse messagerie est attribuée à chaque organisation syndicale représentative.

En aucun cas, la messagerie électronique ne pourra servir à la diffusion d'information ou de tract de façon collective.

La messagerie électronique permet au salarié de s'adresser à l'organisation syndicale de son choix à partir de son outil informatique.

Une organisation syndicale ne peut, en aucun cas, prendre l'initiative d'une communication auprès d'un salarié sans sollicitation préalable de la part de celui-ci. La réponse adressée par l'organisation syndicale ne peut être qu'individuelle et doit être strictement confidentielle.

La messagerie électronique peut être utilisée dans le cadre des actes de gestion courante du mandat, du dialogue entre organisations syndicales ou avec la Direction (interlocuteurs habituels de la Direction de l'entreprise et en particulier de la Direction des Ressources Humaines).

Ces mêmes règles s'appliquent au Comité d'Entreprise et au CHSCT.

Néanmoins, le Comité d'Entreprise, dans le cadre de ses activités sociales et culturelles, pourra prendre l'initiative d'utiliser la messagerie électronique pour informer un ou plusieurs utilisateurs sur le suivi de leurs demandes ou l'organisation d'une activité pour laquelle ils se sont inscrits ou ont demandés des renseignements.

L'entreprise se réserve le droit de remettre en cause cette disposition en cas d'abus manifeste.

4. ENCADREMENT ET SANCTIONS

Les dispositions de la Charte Informatique sont applicables au Comité d'Entreprise, au CHSCT et aux organisations syndicales.

Certaines pratiques sont par ailleurs formellement interdites :

- La diffusion de documents en grand nombre,
- Les outils de discussions en temps réel ("Chats") et forum de discussions,
- La diffusion de tracts par messagerie,
- La diffusion collective démultipliée ("Chaîne"),
- L'envoi de courrier électronique à un salarié ne l'ayant pas sollicité,
- Le téléchargement de vidéo, images animées et bandes son,
- L'installation de logiciels.

En cas de non respect des dispositions du présent document, des mesures seront imposées par l'entreprise. Ces mesures peuvent notamment consister en :

- La diffusion d'un message correctif sur le Cofiweb et dans l'espace réservé aux organisations syndicales, au Comité d'Entreprise ou au CHSCT,
- La fermeture temporaire de l'espace réservé.

Ces mesures peuvent aller, en cas de récidive, jusqu'au retrait des moyens matériels informatiques accompagné de la fermeture définitive de l'espace réservé.