Charte informatique - Droits et obligations de chacun sur l'intranet

Quelques points d'attention particulière dans cette version publiée en Octobre 2014:
- les éléments de cadrage d'un usage privé limité et raisonnable
- les conditions d'accès aux données professionnelles d'un agent absent, parti, ou décédé
- les conditions d'intervention sur une activité informatique inopportune
- l'encouragement à un usage mesuré de la messagerie électronique
- les conditions d'usage du nom "Ifremer" sur sites Web
- la vigilance à garder sur les matériels, logiciels, données de connexion mis à disposition
- les conditions de raccordement de matériel au réseau interne (pas de poste de travail personnel , par exemple...)
etc...

Objet : Conditions d'usage et de sécurité des moyens informatiques de l'IFREMER

PREAMBULE

Chaque salarié de l'IFREMER ou d'établissements hébergés sur un site Ifremer peut disposer d'un compte informatique et accéder grâce à celui-ci à de nombreux services décrits dans les pages :

http://w3z.ifremer.fr/intraric

L'évolution technologique et les nouveaux usages des moyens informatiques rendent nécessaires la mise à jour de l'Instruction PDG n° 03/006 du 13 mai 2003 intitulée « Conditions d'usage et de sécurité des moyens informatiques de l'Ifremer».

La présente Charte a pour objectif la protection des intérêts de l'Ifremer tout en préservant les droits des salariés. Elle vise à améliorer la protection des moyens, matériels et immatériels de l'Ifremer et à rappeler que l'utilisation des **Systèmes d'Information** et des **Outils Informatiques** est destinée aux besoins professionnels. L'usage pour des raisons privées par les personnes doit être limité et raisonnable.

La Charte définit les conditions d'usage et de sécurité que l'Utilisateur au sens de la présente Charte, habituel ou temporaire, des **Outils Informatiques** et/ ou **Système d'Information** de l'IFREMER, s'engage à respecter.

Les présentes dispositions sont applicables, sous réserve des droits des tiers relatifs à la propriété intellectuelle et à la confidentialité.

Tout acte pris en méconnaissance des présentes dispositions ne pourra entraîner la responsabilité de l'Ifremer et sera réputé avoir été réalisé au nom et pour le compte de son auteur. Il pourra faire l'objet, le cas échéant, de mesures disciplinaires ou/et juridiques.

En vertu des dispositions de l'article L 1321-4 du code du travail, la présente Charte a été soumise pour consultation aux Membres du Comité Central d'entreprise de l'UES Ifremer Genavir le 25 mars 2014 et des 6 CHSCT les 14 mai (Centre Atlantique), 16 mai (Issy), 20 mai (Centre Bretagne), 23 mai (Centre Manche Mer du Nord), 27 mai (Centre du Pacifique), et 2 juin 2014 (Centre de Méditerranée). Elle a été déposée à l'inspection du travail de Nanterre et au secrétariat du greffe du Conseil des Prud'hommes de Boulogne-Billancourt. Toute modification de la présente Charte fera l'objet de cette même procédure de consultation, de publicité et de dépôt. En raison de ce formalisme, la présente Charte a la même valeur que le règlement intérieur.

La présente Charte est portée à la connaissance de chaque nouvel arrivant, au travers du premier message électronique adressé par la Direction Informatique de l'Ifremer au moment de la création de son compte informatique. L'utilisation par l'Utilisateur de son compte informatique constitue l'acceptation de toutes les dispositions de la Charte.

1. Objet- définitions.

Par **Utilisateur**, on entend toute personne physique ayant un accès autorisé à un Outil Informatique ou Système d'Information de l'IFREMER (personnel permanent ou temporaire de l'IFREMER, ou personnes extérieures jouissant d'un accès autorisé).

Par **Utilisateur IFREMER**, il faut entendre tout Utilisateur personne physique liée à l'IFREMER par un contrat de travail à durée déterminée ou indéterminée.

Par **Outils Informatiques** ou **Système d'Information** de l'IFREMER, on entend : ordinateurs (fixes ou portables), périphériques, assistants personnels, réseaux informatiques (serveurs, routeurs, commutateurs et connectiques), clés USB, photocopieurs, téléphones, tablettes, logiciels, fichiers, données et bases de données, systèmes de messagerie, intranet, extranet, comptes twitter, blogs, réseaux sociaux, abonnements à des services interactifs, sous la responsabilité et le contrôle de l'IFREMER.

Cette liste n'est ni exhaustive, ni limitative. Tout nouvel élément matériel, logiciel ou plateforme d'accès à distance à venir, acquis au nom et pour le compte de l'IFREMER, devra être entendu comme faisant partie des Outils Informatiques ou Système d'Information.

Pour l'application de la présente Charte, sera aussi réputé comme faisant partie du **Système d'Information**, tout matériel, quel qu'en soit le propriétaire, dès lors que celui-ci est connecté au réseau de l'IFREMER et/ou contient des informations appartenant à l'IFREMER.

Les notions de **Systèmes d'Information** ou d'**Outils Informatiques** recouvrent également tous les aspects fonctionnels de l'informatique, c'est-à-dire l'utilisation qui en est faite par les Utilisateurs et les Animateurs.

Par **Direction Informatique**, on entend le service en charge des Outils Informatiques communs et architectures associées de l'IFREMER.Par **Administrateur Système**, on entend la personne physique identifiée de l'IFREMER, gestionnaire du mot de passe du compte système, sur un ordinateur raccordé au réseau de l'IFREMER.Par **Rédacteur**, on entend l'Utilisateur qui assure la responsabilité ou contribue à l'animation rédactionnelle d'un site Internet ou extranet estampillé du logo de l'IFREMER.Par **Correspondant Informatique**, on entend la personne nommément identifiée par l'Ifremer dans une Unité pour faire l'interfaçage

régulier avec la Direction Informatique, pour le compte de son équipe, et pour diverses interventions informatiques.

2. Accès aux Outils Informatiques et Système d'Information.

2.1. L'accès aux Outils Informatiques et/ ou Système d'Information de l'IFREMER s'opère par l'ouverture d'un compte personnel. L'accès à ce compte est soumis à 3 conditions :

- L'attribution par la Direction Informatique d'un nom de compte Utilisateur, dit compte intranet, personnel à chaque Utilisateur, pour être reconnu par les Systèmes d'Information.
- Le choix par l'Utilisateur d'un mot de passe personnel qui répondra à des règles de longueur et de complexité définies par la Direction Informatique. Ce mot de passe devra être renouvelé périodiquement.
- L'attribution à l'Utilisateur par la Direction Informatique d'un identifiant spécifique, dit compte extranet, confidentiel, qui sera utilisé lors d'une connexion distante.

L'autorisation d'accès à un Outil Informatique ou Système d'Information de l'IFREMER à tout Utilisateur, présent sur une implantation Ifremer ou non, ne peut être délivrée par la Direction Informatique que sur demande d'un agent lié par un contrat de travail à durée indéterminée avec l' IFREMER ou sur demande d'un établissement ayant signé la présente Charte. Cette personne, responsable du compte informatique, peut déléguer la gestion des créations et suppressions de compte au Correspondant Informatique. Chaque agent peut consulter sur la page web

http://w3z.ifremer.fr/intraric/Mon-IntraRIC/Mon-compte/De-qui-suis-je-responsable

la liste des agents dont il est identifié responsable.

Chaque responsable de compte doit participer, de la façon la plus réactive, à la suppression des comptes informatiques obsolètes, en les signalant à l'assistance informatique :

assistance@ifremer.fr

2.2. Chaque Utilisateur est soumis à une obligation particulière de prudence et de vigilance pour l'utilisation des Outils informatiques et/ ou Système d'Information au regard de la sécurité générale de l'IFREMER. Il est responsable de ses identifiants individuels et des conséquences dommageables d'un mauvais emploi d'une connexion à l'aide desdits identifiants. Ceux ci devront être conservés confidentiels par l'Utilisateur et ne devront pas être communiqués à d'autres personnes sauf dans les circonstances énoncées en 6.

L'Utilisateur doit s'assurer de la protection matérielle des programmes et des divers supports mis à sa disposition. Cette protection concerne également la sécurité et l'utilisation des Outils informatiques, notamment portables, à l'extérieur des implantations de l'IFREMER. L'Utilisateur doit s'assurer de la protection de ses informations en suivant les règles élémentaires de sécurité ou/et en utilisant tous les moyens mis à sa disposition.

2.3. Le compte est personnel et confidentiel. Il est ouvert pour les Utilisateurs travaillant sur les implantations de l'Ifremer sur la base d'informations fournies à la Direction Informatique par la DRH Ifremer. Ces informations portent sur l'état civil (prénom et nom), l'employeur, le service d'accueil, le lieu de travail et, pour tout Utilisateur temporaire, le nom du responsable, le numéro de carte IFREMER, le type de contrat avec ses dates de début et de fin, la fonction exercée, le numéro de téléphone et de télécopie, la durée du compte.
Pour les personnes ne travaillant pas sur une implantation de l'Ifremer, les informations sont fournies par le responsable du compte et comportent a minima, les nom, prénom, adresse de messagerie, le nom du responsable et la durée du compte.

Les Utilisateurs autres que les utilisateurs IFREMER, peuvent être inscrits sur les annuaires de l'IFREMER en étant identifiés comme n'appartenant pas au personnel de l'IFREMER. Ils seront automatiquement inscrits dans les listes de diffusion des implantations et des équipes gérées par l'IFREMER dès lors qu'ils sont présents physiquement sur une implantation IFREMER.
Le recueil et le traitement de ces informations font l'objet de la déclaration 352484 du 24 octobre 1994 faite auprès de la CNIL. L'Utilisateur jouit de toutes les protections relatives aux données personnelles en vigueur (voir 9).

2.4. Le catalogue des Directions Informatiques et les engagements de service associés sont décrits dans l'intranet RIC sur :

http://w3z.ifremer.fr/intraric/Mon-IntraRIC/Mon-compte/Engagements-RIC

2.5. L'Utilisateur des Outils Informatiques et/ou Systèmes d'Information s'engage à respecter la charte de l'opérateur Internet auquel est raccordé l'IFREMER. A ce titre, la charte du Réseau National de la Recherche (RENATER), conforme à la présente Charte, doit être observée aussi scrupuleusement que celle de l'IFREMER.

http://www.renater.fr/IMG/pdf/charte_fr.pdf

2.6. Pour la bonne gestion des ressources, l'IFREMER se réserve le droit discrétionnaire de limiter ou modifier, voire supprimer (cf. § 3.1.4), à tout moment et sans préavis, les accès et les fonctionnalités des Outils Informatiques et/ ou Systèmes d'Information.

3. Droits des Utilisateurs et des Rédacteurs lors de leur utilisation du Système d'Information.

3.1. L'utilisation des Systèmes d'Information pour la navigation Internet et la messagerie:

3.1.1. L'usage raisonnable à titre privé d'Internet et de la messagerie est toléré dès lors qu'il préserve l'intégrité du réseau informatique et des intérêts patrimoniaux et moraux de l'IFREMER. Cet usage à titre privé ne doit, en aucune façon, avoir d'effet sur les activités professionnelles de l'Utilisateur IFREMER.

L'IFREMER décline toute responsabilité due à des agissements de l'Utilisateur, dès lors que ces agissements ou propos constituent une faute grave ou sont en dehors de la mission qui lui a été confiée explicitement et pour laquelle l'accès aux Outils Informatiques et aux Systèmes d'Information lui a été accordé. A titre d'exemple, sont notamment considérées comme des

usages non raisonnables, les utilisations suivantes des outils Informatiques et/ ou des Systèmes d'Information, sans que cette liste soit exhaustive:

a) la mention de l'adresse électronique professionnelle IFREMER de l'Utilisateur sur des sites Internet sans rapport avec l'activité professionnelle;

b) la participation de l'Utilisateur à des chaînes de courrier électronique sans lien avec son activité professionnelle;

c) l'utilisation des Outils Informatiques et/ ou Systèmes d'Information par l'Utilisateur pour l'exercice d'une activité commerciale personnelle ou un travail clandestin;

d) Toute action de l'Utilisateur susceptible, notamment:

- de mettre en cause la sécurité matérielle ou juridique de l'IFREMER, et particulièrement des Outils Informatiques et/ ou Systèmes d'Information de l'IFREMER, et ce, de quelque façon que ce soit;
- de porter atteinte à la réputation de l'IFREMER;
- de constituer un manquement à des obligations de l'IFREMER;
- de porter atteinte à un intérêt économique de l'IFREMER;
- de porter à la connaissance de tiers non autorisé des informations confidentielles au sujet des partenaires de l'IFREMER ou de l'IFREMER lui même;

e) L'atteinte par l'Utilisateur aux dispositions des droits de la Presse définie par la loi du 29 juillet 1881 (propos injurieux, diffamatoires ou insultants) envers quiconque, à l'intérieur ou à l'extérieur de l'IFREMER, sur tout support de communication mis à disposition du public que ce soit (blog, réseaux sociaux, forums) à partir des Outils Informatiques et/ ou Systèmes d'Information, sur tous sujets directement ou indirectement liés à l'activité de l'IFREMER ;

f) L'émission par l'Utilisateur de communications offensantes, désobligeantes et/ou des discriminations portant sur la race, l'origine sociale, l'âge ou le handicap, la religion;

g) L'atteinte par l'Utilisateur à un droit de la personnalité de quiconque (droit à l'image et à la voix, droit à la dignité, droit au respect de la vie privée, etc...);

h) L'utilisation des Outils Informatiques et/ ou Systèmes d'Information par l'Utilisateur à des fins politiques ou syndicales (hors les dispositions prévues en application de l'Annexe 1, point 1), ou pour diffuser des tracts ou des messages de même nature;

i) La participation par l'Utilisateur à des jeux et/ou des agissements visant à obtenir des profits ou des gains personnels;

j) La création par l'Utilisateur de sites, de comptes et/ou de pages personnelles en utilisant les Outils Informatiques et/ ou Systèmes d'Information en dehors des conditions énumérées à l'article 3.3 ;

k) La consultation par l'Utilisateur de sites contraires aux bonnes mœurs (pornographie ou tous comportements dégradants) ou ayant des comportements manifestement contraires à l'ordre public (pédopornographie, négation des crimes de génocides, incitation à la haine…)

l) l’utilisation des Outils Informatiques et/ ou Systèmes d’Information par l'Utilisateur pour toute action susceptible d'entraîner la responsabilité civile et/ou pénale de l'IFREMER ou portant atteinte à l'IFREMER ou à l'un de ses intérêts sus-énoncés;

m) l'association par l’Utilisateur du Système d'Information de l'IFREMER à tout délit électronique.

3.1.2. L’utilisation de la messagerie électronique, consommatrice de temps et de ressources disque sur les serveurs, doit être limitée et raisonnée. Il est recommandé de :

- limiter, avec la plus grande attention, le poids des envois et la liste des destinataires en considération des besoins professionnels,
- ne pas oublier que les communications à destination de personnes en mission à l’étranger ou en mer peuvent donner lieu à des factures de télécommunication dont le montant est fonction du volume d'informations reçues,
- favoriser l’usage de quelques lignes introductrices avant toute communication volumineuse.

De façon générale, il importe que chacun ait conscience de ce que ses actions informatiques ont comme incidences sur ses collaborateurs ou sur la mobilisation de la Direction Informatique. Toute intervention logicielle ou matérielle non maîtrisée en terme d'impact doit faire l'objet d'un échange préalable avec la Direction Informatique.

3.1.3 Renvoi des messages électroniques vers l’extérieur

Le renvoi automatisé, par un Utilisateur, de ses messages électroniques, vers une adresse externe peut constituer une fuite d’informations vers des serveurs non maîtrisés susceptibles d’être piratés ou compromis, et donc une perte de propriété intellectuelle. Ce type de renvoi est interdit sauf accord de la Direction Informatique.

3.1.4. L'IFREMER se réserve le droit d’intervenir sur l'accès aux Outils Informatiques et/ ou au Système d'Information à l'Utilisateur en cas d’indices graves d’une utilisation non conforme à la présente Charte. Si le comportement de l’Utilisateur IFREMER est susceptible d’entrainer une procédure disciplinaire, cette déconnexion pourra durer le temps de la procédure déterminant l'existence de sanctions ou non, conformément à l’article 3.5. Si l’Utilisateur est extérieur à l’IFREMER, la mesure sera portée à la connaissance de son établissement de rattachement.

3.2. Droits de propriété intellectuelle

L'IFREMER est titulaire exclusif des droits de propriétés sur sa dénomination sociale et sur son image et seul compétent pour déterminer leur contexte et leur usage. Toute association de la marque ou du logo de l'IFREMER doit être préalablement et expressément autorisée par la Direction de la Communication et des relations institutionnelles de l’IFREMER (DISCOM-RI).

3.3. L’Utilisation d’Internet à des fins de communication en ligne liée à l’activité de l’IFREMER.

La création d'un site Internet au moyen des Outils Informatiques et/ ou des Systèmes d'Information par un Utilisateur IFREMER doit être préalablement et expréssément autorisée selon les conditions fixées par la procédure référencée sur le lien suivant :

http://w3z.ifremer.fr/infosweb/Outils/eZiweb/Demarches.

La procédure comprend :

- une demande d'agrément préalable : comprenant des informations telles que les motifs et objectifs recherchés par le site internet lié à l'IFREMER, l'arborescence, le principe éditorial, le nom du responsable, l'adresse ;
- un avis positif ou négatif rendu conjointement par la Direction de la Communication et des relations institutionnelles de l'IFREMER et la cellule WEB. L'absence de réponse ne vaut pas acceptation implicite.

3.3.1. Dans l'hypothèse d'un avis positif, le Rédacteur sera autorisé à créer un site internet estampillé du sigle de l'IFREMER. Le logo IFREMER et une mention de la propriété intellectuelle de l'IFREMER devront figurer sur chaque page WEB du site.

3.3.2. Le Rédacteur reste soumis à un droit de réserve et à une obligation de confidentialité. Dans ce cadre, tous les propos, toutes les mentions, tous les liens hypertextes, faits par le Rédacteur, se devront de respecter les limites énoncées en 3.1.et ne porteront que sur les matières scientifiques.

3.3.3. La DISCOM-RI peut, en cas de non mise à jour prolongée d'un site, inviter son auteur à le nourrir. A défaut de nouvelles contributions, la DISCOM-RI peut prendre acte et retirer le site, placé sous le sigle de l'IFREMER, de la communication au public.

3.3.4. Au titre de la présente Charte, le Rédacteur d'un site déjà existant et placé sous le sigle IFREMER, reconnaît à la DISCOM-RI un droit rétroactif d'intervenir sur ledit site.

3.3.5. La diffusion d'informations ne doit pas porter atteinte aux intérêts scientifiques et économiques de l'IFREMER ou engager sa responsabilité à l'égard des tiers. Le Rédacteur s'engage à soumettre au préalable au Département ou à la Direction à laquelle il est rattaché, à la Direction scientifique ou à la Direction de la Valorisation et des partenariats économiques, selon le cas, tout projet de contribution avant toute communication au public. L'absence de réponse dans un délai de 2 semaines vaut acceptation implicite de la publication.

Dans l'hypothèse d'un site estampillé IFREMER comprenant des agissements manifestement contraires à l'ordre public (3.1.1.k), l'IFREMER se réserve un droit de suppression immédiat du site litigieux sans le moindre avertissement et communiquera immédiatement toutes les informations d'identification du Rédacteur aux autorités judiciaires compétentes.

3.4. L'Utilisation des Outils Informatiques et Systèmes d'Information à des fins personnelles

Les messages électroniques à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, et sous réserve du respect des principes posés dans la présente Charte.

Pour assurer le caractère personnel des messages envoyés ou reçus, ceux ci doivent mentionner dans leur objet une mention tel que Personnel(s) et être rangés dans un dossier dénommé lui aussi Personnel(s).

L'envoi de message à caractère personnel par l'Utilisateur doit être fait de préférence via un site en ligne.

Le stockage de données privées sur les disques locaux des postes de travail, non sauvegardés, devra être limité, ne pas porter préjudice au fonctionnement général du Système d'Information et être effectué dans un dossier dénommé Personnel(s).

Le stockage de données privées sur les disques réseau, qui font l'objet de sauvegardes automatisées et administrées par la Direction Informatique central, est interdit.

3.5 Utilisation abusive ou non conforme à la charte

L'IFREMER se réserve le droit de faire un avertissement à tout Utilisateur IFREMER salarié, en cas d'utilisation abusive ou non conforme à la présente Charte, des Outils Informatiques et/ ou Systèmes d'Information. Cet avertissement, pris sur le fondement de l'article L 1332-2 du code du Travail, doit être pris en préalable à toute sanction disciplinaire. Le caractère abusif prendra en compte la fréquence d'utilisation à des fins personnelles et la perte de temps effectif travaillé pour l'IFREMER.

3.6.Extensions d'utilisations

Les extensions d'utilisations autorisées des Outils Informatiques de l'IFREMER sont définies dans l'annexe 1.

4. Connexion au réseau

4.1. Tout Utilisateur doit respecter les modalités de connexion au réseau, définies par la Direction Informatique. En particulier, il est interdit de procéder sans l'accord de la Direction Informatique :

- au raccordement d'un équipement réseau – borne wifi, routeur, commutateur, …ou de matériel atypique;
- à la modification d'un raccordement existant ;
- à l'établissement d'un accès Telecom d'un opérateur.

4.2. Toute machine connectée au réseau possède une adresse réseau attribuée par la Direction Informatique. Il est interdit d'utiliser cette adresse pour connecter une autre machine, même temporairement.

4.3 Afin de préserver l'intégrité, la cohérence de la sécurité, et le respect des droits d'usage aux licences logicielles sur l'ensemble de l'intranet, seuls les postes de travail appartenant à l'IFREMER, à des Unités Mixtes ou à des établissements en convention avec l'IFREMER, sont raccordables aux réseaux IFREMER.

De ce fait, afin d'éviter le raccordement de matériel personnel, il apppartient au laboratoire ou service d'accueil de prévoir la mise à disposition d'un matériel informatique lors de l'accueil de tout personnel temporaire (CDD, thésard, stagiaire…)

Il peut être admis, par dérogation, le raccordement ponctuel d'ordinateurs de professionnels partenaires ou prestataires, sous la responsabilité du responsable IFREMER de l'accueil et qui se sera assuré au préalable de la salubrité de la machine (antivirus à jour notamment).

5. Intégrité des systèmes et des informations.

5.1. L'utilisation ou le développement de programmes mettant sciemment en cause l'intégrité des systèmes est interdit.

L'Utilisateur ne doit pas faire preuve de malveillance et modifier ou détruire des fichiers ou des programmes informatiques qui ne sont pas strictement réservés à son seul usage.
Ces règles s'appliquent même si les fichiers ne sont pas protégés et sont sanctionnées par l'article 323-1 à 323-7 du Code Pénal.

5.2. La copie de fichiers internes n'est autorisée que dans le cadre de la mission professionnelle de l'Utilisateur et après réception de l'accord du ou des créateurs du fichier ou du chef de programme supervisant la création dudit fichier.

Lorsqu'un fichier ou une base de données partagée est mis à jour par de multiples utilisateurs ou lorsqu'un développement de programmes informatiques est effectué par plusieurs utilisateurs, l'ensemble de ces utilisateurs sera considéré comme leur créateur.

Tout agent ayant procédé, dans le cadre de ses fonctions à l'IFREMER, à la création d'un fichier, d'une base de données ou de programmes informatiques, devra obligatoirement les transmettre à son service ou laboratoire de rattachement ainsi que les codes sources et la documentation correspondants avant son départ, ou avant l'éxécution d'une mobilité interne. Il ne devra pas non plus en garder de copie, si cela peut porter préjudice à l'Ifremer.

5.3. L'Utilisateur ne dispose d'aucune autorisation pour cacher son identité ou crypter ses données, hormis et seulement avec un accord préalable de son responsable, et uniquement pour des raisons de confidentialité propres à l'IFREMER.

5.4. Le développement et l'utilisation de programmes ou de commandes visant à deviner des mots de passe, à usurper l'identité d'une tierce personne existante ou fictive, ou à créer un compte, pour accéder à des services autres que ceux auxquels il aurait eu un accès autorisé, sans l'accord d'un Administrateur Système ou de la Direction Informatique sont interdits et sanctionnés par l'article 323-1 à 323-7 du Code Pénal.

5.5. Les Utilisateurs sont tenus de respecter les recommandations de la Direction Informatique et des Administrateurs Système relatives à la sécurité des moyens informatiques de l'IFREMER.

Ainsi sont prohibés:

- toute mise en danger de l'infrastructure des Systèmes d'Information par le biais d'introduction volontaire de virus informatique ou du non respect des règles et procédures informatiques usuelles ;
- tout piratage informatique, téléchargement ou utilisation de logiciels et de contenus non autorisés;
- toute utilisation de solutions alternatives « grand public » en lien avec les outils de communication sans validation préalable de la Direction Informatique de l'IFREMER.
- Toute consultation, téléchargement, stockage, copie, transmission, publication, diffusion ou distribution de données et/ou de correspondances entrant dans le champ énoncé à l'article 3.1.
- d'accéder à tous sites Internet susceptibles de présenter un danger pour la sécurité des Outils Informatiques et Systèmes d'Information.

5.6. L'Utilisateur doit strictement respecter les droits d'accès et les procédures d'accès aux différents réseaux de partage de données de l'IFREMER.

5.7. L'Utilisateur doit régulièrement enregistrer, dans les répertoires du Réseau dédié à l'activité concernée, les contenus professionnels créés sur le disque dur de son matériel et /ou sur le réseau.

5.8. Les Utilisateurs ne doivent pas perturber le fonctionnement normal des outils de communication et doivent signaler à la Direction Informatique : assistance@ifremer.fr , dans les meilleurs délais, toute anomalie de sécurité constatée.

6. Confidentialité et organisation du contrôle.

6.1. Les Utilisateurs ne doivent pas tenter de lire ou de divulguer des informations contenues dans les fichiers d'un autre Utilisateur sans y avoir été autorisés. Cette règle s'applique même si les fichiers ne sont pas protégés ou s'ils sont mis en commun sur le réseau.

6.2. L'Utilisateur est responsable de la protection de ses fichiers, ainsi que de l'intégrité des outils mis à sa disposition. A cet effet, il doit s'assurer de la fermeture de sa session en cas d'absence temporaire de son bureau.

6.3. Il est interdit d'essayer d'intercepter toute communication entre tiers.

6.4. En cas d'urgence et, si besoin en est pour l'intérêt de l'Ifremer, après avoir tenté de contacter l'Utilisateur IFREMER sans succès par tout moyen, son responsable hiérarchique pourra avoir accès à sa messagerie et ses fichiers professionnels après consultation et accord du DRH de l'IFREMER, si cela apparaît indispensable pour assurer la continuité de l'activité, en se rapprochant de la Direction Informatique. Ce droit d'accès sera limité aux seuls messages identifiés comme pouvant répondre aux conditions d'urgence et de besoins d'informations décrits ci dessus.
Les messages ou fichiers comportant en objet la mention « Personnel » sont exclus de ce droit d'accès par la hiérarchie. Ce droit d'accès ne se confond pas avec les investigations et contrôles prévus à l'article 6.5.

6.5. Les équipes de la Direction Informatique peuvent être amenées, sur demande de la Direction générale, à établir et/ou restituer des traces et bilan de l'activité réseau et informatique d'un Utilisateur dans les conditions suivantes :

- En cas d’indices concordants d’une utilisation abusive, par un Utilisateur, des Outils Informatiques et/ ou des Systèmes d’Information mis à sa disposition, ou en cas de non respect avéré de la présente Charte (telle une atteinte à la sécurité et au bon fonctionnement des Outils Informatiques et/ ou Systèmes d’Information). La Direction générale, le Directeur de rattachement et le Directeur des Ressources Humaines seront informés des circonstances et valideront au préalable le principe de ces investigations.
- En cas d’anomalie fonctionnelle, constatée ou à craindre, sur les architectures informatiques, les équipes techniques peuvent être amenées à diagnostiquer et localiser des causes de troubles. Elles en informeront les Utilisateurs concernés ainsi que leurs correspondants informatiques locaux, voire leur responsable selon le contexte.

Ces investigations et contrôles porteront sur les relevés de la navigation WEB, le trafic généré sur le réseau, les contenus professionnels de la messagerie et les fichiers de l’Utilisateur, étant rappelé que les contenus sont réputés professionnels, à moins qu’ils répondent aux conditions énoncées au point 3.4.

Toutefois, il est expressément interdit de qualifier de « Personnel » un contenu à caractère professionnel.

En cas d’un risque grave pour l’IFREMER du fait de la présence d’indices concordants d’une atteinte grave à la sécurité ou d’une violation manifeste et excessivement abusive de la présente Charte, la prise de connaissance de contenu de fichiers de l’Utilisateur identifiés comme étant « Personnel » par la Direction générale ou la Direction des Ressources humaines devra être effectuée en présence de l’intéressé.

6.6. Dans le cadre d’une enquête judiciaire, nécessitant des informations sur l’activité informatique d'un ou plusieurs utilisateurs, l’IFREMER collaborera avec la police.

6.7 Filtrage: La direction générale pourra, en cas de besoins, procéder à la mise en place d'un filtrage partiel ou total de la navigation internet.

7. Relations avec les autres sites.

7.1. En dehors de la navigation Web ou ftp sur les sites publics de l'internet, il est interdit de se connecter ou d'essayer de se connecter sur d’autres sites que les sites IFREMER sans y être autorisé par les responsables informatiques de ce site.

7.2. Il est interdit de se livrer depuis des systèmes de l'IFREMER à des actions ne respectant pas les règles de fonctionnement ou mettant en cause la sécurité du site distant.

8. Propriété intellectuelle.

8.1. Logiciels

8.1.1. L'utilisation de logiciels doit se faire dans le respect de la propriété intellectuelle et des engagements pris par l'IFREMER, notamment dans le cadre des contrats de licence relatifs à ces logiciels.

8.1.2. Sous réserve des dérogations prévues dans le contrat de licence et des exceptions légales prévues par le code la propriété intellectuelle:

- la reproduction de logiciel, autre qu'une copie de sauvegarde, est interdite, y compris pour les agents y ayant contribué;
- l'installation d'un logiciel sur une machine de l'IFREMER ne peut se faire sans s'être assurée de la régularité de l'opération: la licence d'exploitation d'un logiciel est concédée pour une machine déterminée ou pour un nombre limité de machines;
- la modification d'un logiciel appartenant à un tiers ne peut être effectuée qu'avec l'autorisation préalable écrite de ce tiers dans le cadre de la licence concédée à l'IFREMER.
- Les Utilisateurs ne doivent pas consulter, reproduire, télécharger, mettre à disposition, diffuser ou communiquer au public, notamment via les réseaux Internet et Intranet, des logiciels et/ou des document protégés par un droit d'auteur ou un droit voisin, sans l'autorisation des titulaires de ce droit.

Le non-respect de ces obligations peut être constitutif d'une intention de nuire de la part de l'Utilisateur à l'égard de l'IFREMER.

Le non respect de ces dispositions peut constituer une contrefaçon sanctionnée civilement et pénalement.

8.2. Diffusion d'informations

La diffusion électronique d'informations, programmes, données, images, en particulier par le serveur ftp anonyme et le serveur WWW, est limitée aux informations validées pour lesquelles l'IFREMER possède les droits de reproduction et de diffusion.

L'Utilisateur et le Rédacteur sont responsables du respect des obligations relatives :

- aux informations nominatives (réglementation Informatiques et Libertés) ;
- aux contrats comportant des clauses de confidentialité ;
- aux droits d'auteur sur les textes, images, sons, vidéos appartenant à des tiers ;
- aux droits à l'image des personnes figurant sur lesdites images.

9. Informatique et liberté.

9.1. Toute personne physique identifiée au titre de la présente Charte dispose d'un droit d'accès et de modification de ses informations personnelles auprès des services des ressources humaines de l'IFREMER. Les informations sont conservées sur support informatique jusqu'à la déchéance des droits d'accès de l'Utilisateur aux Outils Informatiques et/ ou Système d'Information.

9.2. La création de tout fichier contenant des informations nominatives doit faire l'objet de formalités préalables à sa constitution et à la réalisation du traitement envisagé, auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). L'Instruction PDG 2004-006 du 16 décembre 2004, relative aux Conditions de création de traitements de données à caractère personnel, confie à la Direction des Affaires Juridiques, toute demande de création de traitement de données personnelles.

9.3. L'autorisation délivrée par la CNIL n'est valable que pour le traitement déclaré et non pas pour le fichier lui même. Toute nouvelle utilisation du fichier doit donner lieu à une nouvelle déclaration à la CNIL.

10. Vigilance de la part de l'Utilisateur.

10.1. Tout constat de violation, tentative de violation ou soupçon de violation du Système d'Information doit être signalé à la Direction Informatique afin de préserver l'intégrité des moyens et des informations.

10.2. La Direction Informatique est tenue d'établir un rapport pour la Direction Générale sur tous les incidents de sécurité informatique, notamment ceux relevant de comportements non conformes à cette charte.

11. Rôle des Administrateurs Système.

Les Administrateurs Système sont désignés par le Directeur dont ils dépendent.

11.1. Les Administrateurs Système utilisent leurs privilèges système afin d'assurer le fonctionnement des moyens informatiques et assurer la qualité de service.

11.2. Les Administrateurs Système des laboratoires et services sont soumis aux règles de configuration des machines relatives à la sécurité, définies par la Direction Informatique.

11.3. Les Administrateurs Système veillent sur l'utilisation, la diffusion et la protection des mots de passe système.

11.4. Les Administrateurs Système se doivent de respecter la plus stricte confidentialité des informations des Utilisateurs qu'ils peuvent être amenés à connaître.

11.5. Les Administrateurs Système veillent au respect des droits et des devoirs des Utilisateurs dans la limite de leurs aptitudes techniques.

En cas de difficulté, ils en informent la Direction Informatique qui, en cas de besoin, rend compte des dysfonctionnements à la Direction Générale.

12. Départ ou décès d'un Utilisateur.

En cas de décès ou de départ d'un Utilisateur, ses fichiers professionnels seront librement accessibles à son employeur. Ces données seront mises à disposition d'un autre agent, selon les directives du responsable d'équipe concerné. Sa messagerie professionnelle pourra être stockée et utilisée uniquement aux conditions décrites au paragraphe 6.4. Si ces conditions ne sont pas réunies, les données de messagerie seront supprimées.

Lorsque l'Utilisateur n'a, dans les 2 mois civils suivant son départ, fait part d'aucune consigne particulière ou manifesté sa volonté de les récupérer, les dossiers de messagerie et données identifiés comme relevant de sa vie personnelle sont par défaut supprimés.

Annexe 1. Extensions d'utilisations autorisées des moyens informatiques de l'IFREMER

1. Activité syndicale

Les conditions d'utilisation par les organisations syndicales des moyens informatiques de l'IFREMER pour l'exercice de leurs activités sont à définir dans un avenant à l'accord portant sur le fonctionnement du dialogue social et de la représentation du personnel dans le cadre de l'Unité Economique et Sociale entre l'Ifremer et le GIE Genavir du 21 octobre 2009.

2. Comité d'entreprise et Comités d'établissement

Le Comité d'entreprise et les Comités d'établissement sont autorisés à constituer des pages dans la partie privée du serveur Web de l'IFREMER et à utiliser la messagerie et les listes de diffusion dynamiques. Les informations contenues dans ces pages ou données via la messagerie ne peuvent concerner que des activités entrant dans le domaine de compétence desdits comités.

3. Associations sportives et culturelles de l'IFREMER

Les associations sportives et culturelles de l'IFREMER sont autorisées à constituer des pages dans la partie privée du serveur Web de l'IFREMER et à utiliser la messagerie et les listes de diffusion dynamiques. Les informations contenues dans ces pages ou données via la messagerie ne peuvent concerner que des activités entrant dans le domaine de compétence des associations sportives et culturelles de l'IFREMER.

Annexe 2 Extraits des articles de loi cités dans la Charte

Code du travail

Article L1321-4

Le règlement intérieur ne peut être introduit qu'après avoir été soumis à l'avis du comité d'entreprise ou, à défaut, des délégués du personnel ainsi que, pour les matières relevant de sa compétence, à l'avis du comité d'hygiène, de sécurité et des conditions de travail.

Le règlement intérieur indique la date de son entrée en vigueur. Cette date doit être postérieure d'un mois à l'accomplissement des formalités de dépôt et de publicité.

En même temps qu'il fait l'objet des mesures de publicité, le règlement intérieur, accompagné de l'avis du comité d'entreprise ou, à défaut, des délégués du personnel et, le cas échéant, du comité d'hygiène, de sécurité et des conditions de travail, est communiqué à l'inspecteur du travail.

Ces dispositions s'appliquent également en cas de modification ou de retrait des clauses du règlement intérieur.

(p 1 de la Charte)

Article L1332-2

Lorsque l'employeur envisage de prendre une sanction, il convoque le salarié en lui précisant l'objet de la convocation, sauf si la sanction envisagée est un avertissement ou une sanction de même nature n'ayant pas d'incidence, immédiate ou non, sur la présence dans l'entreprise, la fonction, la carrière ou la rémunération du salarié.

Lors de son audition, le salarié peut se faire assister par une personne de son choix appartenant au personnel de l'entreprise.

Au cours de l'entretien, l'employeur indique le motif de la sanction envisagée et recueille les explications du salarié.

La sanction ne peut intervenir moins de deux jours ouvrables, ni plus d'un mois après le jour fixé pour l'entretien. Elle est motivée et notifiée à l'intéressé.

(p 7 de la Charte)

Code Pénal

Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende.

Article 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

Article 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende.

Article 323-3-1

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

(p 8 de la Charte)