

Charte du Système d'information



SOMMAIRE

1.	INTRODUCTION	3
2.	DEFINITIONS	4
3.	CONTEXTE ET ENJEUX.....	4
3.1	Objectif	5
3.2	Le champ d'application	5
3.3	Droits et Devoirs de l'Entité	5
4.	PRINCIPES DE SECURITE.....	6
4.1	Protection des informations et des documents électroniques	6
4.2	Protection des moyens et des droits d'accès aux informations	6
4.3	Protection des équipements informatiques	6
4.4	Protection vis-à-vis des échanges sur les réseaux	7
4.5	Protection vis-à-vis de l'accès aux services en ligne sur internet	7
4.6	Publication d'information sur internet ou sur intranet	8
4.7	Conditions d'accès aux ressources documentaires électroniques	8
4.8	Utilisateurs administrateurs de leur poste de travail.....	8
5.	VIE PRIVEE ET RESSOURCES INFORMATIQUES PERSONNELLES	9
5.1	Vie privée résiduelle.....	9
5.2	Ressources informatiques personnelles.....	9
5.3	Gestion des départs	9
6.	UTILISATION DU TELEPHONE.....	9
6.1	Personnels protégés.....	10
7.	MISE A DISPOSITION D'UN SERVICE DE MESSAGERIE	10
8.	ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES	10
8.1	Administrateur système et réseau.....	10
8.2	Personnels protégés.....	11
9.	DONNEES A CARACTERE PERSONNEL	11
10.	RESPECT DE LA PROPRIETE INTELLECTUELLE.....	11
11.	INFORMATIONS COMPLEMENTAIRES	12
12.	RAPPEL DES PRINCIPALES LOIS ET REGLEMENTATIONS.....	12

1. INTRODUCTION

Cette charte a pour objet d'informer les Utilisateurs de leurs droits et de leurs responsabilités au sujet de l'usage des ressources informatiques et des services internet/intranet de l'IRD, en application de la législation et de la réglementation en vigueur.

Elle répond à la préoccupation de l'IRD de protéger les informations qui constituent son patrimoine immatériel contre toute altération, volontaire ou accidentelle, de sa confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité du système d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique).

L'Utilisateur contribue à son niveau à la sécurité du système d'Information. À ce titre, il applique les règles de sécurité en vigueur et signale tout dysfonctionnement ou événement lui paraissant anormal.

Le personnel d'encadrement favorise l'instauration d'une « culture sécurité » par son exemplarité dans le respect de cette charte et par un soutien actif des équipes en charge de la mise en œuvre de ces règles.

Cette charte résulte d'un équilibre entre les droits et devoirs de l'employeur et de l'agent. Une utilisation personnelle est autorisée sous réserve de ne pas nuire au temps consacré au travail et à la qualité de ce dernier. Un équilibre vie professionnelle et vie privée doit être respecté.

Cette présente charte a été soumise à l'avis des instances représentatives du personnel.

Les Utilisateurs sont tenus de respecter les chartes des partenaires dont l'IRD utilise les moyens. La présente charte peut également être complétée par des chartes locales ou par des dispositions intégrées aux règlements intérieurs propres aux unités, délégations régionales, ou représentations, après avis, le cas échéant, des conseils d'unités, des CTS ou conseils de représentation. En particulier, la charte est accompagnée d'un guide juridique qui rappelle les dispositions législatives et réglementaires en vigueur pour son application. Elle est également complétée par des guides utilisateurs définissant les principales règles d'usage.

Cette charte pourra être réactualisée, auquel cas les utilisateurs en seront informés. La charte en vigueur se trouve également sur l'intranet de l'IRD.

Tout manquement, selon sa gravité, est susceptible d'entraîner pour l'utilisateur des sanctions disciplinaires, et ce sans exclusion d'éventuelles actions pénales ou civiles à son encontre. L'utilisateur pourra, en outre, voir ses droits d'accès aux ressources et système d'information et de communication suspendus ou supprimés, partiellement ou totalement.

2. DEFINITIONS



On désignera de façon générale sous le terme « **ressources informatiques** », les moyens informatiques (tels que postes de travail, serveurs, réseau local) auxquels il est possible d'accéder à partir du réseau de l'IRD.



On désignera par « **services Internet** » la mise à disposition par des serveurs de moyens d'échanges ou d'informations diverses : Web, messagerie, forums ...



On désignera par « **services Intranet** » la mise à disposition de ressources informatiques réservées à tout ou partie du personnel de l'IRD ou habilité comme tel (certaines pages Web, licences logicielles, accès à certaines bases de données, programmes informatiques, applications métiers...).



On désignera sous le terme « **utilisateur** », toutes les personnes ayant accès ou utilisant les ressources informatiques, services Internet ou services Intranet de l'IRD.



On désignera sous le terme « **entité** » : toutes les entités créées par l'IRD pour l'accomplissement de ses missions, notamment les unités de recherche ou de service propres ou mixtes ainsi que les services et directions administratives.



On désignera sous le terme « **administrateur** » : les personnes gérant et assurant le bon fonctionnement d'un ou plusieurs éléments matériels ou logiciels (outils, réseaux, bases de données, messagerie, métier...).



On désignera sous le terme « **application** » : les moyens informatiques utilisés pour une activité.

3. CONTEXTE ET ENJEUX

Les différents outils technologiques peuvent apporter des améliorations de performances importantes si leur utilisation est faite à bon escient et selon certaines règles.

Au contraire, une mauvaise utilisation augmente les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles. De plus, mal utilisés, ces outils peuvent être une source de perte de productivité et de coûts additionnels.

La présente charte et ses annexes tendent à préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun.

3.1 OBJECTIF

La présente charte formalise les règles relatives à l'utilisation de tout système d'information et de communication au sein de l'Entité (applications métiers, bureautique, messagerie, micro-ordinateurs fixes et portables, périphériques, téléphones fixes et portables, Internet, Extranet, Intranet...).

3.2 LE CHAMP D'APPLICATION

Chaque utilisateur doit connaître, respecter et appliquer la présente charte.

La présente charte, signée par le Président-directeur général après avis du Comité technique d'établissement public (CTEP) de l'IRD en date du 6 octobre 2016, s'applique à l'ensemble des agents de l'IRD tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de l'IRD et de ses implantations ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par l'Entité.

La présente charte arrêtée après avis des instances consultatives fait l'objet d'une publicité par voie d'affichage dans les Entités de l'IRD et au bulletin officiel (BO) de l'IRD. Une version informatique est mise à disposition sur l'intranet et l'internet de l'IRD.

Sur ces interfaces, les textes visés en référence et les notes de service seront également disponibles au format numérique.

Chaque agent a le devoir de la promouvoir et de veiller à son application.

Il est entendu que les annexes pourront être modifiées de façon unilatérale et feront l'objet de la publication adéquate.

Il est entendu que toute disposition de la présente charte qui deviendrait contraire aux dispositions légales, réglementaires ou conventionnelles applicables à l'IRD du fait de leur évolution, serait nulle de plein droit.

La charte du 23 janvier 2004 et toute note qui la modifiait/complétait sont abrogées à compter de la date de signature de la présente charte.

3.3 DROITS ET DEVOIRS DE L'ENTITE

L'IRD doit veiller à la disponibilité, à l'intégrité et à la confidentialité de ses données et de son système d'information.

En ce sens, l'IRD définit les règles d'usage de son système d'information. Il informe et accompagne les utilisateurs dans la mise en œuvre de ces mesures de protection et met en place les programmes de formations adaptés pour une bonne utilisation des outils. L'IRD informe les utilisateurs des diverses contraintes d'exploitation du système d'information susceptibles d'occasionner une perturbation. Il effectue les mises à jour nécessaires des matériels et des logiciels afin de maintenir le niveau de sécurité en vigueur. Enfin, l'IRD s'engage à respecter la confidentialité des « données utilisateurs » auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.

4. PRINCIPES DE SECURITE

Les règles ci-après s'appliquent à tous les utilisateurs, et peuvent être complétées par des mesures spécifiques à leur entité qui seront adoptées par la structure de rattachement.

4.1 PROTECTION DES INFORMATIONS ET DES DOCUMENTS ELECTRONIQUES

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.

L'utilisateur protège les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité. Il active les moyens mis à sa disposition (sauvegarde, mise sous clé, verrouillage du poste de travail) et met en œuvre les recommandations de la sécurité du système d'Information de l'IRD (Annexe Charte du SI - Guide Opérationnel).

4.2 PROTECTION DES MOYENS ET DES DROITS D'ACCES AUX INFORMATIONS

L'utilisateur est responsable des ressources informatiques et des services auxquels il a accès ainsi que de l'utilisation des systèmes d'information réalisée avec son compte utilisateur.

Les moyens d'authentification constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Ainsi l'utilisateur assure la protection des moyens d'authentification qui lui ont été affectés ou qu'il a générés (badges, mots de passe, clés privées, clés privées liées aux certificats, etc.)

L'utilisateur informe les administrateurs du système d'information de toute évolution de ses fonctions nécessitant une modification de ses droits d'accès.

4.3 PROTECTION DES EQUIPEMENTS INFORMATIQUES

L'Utilisateur doit veiller à la protection contre toute menace, des équipements qui lui ont été confiés.

L'utilisateur a la charge, à son niveau, de contribuer à la sécurité et à l'intégrité des ressources informatiques. En conséquence, il protège les équipements mis à sa disposition ainsi que les équipements personnels qu'il utilise pour accéder, à distance ou à partir du réseau local d'une entité, au système d'information de l'IRD.

4.4 PROTECTION VIS-A-VIS DES ECHANGES SUR LES RESEAUX

L'utilisateur est responsable du contenu des informations qu'il diffuse et échange sur les réseaux.

4.4.1 Contenu des échanges sur les réseaux

Les échanges électroniques (courriers, forums de discussion, messagerie instantanée, réseaux sociaux professionnels ou non professionnels, partages de documents, voix, images, vidéos, etc.) respectent la correction normalement attendue dans tout type d'échange tant écrit qu'oral. Les agents doivent notamment respecter leurs devoirs de discrétion professionnelle, correction, réserve, neutralité.

4.4.2 Vigilance

L'utilisateur fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage,...). L'utilisateur avertit DSI-Assistance s'il a connaissance de problèmes de ce type.

4.4.3 Statut et Valeur Juridique des informations échangées

Les informations échangées par voie électronique avec des tiers peuvent, au plan juridique, former un contrat sous certaines conditions ou encore être utilisées à des fins probatoires. L'utilisateur doit, en conséquence, être prudent sur la nature des informations qu'il échange par voie électronique au même titre que pour les courriers traditionnels.

4.4.4 Stockage et archivage des informations échangées

L'utilisateur est informé que le courriel peut être reconnu en tant que preuve en cas de contentieux.

4.5 PROTECTION VIS-A-VIS DE L'ACCES AUX SERVICES EN LIGNE SUR INTERNET

L'usage des services en ligne sur internet doit se faire dans le respect des lois et règlements et de manière modérée.

Si une utilisation résiduelle privée peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'Entité sont présumées avoir un caractère professionnel.

L'Entité, dans un souci de sécurité ou par opportunité, s'autorise le droit de bloquer l'accès à des sites frauduleux, des sites sans rapport avec l'activité professionnelle, des sites malveillants connus...

Par activité professionnelle, il convient notamment d'entendre : les activités de recherches, d'enseignements, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentations de nouveaux services présentant un caractère d'innovation technique, et également toute activité administrative et de gestion découlant ou accompagnant les activités.

4.6 PUBLICATION D'INFORMATION SUR INTERNET OU SUR INTRANET

Toute publication d'information sur les sites internet ou intranet de l'IRD est réalisée sous la responsabilité d'un responsable de site ou responsable de publication nommément désigné.

Aucune publication d'information non professionnelle sur les ressources du système d'information de l'IRD n'est autorisée, sauf disposition particulière décidée au sein de l'Entité.

L'usage de service de «Cloud computing» (informatique dans les nuages) externes à l'IRD est toléré à condition qu'il respecte les règles en vigueur (Annexe Charte du SI - Guide Opérationnel).

Il est notamment primordial que les données sensibles (données de recherche, données administratives, etc.) du système d'information ne sortent pas du périmètre maîtrisé par l'IRD et ne soient pas portées à la connaissance de personnels non autorisés.

4.7 CONDITIONS D'ACCES AUX RESSOURCES DOCUMENTAIRES ELECTRONIQUES

L'usage des ressources documentaires électroniques éditoriales doit respecter les conditions contractuelles des licences souscrites par l'IRD.

D'une façon générale, et sauf mention contraire explicite dans la licence, à demander le cas échéant à la Direction des affaires juridiques (daj@ird.fr), les éditeurs n'autorisent qu'une utilisation « raisonnable » et personnelle des ressources documentaires électroniques, dans un but strictement non-commercial et à des fins pédagogiques ou de recherche, conforme à la législation et à la réglementation en vigueur.

4.8 UTILISATEURS ADMINISTRATEURS DE LEUR POSTE DE TRAVAIL

Sur l'intranet de l'IRD, la [charte de l'utilisateur-administrateur](#) est disponible. Il convient d'en prendre connaissance et de s'y conformer dans le cas où vous êtes administrateurs de votre poste de travail.

5. VIE PRIVEE ET RESSOURCES INFORMATIQUES PERSONNELLES

5.1 VIE PRIVEE RESIDUELLE

Un usage personnel des ressources informatiques fournies par l'Entité ou ses partenaires est toléré à condition qu'il reste de courte durée, qu'il n'affecte pas l'usage professionnel, qu'il ne mette pas en danger le bon fonctionnement et la sécurité du système d'information, qu'il n'enfreigne pas la loi, les règlements et les dispositions internes et qu'il ne soit pas à but lucratif.

Toute donnée est réputée professionnelle.

5.2 RESSOURCES INFORMATIQUES PERSONNELLES

Les ressources informatiques personnelles, utilisées pour accéder, à distance ou à partir du réseau local d'une Entité, au système d'information de l'IRD ou pour stocker des données professionnelles, doivent être autorisées et sécurisées. Elles doivent être déclarées au service informatique qui gère le parc matériel de l'Entité. Les personnels qui souhaiteraient faire l'acquisition de tels matériels prennent préalablement conseil auprès de leur service informatique local.

Ces ressources informatiques personnelles ne doivent pas remettre en cause ou affaiblir, les politiques de sécurité en vigueur par une protection insuffisante ou une utilisation inappropriée.

5.3 GESTION DES DEPARTS

Il appartient à l'utilisateur de détruire ses données personnelles préalablement à son départ.

En cas de circonstances exceptionnelles (départ impromptu ou décès) ou si l'utilisateur n'a pas procédé à la destruction de ses données personnelles, l'Entité ne conserve les espaces de données à caractère privé présents sur les ressources informatiques fournies par l'Entité que pour une période de 3 mois maximum (délai permettant à l'Utilisateur ou ses ayants droits de récupérer les informations qui s'y trouvent).

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies au sein de l'IRD (Voir le Guide opérationnel de la charte du SI).

6. UTILISATION DU TELEPHONE

L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles. Un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que

cela n'entrave pas l'activité professionnelle.

L'Entité peut procéder au contrôle de l'ensemble des appels émis (sauf cas particulier des personnels protégés – cf article 6.1). Tout utilisateur tenu responsable d'un usage illicite d'un poste téléphonique s'expose à une sanction.

6.1 PERSONNELS PROTEGES

L'Entité ne peut utiliser des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par **les représentants du personnel et les représentants syndicaux** dans le cadre de leur mandat.

7. MISE A DISPOSITION D'UN SERVICE DE MESSAGERIE

L'utilisation de l'adresse professionnelle nominative se fait sous la responsabilité de l'utilisateur qui est informé que le contenu de ses courriels pourrait lui être opposé.

L'Entité s'engage à mettre à la disposition de l'Utilisateur une boîte à lettres nominative lui permettant d'émettre et de recevoir des messages électroniques professionnels.

Un usage personnel est toléré à condition qu'il reste modéré et n'affecte pas l'usage professionnel. Les courriels à caractère privé et personnel doivent porter la mention « privé » ou « personnel » dans leur objet.

Des règles de bon usage du service de messagerie sont à respecter. Vous trouverez ces règles dans le document « [J'adopte l'e-mail attitude – Cinq principes pour un bon usage de la messagerie électronique](#) » disponible sur l'intranet de l'IRD.

8. ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES

La loi et les règlements imposent à l'Entité de garder un historique des accès réalisés par les utilisateurs. L'Entité a donc mis en place une journalisation des accès (Annexe Charte du SI - Guide Opérationnel).

8.1 ADMINISTRATEUR SYSTEME ET RESEAU

L'administrateur système et réseau doit veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes placés sous sa responsabilité.

L'administrateur est conduit par ses fonctions à avoir accès à l'ensemble des informations relatives aux utilisateurs y compris celles qui sont enregistrées sur leur poste de travail.

Toutefois, l'administrateur est soumis à une obligation de confidentialité et de discrétion professionnelle. Il ne peut donc divulguer les informations qu'il est amené à connaître dans le

cadre de ses fonctions, en particulier lorsqu'elles sont couvertes par le secret des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité. De plus, aucune exploitation de ces informations à des fins autres que celles liées au bon fonctionnement et à la sécurité des ressources informatiques, services internet et services intranet ne saurait être opérée.

L'administrateur ne peut prendre connaissance ou tenter de prendre connaissance du contenu des répertoires, fichiers ou message manifestement et explicitement désignés comme personnels qu'en présence de l'agent et avec son accord, en cas d'urgence ou de nécessité vis-à-vis de la législation ou de la sécurité.

8.2 PERSONNELS PROTEGES

L'Entité respecte le principe de protection de la vie privée de l'utilisateur sur son lieu de travail et donc du secret des correspondances et des fichiers relevant des activités syndicales ou sociales. Ces messages et ces fichiers doivent être placés dans des dossiers dont les noms sont explicites : syndical (ou le nom du syndicat), social. Aucun autre utilisateur que le propriétaire n'est autorisé à accéder au contenu de ces dossiers.

9. DONNEES A CARACTERE PERSONNEL

Si, dans l'accomplissement de ses missions, l'Utilisateur souhaite constituer des fichiers contenant des données à caractère personnel soumis aux dispositions de la loi informatique et libertés, il prend l'attache de la Direction des affaires juridiques et le Responsable de la sécurité des systèmes d'information (RSSI) qui procèderont, le cas échéant, aux déclarations nécessaires auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Informations utiles sur l'intranet de l'IRD : <https://intranet.ird.fr/l-ird-et-moi/reglementation/informatique-et-libertes>

Le transfert de données personnelles depuis le territoire européen vers des pays situés en-dehors de l'Union européenne est interdit sauf cas particulier renseignés par la Direction des affaires juridiques sur demande (voir également en ce sens : Annexe Charte du SI - Guide Juridique).

Les sanctions encourues en cas de non-respect des règles en matière de transferts de données hors de l'Union européenne sont de 300 000 euros d'amende et de 5 ans d'emprisonnement pour une personne physique (articles 226-16, 226-16 A et 226-22-1 du Code pénal).

10. RESPECT DE LA PROPRIETE INTELLECTUELLE

Conformément aux dispositions du Code de la propriété intellectuelle, l'utilisateur ne peut notamment reproduire, télécharger, copier, diffuser, modifier ni utiliser toutes créations protégées par le droit de propriété intellectuelle, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Il est strictement interdit d'effectuer des copies de logiciels pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété

intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin, le Président-directeur général de l'IRD.

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

11. INFORMATIONS COMPLEMENTAIRES

La Direction pour le Développement des Usages Numériques Innovants se tient à la disposition de l'utilisateur pour toute question relative à sa compréhension (rssi@ird.fr).

Par ailleurs, les modalités particulières d'usage des ressources informatiques et services intranet sont décrites dans le Guide Opérationnel annexé à la Charte du SI et sur le site intranet de l'IRD, dans l'espace DDUNI. L'utilisateur y trouvera en particulier, des informations sur les services d'assistance mis à sa disposition, les procédures à suivre lors de son recrutement, d'une mutation ou de son départ à la retraite et les informations légales concernant la conservation des données.

12. RAPPEL DES PRINCIPALES LOIS ET REGLEMENTATIONS

L'utilisateur est tenu de respecter l'ensemble du cadre légal et réglementaire lié à l'utilisation du système d'information ainsi que toute autre réglementation susceptible de s'appliquer.

Le recueil des textes législatifs et réglementaires à respecter sont disponibles dans le guide juridique en Annexe de la charte. Des informations complémentaires sur les lois et réglementations sont développées dans ce guide.

Marseille le 12/01 / 2017

Le Président-directeur général de l'IRD
Monsieur Jean-Paul MOATTI

