La charte informatique du Cirad

CIRAD

La charte informatique du Cirad

Conformément à la loi, un exemplaire du livre II de la présente charte informatique (additif aux règlements intérieurs des sites du Cirad), auquel est jointe la charte dans sa version intégrale, est déposé au secrétariat-greffe du conseil de prud'hommes de chacun des sites d'implantation du Cirad en France (Paris, Montpellier, Guadeloupe, Guyane, Martinique et Réunion).

L'entrée en vigueur du livre II de la charte informatique du Cirad est fixée au 1er janvier 2008.

Toute modification du livre II de la charte informatique du Cirad sera soumise à la même procédure, étant entendu que toute clause qui deviendrait contraire aux dispositions légales ou conventionnelles applicables au Cirad du fait de l'évolution de ces dernières serait nulle de plein droit.

Sommaire

Préambule : objet et champ d'application

▶ Pourquoi une charte informatique ?

Le fonctionnement du Cirad passe par l'utilisation de systèmes d'information et de moyens de communication modernes de plus en plus performants, qui s'appuient sur des réseaux connectés à l'échelle mondiale. Ces réseaux, qui apportent une capacité de travail et une souplesse inégalées, présentent également une grande vulnérabilité, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que celle du Cirad, qui met ces moyens à leur disposition en tant qu'outil de travail.

L'utilisation des nouvelles technologies de communication pose le double problème de la protection de l'information sensible gérée par les utilisateurs et des systèmes d'information placés sous la responsabilité du Cirad.

Les mesures mises en œuvre pour répondre à cette double nécessité doivent permettre au Cirad de remplir ses missions et de satisfaire en même temps aux exigences imposées :

– par ses engagements vis-à-vis de ses partenaires ;

– par le respect de la réglementation sur la protection des données sensibles et la protection du patrimoine scientifique ;

– par le respect des dispositions légales en matières civile et pénale ;

– par le respect de la loi sur la protection des données personnelles.

L'élaboration de règles déontologiques et un contrôle de l'utilisation de ces ressources informatiques sont donc indispensables, de même qu'une information et une sensibilisation des personnels.

C'est pour atteindre ces différents objectifs que le Cirad a décidé de se doter d'une charte informatique et a mis en place des dispositifs et moyens pour assurer la sécurité et le contrôle de l'utilisation des ressources télématiques et informatiques. En même temps, il a fixé les conditions d'utilisation de ces moyens afin de garantir les droits individuels de chaque utilisateur.

▶ Objet et champ d'application de la charte informatique

La présente charte a pour objet de définir les conditions d'utilisation et les règles de bon usage des ressources informatiques du Cirad.

S'entendent par « ressources informatiques » : la messagerie électronique, l'accès à Internet/Intranet, la connexion de terminaux à distance, le transfert, la consultation, la mise à disposition de fichiers et/ou de logiciels quels qu'ils soient, la participation à des forums, la consultation de bases de données multimédias et ce, au moyen de l'ensemble des composants matériels, réseaux, logiciels, serveurs, postes informatiques et périphériques mis à la disposition des utilisateurs par le Cirad, y compris l'informatique nomade, tels qu'assistants personnels, scanners, ordinateurs portables, appareils photos numériques et tout autre périphérique informatique.

La présente charte est applicable à l'ensemble des agents et des personnes autorisées à utiliser les ressources informatiques du Cirad, appelés utilisateurs.

S'entendent par « utilisateurs » : les salariés, ainsi que toutes les personnes non salariées du Cirad quel que soit leur statut, y compris les intérimaires, les stagiaires, les différents partenaires, prestataires et sous-traitants du Cirad ayant accès au système informatique en quelque lieu que ce soit.

La charte précise les droits, obligations et responsabilités des utilisateurs, dans le respect de la législation en vigueur, afin de promouvoir un usage correct des ressources informatiques, tenant compte des règles minimales de courtoisie et de respect d'autrui et sous réserve des droits des institutions représentatives du personnel et des organisations syndicales.

Chaque utilisateur doit prendre connaissance et appliquer les dispositions de la présente charte, et plus particulièrement son livre II, qui constitue un additif au règlement intérieur.

Le non-respect de la charte par un utilisateur peut conduire la direction du Cirad à lui interdire l'accès à ses ressources informatiques.

Par ailleurs, tout manquement aux règles obligatoires édictées au livre II de la charte informatique du Cirad peut donner lieu à des sanctions disciplinaires.

En cas de non-respect de la réglementation, la responsabilité civile ou pénale de l'utilisateur peut être engagée.

▶ Pour vous aider à bien appliquer la charte

Pour obtenir des informations complémentaires et des précisions sur les recommandations de la charte et les procédures visées (sauvegardes, par exemple), les utilisateurs peuvent se référer au site Intranet de la DSI (Délégation aux systèmes d'information). Pour plus de précisions, ils peuvent s'adresser à l'assistance informatique ou, selon les cas, aux services informatiques. De même, pour signaler des problèmes de sécurité.

Par ailleurs, une adresse de messagerie, **SVP-info@cirad.fr**, est à la disposition de chacun pour saisir la DSI d'une difficulté particulière d'application de la charte.

La DSI organisera des formations adaptées.

L'élaboration de la charte

La charte informatique du Cirad a été élaborée par la direction, avec l'appui d'un groupe de travail composé de représentants des organisations syndicales et du comité d'entreprise.

Elle a été présentée et soumise à l'avis des commissions de site et des CHSCT (Comités d'hygiène, de sécurité et des conditions de travail) ainsi qu'au comité d'entreprise (avis du 27 juin 2007).

La présente charte est publiée sur le site Intranet du Cirad.

L'évolution de la charte

Afin de tenir compte du contexte juridique et technologique en rapide évolution en matière de technologies de l'information, la charte sera réactualisée régulièrement et les utilisateurs en seront informés.

Livre I. Les principes généraux

▶ Le contexte juridique : un éventail de dispositions légales très diverses

Les règles précisées dans la présente charte découlent en grande partie des textes de référence suivants :

– le code pénal ;

– le code du travail ;

– le code civil ;

– le code de la propriété intellectuelle ;

– les lois relatives « à l'informatique, aux fichiers et aux libertés » ;

– la charte déontologique du Gip Rénater dont le Cirad est signataire ;

– les règlements intérieurs applicables sur les sites du Cirad.

Ces textes concernent en particulier :

– la disponibilité et l'intégrité des ressources informatiques ;

– la confidentialité des informations ;

– la falsification et la fraude informatiques ;

– l'illicéité des contenus (propagation d'idées racistes, xénophobes…) ;

– les infractions liées à la propriété intellectuelle et aux droits connexes (copies illégales d'œuvres protégées…).

En outre, en sa qualité d'établissement public de recherche à caractère industriel et commercial, exerçant ses activités dans un cadre international et du fait de son appartenance au réseau Rénater, par la charte duquel il est impliqué, le Cirad pourrait voir sa responsabilité engagée de manière particulière, au titre de manquements commis par les utilisateurs.

Ces règles ne sont pas exclusives de celles qui s'imposent par ailleurs à tout agent du Cirad en ce qui concerne l'obligation de discrétion et de secret professionnel.

▶ Une préoccupation particulière : garantir les utilisateurs contre les risques d'atteintes aux libertés individuelles

Le Cirad souhaite protéger les utilisateurs des ressources informatiques de l'établissement contre les risques d'atteintes aux libertés individuelles. Celles-ci peuvent se produire du fait des multiples procédures de collecte d'informations liées aux activités et à leur gestion et en raison de l'existence de traitements automatisés des données personnelles qui peuvent y être liés.

Conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par de multiples textes, en particulier par la loi n° 2004-801 du 6 août 2004, le Cirad s'efforce de respecter toutes dispositions y afférentes et à cet effet **se dote d'un correspondant à la protection des données personnelles**.

Le correspondant à la protection des données personnelles a notamment en charge de dresser la liste des traitements automatisés mis en œuvre. Il doit assurer de manière indépendante, le respect des obligations prévues par la loi Informatique et libertés.

D'autres missions peuvent, de convention expresse, lui être confiées, parmi lesquelles figurent l'élaboration des dossiers de formalités auprès de la Cnil (Commission nationale de l'informatique et des libertés), pour les traitements non exonérés, l'élaboration d'une politique de données à caractère personnel ou la sensibilisation des personnels aux dispositions de la loi.

Chaque utilisateur est informé qu'il dispose, dans ce cadre, d'un droit personnel d'accès, de rectification, de complément, de mise à jour et de verrouillage sur l'ensemble des données le concernant qui seraient, selon les cas, inexactes, incomplètes, équivoques, périmées ; il dispose également d'un droit d'opposition, en cas de motif légitime, au traitement de données à caractère personnel le concernant et faisant l'objet d'un tel traitement automatisé.

A cet égard, les utilisateurs sont informés que, afin de prévenir tout risque de mise en cause accidentelle ou fortuite de leurs droits, les services responsables de la sécurité informatique du Cirad exercent, pour la protection de ces droits, une vigilance particulière. De ce point de vue, ils veillent notamment :

– à l'information et à la consultation des instances représentatives du personnel ;

– à l'information préalable des utilisateurs ;

– au respect du principe de proportionnalité : en ce sens, ne peuvent pas être apportées aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas proportionnées au but recherché ;

– au respect du principe de protection de la vie privée de l'utilisateur sur son lieu de travail.

La sécurisation des ressources informatiques : fonctionnement et procédures

Le traçage

Chaque utilisateur est informé que l'ensemble des opérations informatiques et électroniques laisse des traces (source, horaire, destination, durée, sites visités…), qui sont enregistrées automatiquement par la DSI et sous sa responsabilité.

Ces traces permettent de veiller au bon fonctionnement des ressources informatiques et de savoir, le cas échéant, à qui imputer la responsabilité des opérations effectuées.

L'objectif du traçage est essentiellement d'assurer la sécurité et l'optimisation des systèmes d'information, et non de réaliser un contrôle individuel de l'activité des utilisateurs (sauf cas particulier, cf. notamment les « Modalités de contrôle », ci-dessous).

La conservation

Sous réserve des situations de litige ou de contentieux, les traces d'utilisation des ressources informatiques par les utilisateurs sont enregistrées et conservées, en principe, au maximum pendant un an.

Les seules informations qui peuvent être conservées au-delà d'une année concernent les volumes de ressources utilisées. Dans ce cas, elles sont préalablement rendues anonymes.

La sécurité

La sécurité des espaces de stockages : utilisation d'antivirus

Les ressources informatiques doivent être contrôlées par des antivirus.

Des processus automatiques analysent les ressources informatiques, y compris les espaces personnels, pour détecter la présence de programmes malveillants, notamment la présence de virus informatiques, susceptibles de compromettre la sécurité de ces ressources ou celle de ressources externes à l'équipement. Le rôle de ces processus automatiques est de permettre aux administrateurs de mettre ces programmes malveillants hors d'état de nuire.

Les utilisateurs sont informés que, par l'intermédiaire de l'antivirus, l'administrateur du système informatique peut avoir accès au nom des répertoires et des fichiers contenus dans les disques durs.

Sécurité et dispositifs de filtrage des communications informatiques

Afin de renforcer la sécurité de ses ressources informatiques, le Cirad se réserve le droit de mettre en place des dispositifs de filtrage des communications informatiques. Ces dispositifs de filtrage ont pour effet de neutraliser, par exemple, les applications (ou logiciels) non autorisées, la réception de messages électroniques non sollicités (spam) ou contenant des virus et des sites Web dont il n'autorise pas l'accès.

Toute mise en place de dispositifs de filtrage sera communiquée aux utilisateurs.

Dispositifs de filtrage des messages électroniques. Des dispositifs de filtrage des messages électroniques, dont le but est de neutraliser la réception ou l'envoi de messages, notamment de ceux contenant des virus, ainsi que la réception de messages non sollicités (spam), ont été mis en place. Ces dispositifs fonctionnent selon des règles fixées par les administrateurs de ressources informatiques. Ils sont entièrement automatisés et garantissent qu'aucune personne ne peut avoir connaissance du contenu des messages.

Les logiciels antivirus de messagerie mis en place par le Cirad bloquent l'envoi ou la réception de fichiers dits « exécutables » : logiciels, programmes, scripts... (fichiers dont l'extension est : .pif, .bat, .exe, .com, .cmd, .scr). Cette liste sera adaptée en fonction des circonstances.

Les utilisateurs sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de l'administrateur réseaux, qui en informe l'émetteur ou le destinataire.

Dispositifs de filtrage de certaines applications. Le Cirad peut interdire l'usage de certaine applications (ou logiciels) par la mise en place de filtres. Les dispositifs et les règles de filtrage seront établis par la DSI en fonction de ses propres besoins et de ceux exprimés par les utilisateurs et en tenant compte notamment des avis des équipes de sécurité du Gip Rénater, de la Direction centrale de la sécurité des systèmes d'information (ou du Certa, Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques) ou de nos tutelles.

Dispositifs de filtrage de sites Web. Le Cirad peut également mettre en place un dispositif de filtrage de sites Web dont il n'autorise pas l'accès, notamment les sites comportant des éléments à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, pornographique, pédophile ou susceptible de porter atteinte au respect et à la dignité de la personne humaine.

Livre II. Les obligations à respecter par tout utilisateur
(additif aux règlements intérieurs des sites du Cirad)

Ce livre II de la charte informatique constitue un additif aux règlements intérieurs actuellement en vigueur au Cirad et, à ce titre, relève de la procédure spécifique d'élaboration, de consultation et de respect des formalités de dépôt et d'affichage applicable à tout document portant prescriptions générales et permanentes en matière d'hygiène de sécurité et de discipline dans l'entreprise.

Il est rappelé aux utilisateurs que les manquements aux règles obligatoires précisées au présent livre II de la charte informatique du Cirad peuvent donner lieu à l'application de sanctions disciplinaires.

Les dispositions contenues dans la charte sont appliquées dans le respect des droits des instances représentatives du personnel et des organisations syndicales.

L'utilisation professionnelle des ressources informatiques

L'utilisateur s'engage à n'utiliser les ressources informatiques que le Cirad met à sa disposition qu'à seule fin professionnelle.

Les activités professionnelles sont les activités de recherche, d'enseignement, de développement technique, de transfert de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, ainsi que toute activité administrative, de gestion ou d'appui à la recherche découlant ou accompagnant ces activités.

Toutefois, comme le prévoient les règlements intérieurs du Cirad, une utilisation personnelle est autorisée dans les cas d'urgence et de nécessité. En outre, elle est tolérée sous réserve de ne pas nuire au temps consacré au travail ni à la qualité de celui-ci, de ne pas entraver le bon fonctionnement du service ni des ressources informatiques et en respectant la législation civile et pénale en vigueur. L'outil et les ressources informatiques ne peuvent être utilisés à des fins de propagande politique ou religieuse.

Toute information ou donnée, tout fichier, répertoire ou dossier, ainsi que tout message est considéré comme professionnel s'il n'est pas expressément « identifié » comme personnel ou privé.

Pour être considérés comme personnels ou privés, les fichiers, les informations, les données et les messages gérés par les utilisateurs doivent être placés dans un répertoire ou un dossier intitulé « personnel ou privé ». Les courriers envoyés doivent porter la même mention dans leur objet ; les courriers personnels reçus doivent immédiatement après réception et lecture être classés dans un dossier spécifique portant la mention « personnel ».

Dès lors qu'ils remplissent cette condition, les données, informations, dossiers, répertoires et fichiers « personnels » sont soumis aux dispositions spécifiques relatives au respect de la vie privée, et les messages, aux dispositions relatives au secret des correspondances privées.

Dans le cadre privé, les utilisateurs s'obligent également à respecter la réglementation et la charte informatique, y compris son livre II.

En tout état de cause, ils s'interdisent l'envoi de message en chaîne ou en masse, ainsi que la participation à des forums non professionnels.

Les règles obligatoires de sécurité et de bon usage

Les conditions d'accès aux ressources informatiques

L'utilisation des ressources informatiques du Cirad, notamment l'ouverture d'un compte ou la connexion d'un équipement sur le réseau du Cirad, est soumise à autorisation.

Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée, sauf cas particulier, ainsi qu'en cas de manquements graves ou répétés à la présente charte.

L'utilisation d'équipements informatiques mobiles raccordés au réseau doit faire l'objet d'une validation préalable par la DSI, qui vérifie la conformité de l'équipement aux réseaux du Cirad ainsi que sa protection contre les virus et les intrusions.

Les obligations à respecter par tout utilisateur

Tout utilisateur des ressources informatiques du Cirad doit assurer la protection de ses données ; il est responsable des droits d'accès qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde, individuels ou collectifs, mis à sa disposition.

Il doit choisir des mots de passe sûrs, en respectant les règles fixées par les administrateurs (cf. livre III). Il doit les garder secrets et ne pas les communiquer à des tiers. Toutefois, en cas d'absence, l'utilisateur pourra — à la demande de son responsable hiérarchique et si l'accès à un fichier, dossier, message… professionnel est indispensable au bon fonctionnement du service — être tenu de communiquer son mot de passe audit responsable hiérarchique ou à un collègue. Il appartiendra à l'agent de modifier son mot de passe à son retour.

Tout accès en l'absence de l'utilisateur sera réalisé dans le respect de sa vie privée et du secret des correspondances privées.

Lorsqu'il quitte un poste de travail, il doit verrouiller ou fermer les sessions ouvertes afin de ne pas laisser des ressources ou des services disponibles sans identification.

Il doit se conformer aux obligations de discrétion professionnelle et respecter l'ensemble des lois pénales ou civiles en vigueur, relatives notamment :

– aux publications à caractère raciste, pédophile, injurieux, diffamatoire ;

– au harcèlement sexuel ou moral, à la discrimination ;

– aux dispositions en matière de propriété intellectuelle, notamment l'utilisation des logiciels (licences) et les droits d'auteur.

Il doit appliquer les consignes de sécurité définies par le Cirad et, pour toute installation de logiciel, suivre les règles en vigueur au Cirad, qu'il pourra consulter sur le site de la DSI.

Les interdictions à respecter par tout utilisateur

Il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.

Il ne doit pas tenter de lire, modifier, déposer ou détruire des données sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.

Il ne doit pas tenter de lire, modifier, déposer ou détruire des données détenues par d'autres utilisateurs, même si ces données ne sont pas explicitement protégées, sauf autorisation expresse des intéressés.

Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.

Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.

Il ne doit pas connecter un matériel sur le réseau sans autorisation préalable. Cette interdiction concerne, en priorité, les visiteurs et les partenaires.

Il ne doit pas mettre à la disposition de personnes non autorisées un accès aux ressources informatiques du Cirad.

Il ne doit pas, par quelque moyen que ce soit, proposer ou rendre accessible aux tiers des informations confidentielles ou contraires à la législation en vigueur.

Il ne doit pas télécharger ou diffuser des données en violation des lois protégeant les droits d'auteur, quel que soit le domaine (écrits, images, logiciels, bases de données…).

Il ne doit pas contourner les restrictions d'utilisation d'un logiciel.

Il ne doit pas utiliser les listes de diffusion institutionnelles hors du cadre strictement professionnel, sauf autorisation de la direction.

Responsabilité générale

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques mises à sa disposition et s'engage à ne pas effectuer volontairement des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement de ces ressources, sur l'intégrité des systèmes d'information et sur les relations internes et externes du Cirad.

Chaque utilisateur a la charge, à son niveau, de contribuer à la sécurité générale des systèmes d'information et à celle du Cirad. Il s'interdit notamment toute manipulation anormale et tout introduction de ressources non autorisées et s'engage à respecter les procédures de sécurité communiquées par la DSI et, particulièrement, les procédures d'authentification.

L'utilisation des ressources informatiques doit être rationnelle et conforme à l'intérêt du service, contribuant ainsi à éviter sa saturation ou son détournement.

Toute anomalie constatée, susceptible d'affecter la sécurité des ressources informatiques, doit être signalée à l'équipe informatique du Cirad.

Le Cirad ne pourra être tenu pour responsable des détériorations d'informations ou des manquements commis par un utilisateur qui ne se sera pas conformé à ces règles. Tout manquement à ces stipulations engage la responsabilité personnelle de l'utilisateur.

La protection des mineurs

Dans le cadre de ses activités, le Cirad est susceptible d'accueillir des mineurs (stagiaires de l'enseignement secondaire notamment) dans ses locaux. Il incombe aux utilisateurs accueillant ces mineurs de les protéger en les préparant, en les conseillant, en les assistant, notamment dans leur utilisation d'Internet et des réseaux numériques ainsi que de leur communiquer la charte en vigueur.

L'ensemble des activités liées aux technologies de l'information et de la communication, effectuées dans l'enceinte du Cirad et mettant en œuvre les services proposés, doit être précédé d'explications ou d'instructions très précises données aux mineurs. Celles-ci doivent notamment porter sur les conditions visées dans cette charte et, le cas échéant, insister sur des consignes spécifiques de sécurité.

Les utilisateurs doivent garder à tout moment, la maîtrise des activités liées à l'utilisation des services proposés par le Cirad, notamment en exerçant une surveillance suivie des activités des mineurs, de manière à pouvoir intervenir rapidement en cas de problème, à repérer et à faire cesser tout comportement pouvant devenir dangereux.

Les modalités de contrôle

Afin de garantir le respect de la présente charte et le bon fonctionnement des ressources informatiques, le Cirad pourra être amené à contrôler l'utilisation des ressources informatiques par les utilisateurs. Ces contrôles se feront dans le respect des lois et règlements en vigueur et notamment du principe du respect de la vie privée de chacun.

Dans ce cadre, la direction a la faculté de mettre en place et d'utiliser, notamment, les dispositifs suivants :

– dispositif de contrôle et d'analyse, par utilisateur, du nombre, de la taille et de la fréquence des messages échangés sur Internet ;

– dispositif d'enregistrement et d'analyse des traces des connexions (par exemple, serveurs Web ou bases de données visités depuis un micro-ordinateur) ;

– dispositif de mesure de la taille des répertoires.

Ces dispositifs peuvent être utilisés pour la détection des abus ou des atteintes à la sécurité ou à la législation. Sauf dans les situations de litige ou de contentieux, les informations recueillies dans le cadre de ces dispositifs sont conservées pendant 12 mois.

Nettiquette

Les recommandations insérées au présent article ne constituent pas des prescriptions ; elles s'appuient sur des considérations d'ordre éthique ou de courtoisie et sont destinées à assurer une utilisation collective des ressources informatiques, sur un mode convivial et selon des principes partagés.

Une expression mesurée : le net ou Internet ne doit pas constituer un espace d'expression débridée et d'actions illicites (cf. livre II de la présente charte).

Eviter les messages en masse ou chaîne : afin d'éviter la saturation du réseau, les envois de messages en masse (plus de 20 destinataires) sont déconseillés, hors diffusion sur les listes institutionnelles du Cirad pour raison de service. Il en va de même pour les messages « en chaîne » (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement).

Messages et courtoisie : soin et courtoisie doivent présider à la rédaction et aux échanges des messages. De même, le contenu des messages envoyés ne doit pas nuire au Cirad ni à son image. Dans le même esprit, il incombe à chacun d'éviter un usage abusif des fonctions « copie cachée » et « faire suivre ». De même, il est préférable d'expédier des messages courts. L'envoi de messages écrits intégralement en majuscules est déconseillé.

Forums professionnels de discussion : les mêmes règles de bon usage sont transposables aux forums. En outre, le sens de la responsabilité de chacun doit conduire à ne pas y participer de façon anonyme et à respecter le sujet du forum ou du groupe de discussion.

Internet et prévention des risques : l'utilisation du réseau Internet est génératrice de risques potentiels. En ce domaine, les garanties proposées ont toutes leurs limites, notamment pour ce qui concerne la sécurité dans la transmission des données, la fiabilité relative des informations présentes sur le réseau et les temps de réponse.

Les règles de bon fonctionnement : procédures informatiques

Les principes évoqués dans ce chapitre sont développés sur le site Intranet de la DSI.

Le but des procédures informatiques définies par le Cirad est d'assurer la sécurité et la bonne marche du système d'information.

Définition et gestion des mots de passe

Principe : Il est recommandé de veiller en priorité à sécuriser les mots de passe permettant l'accès à son environnement.

A cet égard :

– chacun choisit un mot de passe sûr, n'ayant aucun lien avec son environnement familier. Le mot de passe ne doit contenir aucun des noms communs figurant au dictionnaire ni aucun nom propre anglais ou français ;

– chaque mot de passe doit être changé régulièrement, si les applications le permettent ;

– en aucun cas, le mot de passe ne doit être écrit sur un support facilement accessible.

Protection du poste de travail

Principe : le poste de travail de l'utilisateur doit être protégé des intrusions. Pour ce faire, l'utilisateur doit se déconnecter des serveurs réseaux et applications avant de quitter son poste de travail.

A cet égard :

– il paramètre la mise en veille automatique des postes de travail avec demande du mot de passe pour la réactivation du poste après un temps déterminé (généralement 15 minutes) ;

– il veille à ne pas se connecter au réseau ou ouvrir des sessions applicatives inutilement ;

– il veille à se déconnecter des serveurs réseaux et quitte les applications actives avant de quitter son poste de travail ;

– il veille à ne pas entraver la mise à jour des logiciels antivirus, lorsque cette mise à jour est automatique et procède à une mise à jour régulière lorsqu'elle n'est pas automatique ;

– il facilite la mise à jour du système d'exploitation lorsque celle-ci est automatique et consulte régulièrement le site de l'éditeur du système d'exploitation si la mise à jour n'est pas automatique.

Le site de la DSI comporte toutes les indications utiles à ce sujet.

Les précautions concernant les postes nomades

Principe : l'utilisateur à qui a été confié, dans le cadre de ses activités professionnelles, un équipement de type appareil photo numérique, caméscope, téléphone portable ou ordinateur portable doit veiller à le protéger.

A cet égard :

– en cas de non utilisation, il le range dans un endroit sécurisé et fermé à clef ;

– il veille particulièrement à ne pas exposer à la chaleur ou à l'humidité l'équipement confié, à ne pas le laisser sans surveillance, à ne pas l'oublier ou lui faire subir des chocs ;

– il utilise le câble antivol distribué à cet effet, y compris dans ses propres locaux professionnels ;

– il veille à fermer son bureau à clef, en dehors des heures de travail et en cas d'absence prolongée.

En cas de vol d'un équipement fourni, une déclaration doit être effectuée sans délai au commissariat de police le plus proche avec une copie adressée au Sage du département, ainsi qu'une courte note relatant les circonstances du vol et une copie de la facture d'achat du matériel volé.

En cas de perte de l'équipement confié, une déclaration détaillée doit être adressée au Sage du département.

Les règles d'utilisation de la messagerie

Limitations de la messagerie électronique

La taille des messages envoyés ou reçus est délibérément limitée. La taille limite actuelle est de 7 Mo et de 1 Mo en ce qui concerne les forums gérés par le Cirad. Ces limitations peuvent être modifiées en fonction des contraintes que le Cirad pourrait rencontrer.

En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un avis de non distribution.

La taille de la boîte aux lettres sur le serveur n'est pas limitée ; toutefois il est conseillé de ne pas laisser plus de 200 messages non lus sur le serveur afin d'éviter la saturation des disques de celui-ci.

Il est inutile de consulter sa boîte aux lettres avec une fréquence inférieure à 10 minutes, afin d'éviter une utilisation abusive des ressources du serveur et donc de dégrader ses performances.

Stockage et archivage des messages

Chaque utilisateur est responsable de l'archivage et du classement des messages qu'il a relevés sur le serveur hébergeant sa boîte de réception.

Les serveurs de messagerie sont sauvegardés, les messages stockés sur les serveurs et non lus par les utilisateurs sont conservés.

L'utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables, notamment en tant qu'élément de preuve.

Il est rappelé que les boîtes aux lettres à accès partagé ne doivent pas servir d'espace de stockage ou d'archivage pour les messages ou dossiers partagés.

La sécurité antivirale

Les messages ou fichiers contenant des virus, spyware ou autre malware sur le poste de travail de l'utilisateur ne sont pas supprimés mais mis en quarantaine, le choix de la suppression des fichiers ou messages infectés étant à la discrétion de l'utilisateur.

De manière générale, il est déconseillé d'ouvrir des fichiers, de quelque nature que ce soit, en provenance d'un expéditeur inconnu.

La lutte antispam

Il est fortement déconseillé de répondre, pour quelque motif que ce soit, à un message de type spam. En effet cela peut indiquer à l'émetteur du spam que la boîte aux lettres est active et donc amplifier le phénomène. De la même façon, il est recommandé de ne pas communiquer son adresse e-mail professionnelle sur Internet.

Le Cirad a mis en place des dispositifs de lutte antispam susceptibles d'évoluer.

Attention : les logiciels de lutte antispam ne sont pas fiables à cent pour cent ; certains spams peuvent passer à travers les mailles du logiciel ; de même le logiciel peut reconnaître des messages normaux comme étant des spams.

La sauvegarde des données du poste de travail

Il est rappelé que la sauvegarde des données du poste de travail est à la charge de l'utilisateur. Elle ne dépend ni de la Délégation aux systèmes d'information, ni de l'assistance informatique.

Lors d'une remise à plat du poste d'un utilisateur, les données sont conservées pendant une durée de trois jours. Lors d'une installation ou d'une réaffectation du poste, les données sont conservées pendant un mois.

Toutefois, il est rappelé que seule une sauvegarde personnelle et régulière des données préservera l'utilisateur de la perte de celles-ci.

▶ L'assistance informatique : prise de main à distance

Afin d'améliorer l'efficacité de leurs services et prestations, les administrateurs du système informatique peuvent utiliser des logiciels de prise de main à distance pour accéder à n'importe quel poste de travail informatisé du Cirad.

Dans ce cas, l'utilisateur en est informé préalablement et donne son accord en validant un message d'information apparaissant sur son écran. La fin de l'assistance implique la reprise de main automatique au profit de l'utilisateur.

Livre IV. Droits et obligations des administrateurs système, réseaux et applications

Le présent livre IV de la charte informatique du Cirad a pour objet de formaliser les règles de déontologie et les procédures de sécurité spécifiques qui s'imposent, dans la limite de leur responsabilité effective, aux administrateurs système/réseaux, aux administrateurs fonctionnels des applications et aux correspondants techniques du Cirad.

S'entend par « administrateur de ressources informatiques » : toute personne chargée de l'exploitation, de la maintenance, du suivi de l'utilisation de ces ressources informatiques et de télécommunication, de la mise en œuvre des logiciels et de la gestion fonctionnelle des applications.

Les administrateurs de ressources informatiques possèdent des droits étendus quant à l'utilisation et à la gestion des ressources informatiques ou quant à l'utilisation et à la gestion des applications. Dans le cadre de leurs activités, ils sont amenés à avoir accès aux informations des autres utilisateurs des ressources informatiques, ainsi qu'à des sources d'informations confidentielles.

Les administrateurs de ressources informatiques sont soumis au secret professionnel.

L'administrateur est, en tout état de cause, soumis à l'ensemble de la charte et, notamment, à son livre II.

Les droits d'intervention des administrateurs

Il appartient aux administrateurs de signaler à leur hiérarchie toute anomalie persistante de fonctionnement ou toute infraction aux dispositions de la charte.

En cas de non-respect des dispositions de la charte, les administrateurs pourront contrôler et prendre connaissance de tous les messages, hors messages identifiés ou classés dans des répertoires privés ou personnels, émis ou reçus par chacun des utilisateurs.

En tout état de cause, la hiérarchie peut être amenée à demander aux administrateurs communication des informations qu'ils sont susceptibles d'obtenir dans l'exercice de leurs fonctions et ce, dans le respect de la vie privée des utilisateurs et du secret des correspondances privées.

La sécurité

La sécurité de ces moyens informatiques et de télécommunication impose à l'administrateur :

– de n'utiliser que les matériels confiés par la DSI ou par la direction du Cirad ;

– de ne pas installer et de ne pas utiliser sur les ordinateurs, et plus généralement sur les matériels informatiques, un logiciel et/ou un progiciel sans qu'une licence d'utilisation appropriée n'ait été préalablement souscrite ;

– de garder strictement confidentiel son mot de passe « administrateur » sous réserve des dispositions prévues au paragraphe « continuité de service » ;

– de respecter la plus stricte confidentialité des mots de passe des utilisateurs dont il aurait pu avoir connaissance ;

– d'inciter régulièrement les utilisateurs au respect des consignes de sécurité figurant dans la charte.

La gestion des traces

L'administrateur assure la gestion des traces des ressources informatiques.

L'administrateur assure, pendant la durée de conservation prévue (un an), la sauvegarde et la conservation des traces, sauf situation de litige ou de contentieux.

Messagerie électronique, Web et sécurité

Les administrateurs doivent utiliser les moyens mis à leur disposition pour empêcher l'activation de virus, de bombe logique, de cheval de Troie provenant notamment de l'ouverture de messages reçus par les systèmes de messagerie ou lors de l'accès par les utilisateurs aux ressources du Web.

Les administrateurs doivent procéder à la mise à jour régulière des logiciels et/ou progiciels assurant la sécurité du système d'information.

En cas de doute sur l'efficacité des mesures, les administrateurs doivent, en accord avec leur hiérarchie, appliquer le principe de précaution et détruire les fichiers qu'ils estimeraient susceptibles de porter atteinte à l'intégrité et à la sécurité du système d'information et, notamment le cas échéant, les fichiers comprimés ou auto-extractibles.

La continuité du service

La continuité du service et de la mission de l'administrateur doit être assurée dans le cadre de la politique mise en place par sa hiérarchie.

L'administrateur doit donc faire le nécessaire pour que soit assurée cette continuité de service avec les moyens fournis par sa hiérarchie pendant les heures normales d'ouverture du site sur lequel il se trouve et dans le respect du temps de travail légal.

La confidentialité

L'administrateur est une personne ayant des droits particulièrement étendus quant à l'utilisation et la gestion des systèmes d'information.

A ce titre, il doit garder confidentielle toute information à laquelle il peut avoir accès, ce qui implique notamment :

– de ne transmettre aucune information essentielle sans concertation préalable avec sa hiérarchie et accord de cette dernière ;

– de veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations.

D'une manière générale, il doit respecter les règles d'éthique professionnelle et de déontologie, l'obligation de réserve ainsi que le devoir de discrétion.

Les droits de propriété

L'utilisation des systèmes d'information implique le respect des droits de propriété de nos partenaires et, plus généralement, des tiers.

Chaque administrateur doit donc :

– veiller à ce que les logiciels soient utilisés dans les conditions de licences souscrites et peut informer sa hiérarchie en cas de manquement ;

– veiller à ce que les logiciels, bases de données, pages Web ou autres créations de tiers protégées par le droit d'auteur ou un droit privatif ne soient pas reproduits, utilisés ou remis à des tiers.

L'infogérance

Le Cirad est susceptible de confier à une entreprise extérieure, le soin d'assurer les opérations de maintenance de tout ou partie de ses ressources informatiques, dans le cadre d'un contrat dit « d'infogérance ».

Dans ce cas, ce contrat prévoit les dispositions nécessaires au respect de la présente charte par le prestataire et ses préposés, qui sont soumis aux mêmes obligations, dans le cadre précisément défini de leurs missions, que les administrateurs de ressources informatiques du Cirad. Comme tels, les dispositions de la charte, et en particulier celles du présent livre, doivent leur être appliquées.

De ce fait, la charte informatique du Cirad sera transmise, dès son entrée en vigueur, aux responsables de la société prestataire en charge de l'infogérance au moment de sa première parution. Une communication pourra être effectuée à ce sujet par les représentants du Cirad au comité de pilotage et/ou au comité stratégique prévus par le contrat d'infogérance, qui sont désignés par la direction.

Un avenant au contrat liant le Cirad à cette entreprise pourra, en tant que de besoin, matérialiser les obligations de la société prestataire en ce domaine et leur reconnaissance explicite par celle-ci.

Ultérieurement, un exemplaire de la charte sera systématiquement remis à tout nouveau prestataire et joint au contrat d'infogérance.

D'une manière générale, la société prestataire s'oblige à prendre toutes dispositions pour assurer la sécurité logique et physique des ressources informatiques du Cirad. Le Cirad définit seul les règles et procédures en matière d'autorisations d'accès aux ressources informatiques des équipements sur les sites et il conserve la maîtrise des autorisations d'accès qui sont consenties au prestataire. Les tâches déléguées à l'entreprise par le Cirad restent soumises au contrôle du Cirad.

Les personnels du prestataire travaillant dans les locaux du Cirad doivent respecter la présente charte et doivent se conformer au règlement intérieur et aux procédures de sécurité et d'habilitation en vigueur au Cirad.

L'entreprise prestataire doit également respecter les droits de propriété du Cirad sur ses ressources informatiques et limiter leur utilisation aux seuls besoins des prestations d'infogérance, sauf dispositions contraires conclues expressément d'accord parties.

L'entreprise prestataire s'engage par ailleurs à respecter la confidentialité des informations dont ses préposés auraient connaissance au cours de leurs prestations.

Glossaire

Archivage : opérations visant à mettre des fichiers, généralement sous forme compressée, sur un support de stockage magnétique ou optique et à assurer la conservation des fichiers sur une longue durée. L'accès aux données archivées n'est pas immédiat et peut nécessiter plusieurs opérations.

Certa : Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques.
Voir : **http://www.certa.ssi.gouv.fr/**

Cnil : Commission nationale de l'informatique et des libertés. La Cnil a pour mission essentielle de protéger la vie privée et les libertés individuelles ou publiques. Elle est chargée de veiller au respect de la loi dite « Informatique et libertés ».

Cryptage : technique de sécurisation des données. Action de rendre inintelligible un message par l'emploi d'un code chiffré.

DCSSI : Direction centrale de la sécurité des systèmes d'information, dépend du secrétariat général de la Défense nationale.
Voir : **http://www.ssi.gouv.fr/fr/dcssi/**

Espace de stockage : espace servant à enregistrer toutes les données que l'on désire conserver : logiciels et fichiers (documents, images, sons, bases de données...). Il y en a de plusieurs sortes. Les plus usuels sont : le disque dur, les disquettes, les CD, les bandes magnétiques. Ils peuvent être dédiés à un utilisateur ou partagés entre plusieurs utilisateurs (c'est souvent le cas pour l'espace de stockage d'un serveur).

Filtrage : le filtrage est un ensemble de technologies visant à limiter l'accès à certaines applications, à certains sites Web normalement accessibles sur le réseau Internet ou à certains messages (filtres antispam, antivirus).

Forum : les forums ou groupes de discussion (*newsgroup* en anglais) désignent les lieux d'échanges de messages électroniques situés sur les sites Internet. Organisés généralement par thèmes, ils rassemblent les internautes qui échangent des avis et des informations ou formulent des questions sur les sujets qui les intéressent.

Informations nominatives : il s'agit des informations « qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».

Internet : réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destinés à l'échange de messages électroniques, d'informations multimédias et de fichiers. Ne pas confondre avec le serveur Web institutionnel accessible depuis Internet et communément appelé serveur Internet.

Intranet : réseau de télécommunication et de téléinformatique destiné à l'usage exclusif d'un organisme et utilisant les mêmes protocoles techniques qu'Internet. Ne pas confondre avec le serveur Web interne accessible seulement depuis le réseau Intranet du Cirad et communément appelé serveur Intranet.

Messagerie électronique ou courriel : service géré par ordinateur permettant aux utilisateurs habilités de saisir, de distribuer et de consulter en différé des messages comportant des écrits, des images ou des sons.

Navigateur : logiciel permettant à l'utilisateur de rechercher et de consulter des documents, et d'exploiter les liens hypertextes qu'ils comportent.

Pare-feu *(firewall)* : dispositifs informatiques qui permettent le filtrage des flux d'information entre un réseau interne à un organisme et un réseau externe et entre les composantes d'un même réseau interne, et qui ont pour objectif, d'une part, de neutraliser les tentatives non autorisées de pénétration en provenance de l'extérieur ainsi que les tentatives de corruption du système informatique depuis l'intérieur du réseau et, d'autre part, de maîtriser les accès vers l'extérieur.

Répertoire : liste d'identificateurs, classés selon des arguments appropriés, permettant l'accès aux informations qu'ils désignent.

Serveur : ordinateur, connecté à un réseau, dont le rôle est d'héberger et de rendre accessibles des données et des logiciels.

Spam : courrier électronique commercial non sollicité par l'internaute qui le reçoit, également appelé pourriel.

Stockage : enregistrement de données à plus ou moins long terme sur un support (disque dur, par exemple) permettant d'enregistrer des quantités importantes de données. L'accès à ces données est rapide.

Traces : enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque connexion. Elles recensent et archivent l'activité liée à des services avec des informations parfois nominatives.

Centre
de coopération
internationale
en recherche
agronomique
pour le
développement