

CHARTRE

UTILISATION DU SYSTEME D'INFORMATION

Table des matières

1. Préambule	4
2. Définitions	4
3. Domaine d'application de la charte	5
3.1. Personnes concernées	5
3.2. Dérogation	5
4. Règles d'utilisation du système d'information	5
4.1. Utilisation professionnelle	5
4.2. Utilisation privée résiduelle	7
5. Conditions d'accès, absences et départs de l'utilisateur	7
5.1. Conditions d'accès	7
5.2. Gestion des absences	8
5.3. Gestion des départs	8
6. Confidentialité et sécurité	8
6.1. Confidentialité	8
6.2. Sécurité	9
6.3. Secrets particuliers	9
7. Plan de continuité d'activité	10
8. Mobilité et matériels mis à disposition par UBIFRANCE	10
9. Outils collaboratifs et plate-formes de communication collectives	10
9.1. Principes	10
9.2. Forum	10
9.3. Liste de diffusion	11
9.4. Logiciel externe	11
9.5. Services hébergés	11
10. Données à caractère personnel	11
10.1. Devoirs des utilisateurs	11
10.2. Droits des utilisateurs	11
11. Propriété	12
12. Contrôle du système d'information	12
12.1. Principes directeurs	12
12.2. Contrôle du système d'information	13
12.3. Contrôle de la messagerie	14
12.4. Contrôle des consommations de téléphonie fixe et mobile	14
13. Sauvegarde et archivage	15

13.1.	Données	15
13.2.	Messages électroniques	15
13.3.	Données techniques	15
13.4.	Archivage	15
14.	Sanctions	15
15.	Entrée en vigueur	15

1. PREAMBULE

1. La présente charte a pour objet de fixer les principes généraux d'utilisation du système d'information mis à disposition des utilisateurs, dans le cadre de leur activité professionnelle.
2. L'utilisation, dans le cadre d'UBIFRANCE, du système d'information, suppose, de la part des utilisateurs, le respect d'un certain nombre de règles, dont le rôle est :
 - de garantir la disponibilité des systèmes informatiques pour une utilisation conforme à son objet ;
 - d'assurer la sécurité et la préservation des données confidentielles ;
 - de définir les responsabilités respectives d'UBIFRANCE et des utilisateurs.
3. L'utilisation du système d'information suppose le respect des règles destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance, ainsi que, d'une manière générale, le respect des dispositions légales et réglementaires applicables. La présente charte est rédigée dans l'intérêt de chaque utilisateur et manifeste la volonté d'UBIFRANCE d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation du système d'information.
4. Cette charte a pour objectif de formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition par UBIFRANCE du système d'information.
5. La présente charte participe à « la culture de la sécurité » qui constitue une exigence essentielle d'UBIFRANCE et illustre le comportement responsable que chaque utilisateur doit avoir afin de protéger le patrimoine confidentiel et l'image de marque d'UBIFRANCE.
6. En tant que de besoin, la charte peut être complétée par un « livret des procédures », dont l'objet est de décliner au plan pratique les principes de mise en œuvre.
7. La présente charte peut également être complétée de documents spécifiques pour certaines catégories de personnel.

2. DEFINITIONS

1. Au sens de la présente charte, les termes ci-dessous ont la signification suivante :
 - « administrateur » : personne, habilitée par UBIFRANCE, en charge de veiller au bon fonctionnement et à la sécurité du système d'information ;
 - « courrier électronique » : tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public ou privé de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;
 - « donnée » : toute information, sous forme de fichier ou document, détenue par UBIFRANCE ;
 - « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ;
 - « matériel nomade » : moyens techniques, tels que notamment ordinateur portable, téléphone mobile, assistant personnel (PDA) et éléments accessoires (support magnéto-optique, disque dur externe, CD-Rom, clé USB, carte de communication à distance, boîtier d'authentification) qui peuvent être utilisés à l'extérieur d'UBIFRANCE ;

- « prospection directe par courrier électronique » : tout message utilisant la voie électronique destiné à promouvoir directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;
- « secret spécifique » : renseignements, procédés, objets, documents, données informatisées ou fichiers et, notamment, le patrimoine scientifique d'UBIFRANCE, pour lesquels UBIFRANCE, ses clients ou organisations étatiques, définissent des mesures de protection destinées à restreindre leur accès ou leur diffusion ;
- « système d'information » : ensemble des moyens informatiques et de communication électronique et des matériels nomades, y inclus les courriers électroniques, les données, la messagerie et les secrets spécifiques, mis à disposition des utilisateurs pour des utilisations internes (intranet) et externes (internet et réseaux privés ou publics de communication électronique) ;
- « traitement de données à caractère personnel » : toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;
- « UBIFRANCE » : Agence française pour le développement international des entreprises, les missions économiques-UBIFRANCE et les entités de droit local dépendant d'UBIFRANCE ;
- « utilisateur » : les personnes salariées ou non, tous statuts juridiques confondus, permanents ou temporaires, autorisées à utiliser le matériel et le système d'information d'UBIFRANCE.

3. DOMAINE D'APPLICATION DE LA CHARTE

3.1. Personnes concernées

1. Les obligations décrites dans la présente charte s'appliquent à tout utilisateur qui utilise le système d'information d'UBIFRANCE.

3.2. Dérogation

1. Toute demande de dérogation aux différents points définis dans cette charte doit être présentée par écrit à la Direction des systèmes d'information qui se réserve le droit de l'accepter ou de la refuser.

4. REGLES D'UTILISATION DU SYSTEME D'INFORMATION

4.1. Utilisation professionnelle

1. Le système d'information mis à disposition des utilisateurs est réservé à un usage professionnel exclusif.
2. Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner le contrôle renforcé, la suspension immédiate temporaire ou définitive du droit d'utilisation de tout ou partie du système d'information, le retrait du matériel mis à disposition.
3. En tout état de cause, les utilisateurs sont responsables du bon usage du système d'information au regard de la réglementation applicable.

4. Les nouveaux modes de mise à disposition de contenus par voie électronique comportent des risques inhérents à la technologie employée. Ces risques peuvent être causés par :

- un mauvais contrôle de l'information qui, une fois mise à disposition sur un réseau, peut être détournée de sa finalité ;
- la récupération par téléchargement de contenus privatifs (logiciels ou œuvres protégées...) ou la consultation de sites à contenus illicites et contraires aux bonnes mœurs ;
- l'extraction ou l'utilisation de données non conformes à leur finalité émanant d'applications informatiques.

5. Toutes les données d'UBIFRANCE mises en ligne sur un site (interne ou externe), sous forme de carnets d'adresses, annuaires, photographies, logiciels, articles de presse, œuvres protégées ou toutes autres données de toutes natures, devront faire l'objet d'une autorisation préalable d'UBIFRANCE.

6. Les utilisateurs doivent impérativement respecter les règles de bonne conduite définies ci-dessous :

- ne pas communiquer en ligne des informations ayant un caractère diffamatoire, injurieux ou mensonger à l'égard de tiers ;
- ne pas introduire de données à caractère personnel sans l'autorisation préalable d'UBIFRANCE ;
- ne pas consulter ou communiquer en ligne des données à caractère illicite, l'utilisation d'internet permettant d'avoir accès à des sites dont le contenu diffusé est en infraction avec la législation nationale (par exemple : contenus pédophiles, incitation à la haine raciale).

7. Il est notamment interdit sans que cette liste soit limitative de:

- envoyer des messages à caractère injurieux, insultant, dénigrant, diffamatoire, dégradant ou susceptibles de porter atteinte à la vie privée des personnes ou à leur dignité, relatif à la race, l'origine nationale, les mœurs, la religion, les opinions politiques, les origines sociales, l'âge, le sexe ou le handicap ; en cas de réception de tel message, l'utilisateur doit en informer la Direction des ressources humaines s'agissant des salariés, des stagiaires ou intérimaires, et du cas spécifique des volontaires internationaux ou la Direction administrative et financière dans tous les autres cas et notamment s'agissant des prestataires extérieurs, et agir sur instruction de celles-ci ;
- consulter, de copier ou de télécharger le contenu de fichiers ou de sites à caractère pornographique, pédophile, négationniste, extrémiste, raciste, xénophobe, violent ou contraire aux bonnes mœurs ou à l'ordre public tels que notamment la pornographie, la pédophilie et plus généralement tous comportements dégradants. Ces actes peuvent revêtir le caractère d'une infraction pénale qui pourra être dénoncée, à qui de droit, par UBIFRANCE, sans préjudice des sanctions de nature disciplinaire telles que prévues au règlement intérieur d'UBIFRANCE ;
- créer des pages internet (blogs, forums, chats...) afin de tenir des propos relatifs à l'activité professionnelle ;
- diffuser l'adresse e-mail sur des sites Internet sans rapport avec l'activité professionnelle ;
- commettre toute action susceptible de mettre en cause la sécurité matérielle ou juridique d'UBIFRANCE, de porter atteinte à sa réputation ou de constituer pour elle une gêne quelconque, notamment en laissant croire que le message est rédigé et/ou envoyé par l'utilisateur dans l'exercice de ses fonctions ;

- de porter atteinte au système d'information d'UBIFRANCE ou de toutes autres organisations ;
- commettre toute action impliquant :
 - tout mode de chiffrement non conforme aux procédures internes d'UBIFRANCE , sauf dérogation expresse de la Direction des systèmes d'information ;
 - la dissimulation de l'identité par utilisation de pseudonymes ainsi que l'usurpation d'identité de tiers ;
 - toute forme de dénigrement et tout propos de nature diffamatoire à l'égard d'UBIFRANCE (jeux de hasard, bourse...) ;
 - le harcèlement sexuel et/ou moral ;
 - et plus généralement toute action illégale, contraire à la charte ou aux procédures applicables à UBIFRANCE et toute action susceptible d'entraîner la responsabilité civile et/ou pénale d'UBIFRANCE.

8. L'utilisateur s'engage à exercer une vigilance particulière dans le contrôle des contenus échangés et à prendre toutes les précautions nécessaires en cas de reproduction ou de rediffusion d'œuvres ou de données susceptibles de bénéficier d'une protection. Dans le doute, l'utilisateur devra en référer à son responsable hiérarchique qui devra prendre les dispositions appropriées.

4.2. Utilisation privée résiduelle

1. De manière particulière, par dérogation à l'usage exclusif à des fins professionnelles, toute utilisation du système d'information à des fins personnelles doit être résiduelle, tant dans la fréquence que dans la durée, conformément aux conditions et limites figurant dans la présente charte, et ne doit perturber ni l'activité de l'utilisateur, ni celle d'autres utilisateurs. Dans ce cadre, il appartient à l'utilisateur de procéder au stockage de ses contenus et données à caractère privé dans un répertoire de données nommé « PRIVE ». Tous les messages ne portant pas dans l'objet la mention « PRIVE » sont considérés comme des messages de nature professionnelle.

5. CONDITIONS D'ACCES, ABSENCES ET DEPARTS DE L'UTILISATEUR

5.1. Conditions d'accès

1. Chaque utilisateur reçoit un droit d'accès individuel, personnel et confidentiel qui se matérialise par tout moyen logique ou physique (code utilisateur et mot de passe), et qu'il ne doit pas communiquer à des tiers.
2. L'efficacité d'un mot de passe dépend du nombre de caractères alphanumériques (huit au moins), de son originalité, de son renouvellement régulier par l'utilisateur.
3. Chaque utilisateur doit s'identifier clairement et ne peut utiliser l'identité d'autrui.
4. Ce droit d'accès cesse automatiquement lors d'un départ (l'utilisateur quittant UBIFRANCE) ou lors d'un changement d'affectation (changement de poste, mutation, etc...). UBIFRANCE se réserve le droit de le suspendre s'il est constaté que l'utilisateur a violé l'une des obligations imposées par la présente charte.
5. Le droit d'accès n'est conféré à l'utilisateur qu'aux fins d'une utilisation conforme à son activité professionnelle au sein d'UBIFRANCE et exclut toute autre utilisation.
6. L'utilisateur reconnaît que l'usage de son droit d'accès peut engager sa responsabilité.
7. Il est interdit à un utilisateur d'user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.

8. De même, il est interdit à tout utilisateur d'user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur.

5.2. Gestion des absences

1. Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation du service et telles que définies par la hiérarchie.

2. En cas d'absence de l'utilisateur ce dernier prend les dispositions nécessaires, en concertation avec sa hiérarchie, suivantes :

- délégation au profit d'un autre utilisateur, afin de lui permettre de prendre connaissance des messages qui lui sont adressés ;
- création d'un message automatique d'absence indiquant à l'émetteur du message la durée de son absence et les coordonnées d'un autre utilisateur pouvant être contacté en son absence.

3. En cas d'absence de l'utilisateur, pour quelque raison que ce soit, l'autorité hiérarchique se réserve le droit d'accéder directement aux différents contenus et données et plus généralement à tous documents à caractère professionnel de l'utilisateur, ayant recours en tant que de besoin, aux droits des administrateurs.

4. En cas d'absence prolongée, UBIFRANCE se réserve le droit de suspendre le droit d'usage et/ou d'accès à tout ou partie du système d'information.

5.3. Gestion des départs

1. Lors de son départ d'UBIFRANCE, il appartient à l'utilisateur de remettre l'ensemble des moyens informatiques et de communications électroniques, y inclus les matériels nomades, à la Direction des systèmes d'information dans un bon état de fonctionnement.

2. Par ailleurs, il appartient à l'utilisateur de détruire son répertoire « privé ».

3. Le répertoire « privé » d'un utilisateur quittant UBIFRANCE, s'il n'a pas été détruit par ce dernier, sera supprimé sans copie, ni prise de connaissance préalable du contenu par UBIFRANCE, sauf s'il est présent ou s'il a été dûment informé et sauf en cas de risque ou événement particulier.

4. Le départ d'un utilisateur entraîne la fermeture immédiate de ses comptes utilisateurs, de sa boîte aux lettres, sauf décision contraire de l'autorité hiérarchique de l'utilisateur. Il est de la responsabilité de l'utilisateur de faire suivre ses messages à caractère personnel en communiquant sa nouvelle adresse à ses interlocuteurs.

5. Lors du départ de l'utilisateur, aucun élément ne doit être protégé par un code d'accès ou un mécanisme de protection quelconque.

6. CONFIDENTIALITE ET SECURITE

6.1. Confidentialité

1. Le respect de la confidentialité des données est une exigence essentielle d'UBIFRANCE.

2. La sauvegarde des intérêts d'UBIFRANCE nécessite le respect par tous d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des données.

3. Le respect de cette confidentialité implique notamment de veiller à ce que les tiers non autorisés n'aient pas connaissance de telles données.

4. La transmission de données confidentielles ne peut être réalisée qu'aux conditions suivantes:

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

5. Quelle que soit la nature des données stockées ou transmises par le système d'information d'UBIFRANCE, l'utilisation de procédés de cryptage est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés. Il est interdit d'utiliser des moyens de cryptologie autres que ceux expressément autorisés par la Direction des systèmes d'information.

6.2. Sécurité

1. L'utilisateur doit mettre en œuvre les moyens mis à sa disposition par UBIFRANCE pour préserver la sécurité des données et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

2. En particulier, l'utilisateur veille à verrouiller systématiquement son poste de travail en cas d'absence, même momentanée.

3. Les utilisateurs doivent signaler tout incident de sécurité, toute suspicion de compromission, toute tentative d'intrusion extérieure, de falsification ou de présence de virus à la Direction des systèmes d'information.

4. Tout utilisateur doit éviter l'intrusion de tout fichier ou données (virus, chevaux de troie...) susceptibles de porter atteinte à la confidentialité ou l'intégrité du système d'information, c'est-à-dire :

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'adresse de l'émetteur du message et/ou l'objet du message sont suspects ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la Direction des systèmes d'information.

5. En cas de réception de message non sollicité (spam), l'utilisateur veille à :

- ne pas l'ouvrir sans s'être assuré préalablement de son innocuité ;
- ne pas y répondre ;
- ne pas le transférer ;
- informer la Direction des systèmes d'information ;
- agir sur instruction de cette dernière.

6. L'utilisateur ne doit pas, sauf autorisation préalable et expresse de la Direction des systèmes d'information :

- communiquer à des tiers toute information technique relative au système d'information ;
- modifier les configurations informatiques ;
- établir des connexions à internet par modem ou WiFi ;
- modifier ou supprimer des données, notamment comptables ou financières.

6.3. Secrets particuliers

1. Les règles correspondant à la gestion des secrets spécifiques faisant l'objet d'une organisation particulière s'appliquent à ces informations lorsqu'elles sont mises en œuvre au sein du système d'information et ce, nonobstant l'application de la présente charte.

7. PLAN DE CONTINUITE D'ACTIVITE

1. L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, UBIFRANCE peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.
2. Ces mesures peuvent inclure notamment une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

8. MOBILITE ET MATERIELS MIS A DISPOSITION PAR UBIFRANCE

1. Tout utilisateur qui dispose de matériels nomades est informé des consignes de sécurité particulières et de la procédure à suivre en cas de détérioration, de vol ou de perte de ces matériels.
2. Seuls les matériels nomades autorisés peuvent être connectés aux réseaux d'UBIFRANCE.
3. Les matériels nomades sont mis à la disposition des utilisateurs, selon les procédures définies par la Direction des Systèmes d'Information.
4. Lorsque ces matériels nomades sont utilisés à l'extérieur d'UBIFRANCE, l'utilisateur en assure la garde et la responsabilité.
5. L'utilisation des matériels nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcée.
6. Il doit notamment veiller à ce que des tiers ne puissent prendre possession de ces matériels nomades, les utilisent ou accèdent à leurs contenus ; dans le cas contraire, l'utilisateur doit immédiatement appliquer les consignes définies par la Direction des Systèmes d'Information.

9. OUTILS COLLABORATIFS ET PLATE-FORMES DE COMMUNICATION COLLECTIVES

9.1. Principes

1. La mise en place des outils collaboratifs et plate-formes de communication collectives, notamment blogs, chats, réseaux sociaux, twitters..., ne peut se faire que sur autorisation écrite et préalable de l'autorité hiérarchique.

9.2. Forum

1. L'ouverture d'un forum professionnel interne à UBIFRANCE, d'un thème de "News Group" ou d'une communauté par un utilisateur s'effectue sur demande motivée de l'utilisateur et sur autorisation écrite de sa hiérarchie.
2. Ces forums peuvent faire l'objet d'un contrôle par un modérateur désigné à cet effet.
3. Les messages circulant sur les forums autorisés ne sont pas nécessairement sauvegardés. Il appartient donc à chaque utilisateur de sauvegarder les messages qui lui sont utiles.
4. La participation des utilisateurs à des forums externes à UBIFRANCE est interdite, sauf autorisation expresse de leur hiérarchie.

5. L'utilisateur demeure responsable des messages qu'il rédige.

9.3. Liste de diffusion

1. L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est réservée à un usage strictement professionnel et nécessite l'obtention préalable par l'utilisateur d'une autorisation de sa hiérarchie.
2. En outre, l'utilisateur doit systématiquement vérifier lors de l'inscription qu'il existe une procédure de désabonnement.
3. En cas de création dûment autorisée d'une liste de diffusion pour l'envoi de messages à des tiers, l'utilisateur veille à ne pas faire apparaître aux tiers les adresses nominatives des autres destinataires.

9.4. Logiciel externe

1. Toute installation ou utilisation de logiciels non expressément autorisée par la Direction des systèmes d'information est interdite. L'installation par un utilisateur d'un logiciel est strictement interdite et ce, quel qu'en soit le support.
2. Le fait pour un utilisateur d'installer un logiciel ou progiciel, même gratuit, sans autorisation préalable de sa hiérarchie est interdit et est susceptible d'engager la responsabilité personnelle de l'utilisateur.

9.5. Services hébergés

1. L'utilisation de services hébergés dans le système d'information d'UBIFRANCE est interdite sauf autorisation de la Direction des systèmes d'information.

10. DONNEES A CARACTERE PERSONNEL

10.1. Devoirs des utilisateurs

1. Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitement automatisé ou non de données à caractère personnel.
2. Tout traitement de données à caractère personnel doit faire l'objet de formalités préalables, sauf dérogations légales ou réglementaires. Dans ce cadre, l'utilisateur doit respecter les finalités des traitements de données à caractère personnel objet des formalités préalables susvisées.
3. Les principes directeurs à respecter sont :
 - la pertinence et l'exactitude des données au regard des finalités poursuivies ;
 - le consentement individuel à la collecte des données ;
 - le droit d'accès, de rectification et d'opposition ;
 - la protection adaptée aux risques présentés par le traitement sur les plans technique et organisationnel.
4. L'utilisateur veille, en cas d'opération de prospection directe par courrier électronique à respecter les dispositions légales et réglementaires en vigueur.

10.2. Droits des utilisateurs

1. UBIFRANCE s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite.
2. Les traitements opérés dans le cadre de la présente charte ont pour finalités :

- le suivi et la maintenance du système d'information ;
- la gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux ;
- la gestion de la messagerie électronique professionnelle ;
- le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation et de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;
- la sécurité du système d'information ;
- le respect de la présente charte.

3. Conformément à la loi « Informatique et Libertés », les utilisateurs sont informés qu'ils disposent d'un droit d'accès, de rectification et d'opposition, pour motif légitime, relatif à l'ensemble des informations à caractère personnel les concernant, qui s'exerce auprès de la Direction des ressources humaines s'agissant des salariés, stagiaires ou intérimaires, et du cas spécifique des volontaires internationaux ou de la Direction administrative et financière dans tous les autres cas et notamment s'agissant des prestataires extérieurs.

11. PROPRIETE

1. L'utilisation du système d'information d'UBIFRANCE implique le respect des droits de propriété intellectuelle et notamment de la réglementation relative à la propriété littéraire et artistique.

2. En conséquence, chaque utilisateur doit :

- utiliser les logiciels, applications, dans les conditions de la licence souscrite par UBIFRANCE ;
- ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels UBIFRANCE ne posséderait pas un droit d'usage ;
- ne pas reproduire et utiliser les bases de données, pages web ou autres créations de UBIFRANCE ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet ;
- ne pas copier et remettre à des tiers des créations appartenant à des tiers ou à UBIFRANCE sans s'assurer de l'autorisation du titulaire des droits qui s'y rapporte. Chaque utilisateur ne peut effectuer une copie d'œuvre protégée par le droit d'auteur que pour autant que celle-ci soit accessible sans restriction d'usage et que la copie qu'il en effectue ne soit destinée qu'à son usage strictement personnel.

3. L'installation d'un logiciel est subordonnée à l'accord de la Direction des systèmes d'information après validation de l'autorité hiérarchique de l'utilisateur et mise en œuvre par la DSI.

12. CONTROLE DU SYSTEME D'INFORMATION

12.1. Principes directeurs

1. La Direction des systèmes d'information a la charge de la qualité et de la sécurité du système d'information fournis aux utilisateurs.

2. Tout intervenant de la Direction des systèmes d'information doit impérativement respecter la confidentialité des données et de toutes informations auxquelles il peut avoir accès dans le cadre de son activité.

3. Des contrôles sont mis en place, au titre de surveillance générale ou d'enquêtes, dans le respect de la législation en vigueur, afin :

- d'assurer le bon fonctionnement et la sécurité du système d'information ;
- d'empêcher l'utilisation du système d'information dans un cadre non conforme aux règles définies dans la présente charte et les réglementations en vigueur.

12.2. Contrôle du système d'information

1. Les personnels de la Direction des systèmes d'information, dûment mandatés pour mener ces démarches, garderont confidentielles les informations qu'ils pourraient être amenés à connaître à cette occasion.

2. A ce titre, les utilisateurs sont informés que les administrateurs qui doivent veiller au fonctionnement normal et à la sécurité des réseaux et systèmes informatiques sont conduits, de par leur fonctions, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexion à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

3. Néanmoins, ces administrateurs sont tenus à une obligation de discrétion et ne peuvent utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

4. La Direction des systèmes d'information, dûment mandatée par le chef de département ou le directeur ou le directeur pays d'une part et la Direction des ressources humaines d'autre part, possède le droit de contrôler le système d'information dans le détail, y compris la session de travail d'un utilisateur, afin de vérifier que ce dernier respecte les clauses définies dans la présente charte.

5. UBIFRANCE se réserve notamment le droit :

- de vérifier le trafic informatique entrant et sortant d'UBIFRANCE, ainsi que le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées à l'égard du système d'information ;
- de contrôler l'origine licite des logiciels installés ;
- de filtrer les adresses électroniques (URL) des sites non autorisés par UBIFRANCE ;
- de conserver des fichiers de journalisation des traces de connexion globales ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

6. En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité d'UBIFRANCE en ne respectant pas les règles instituées par la présente charte, la Direction des systèmes d'information fournit à la Direction des ressources humaines, sur sa demande écrite et motivée, les traces individuelles des connexions incriminées.

7. En outre, en cas d'incident, UBIFRANCE se réserve le droit de :

- surveiller le contenu des informations qui transitent sur le système d'information d'UBIFRANCE ;
- vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;
- procéder à toutes copies utiles à faire valoir les droits d'UBIFRANCE.

8. La Direction des systèmes d'information exerce un contrôle du système d'information sur les durées de connexion, les sites les plus visités dans le cadre de la mission de protection des systèmes informatiques. En cas de perturbation, induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, la Direction des systèmes d'information est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

9. En cas de non-respect de la présente charte par un utilisateur, la Direction des systèmes d'information se verra dans l'obligation d'avertir la hiérarchie de l'utilisateur pour que celle-ci décide de la suite à donner.

10. Suivant la gravité des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus temporairement ou définitivement.

11. Tout logiciel installé illicitement ou tout fichier suspect sera supprimé par les intervenants de la Direction des systèmes d'information dès le constat de leur présence sur le poste de travail.

12.3. Contrôle de la messagerie

1. Des contrôles peuvent être réalisés sur l'usage de la messagerie. Ils peuvent porter en particulier sur :

- les volumes / le nombre de messages échangés ;
- les tailles des messages ;
- le format des pièces jointes (images, vidéos, exécutable, fichiers compressés, etc.) ;
- la quantité d'espace disque utilisée ;
- une analyse des messages (sélection de mots à caractère pornographique, raciste, etc.).

2. La Direction des systèmes d'information s'engage à ne pas prendre connaissance des messages que l'utilisateur pourrait avoir envoyés ou reçus lorsqu'il s'agit de correspondances à caractère privé, sauf dans les cas où l'utilisateur est présent ou a été dûment appelé. Dans ces cas, une liste récapitulant les messages ouverts par adresse (expéditeur, destinataire), par date, et le cas échéant, par titre sera établie et signée par l'utilisateur.

3. Toutefois, en cas de risque ou événement particulier, la Direction des systèmes d'information pourra ouvrir les fichiers privés de l'utilisateur en son absence.

12.4. Contrôle des consommations de téléphonie fixe et mobile

1. De la même manière que l'usage du système d'information, l'utilisation du téléphone à des fins personnelles doit être résiduelle, tant dans la fréquence que dans la durée, conformément aux conditions et limites figurant dans la présente charte, et ne doit perturber ni l'activité de l'utilisateur, ni celles d'autres utilisateurs. En cas de consommation excessive et non justifiée, UBIFRANCE se réserve le droit de refacturer tout ou partie du coût lié à cette consommation.

2. Sauf autorisation préalable expresse, les numéros taxés ou surtaxés ne doivent pas être utilisés.

3. Pour la bonne gestion de ces ressources, un autocommutateur enregistre, à partir de chacun des postes téléphoniques, les éléments de la communication (date, heure, durée, coût et les six premiers chiffres des numéros appelés).

4. Tant pour la téléphonie fixe que mobile, des consultations ponctuelles des données enregistrées peuvent être faites en cas de consommation anormale ou abusive, ainsi qu'aux fins d'établir des statistiques utiles à l'analyse des besoins.

5. Dans un souci de préservation de la confidentialité de leurs communications et plus généralement de l'exercice de leurs mandats, les lignes téléphoniques mises à disposition des

représentants du personnel dans les locaux qui leur sont réservés ne sont pas connectées à l'autocommutateur.

13. SAUVEGARDE ET ARCHIVAGE

13.1. Données

1. L'utilisateur doit stocker ses fichiers et données électroniques dans des espaces définis par la Direction des systèmes d'information.
2. La sauvegarde des données locales résidentes sur le disque dur local du poste de travail est à la charge de l'utilisateur. Les moyens d'archivage locaux peuvent également être utilisés à cette fin.

13.2. Messages électroniques

1. Les messages échangés à l'intérieur et à l'extérieur d'UBIFRANCE sont sauvegardés afin d'assurer la continuité du service.

13.3. Données techniques

1. Les données de connexion sont conservées conformément à la réglementation en vigueur.

13.4. Archivage

1. L'archivage des données est effectué conformément à la réglementation applicable ainsi qu'à la politique d'archivage d'UBIFRANCE.

14. SANCTIONS

1. Sera passible d'une sanction disciplinaire prévue au règlement intérieur tout utilisateur qui n'aura pas respecté la présente charte par son comportement et ses agissements fautifs, ainsi que par toute abstention ou insuffisance délibérée, qui aura abusé de la tolérance accordée ou qui se sera personnellement livré à des activités contraires à la probité, aux bonnes mœurs ou à des dispositions pénales.
2. Les sanctions qui seraient prises par l'employeur ne sont pas exclusives d'éventuelles poursuites judiciaires à l'encontre des intéressés.

15. ENTREE EN VIGUEUR

1. La présente charte entrera en vigueur un mois après l'accomplissement des formalités de communication à l'Inspection du travail, de dépôt et de publicité telles que prévues à l'article L 1321-4 du code du travail, soit le 7 décembre 2009
2. Toute modification ultérieure, adjonction ou retrait de clause de la présente charte seront soumis à la même procédure, conformément aux prescriptions de l'article L 1321-4 du code du travail, étant entendu que toute clause de la charte qui deviendrait contraire aux dispositions légales, réglementaires ou conventionnelles applicables à UBIFRANCE du fait de l'évolution de ces dernières, serait nulle de plein droit.