

Préambule

D-SINE AFRICA met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique physique et virtuelle, ainsi que des équipements informatiques fixes et mobiles.

Les utilisateurs/ chercheurs, dans l'exercice de leurs fonctions, sont conduits à accéder et à utiliser lesdits équipements informatiques, ainsi que les systèmes d'information de communication et collecte des données (REDCAP) mis à leur disposition.

L'utilisation du système d'information, de communication et de collecte des données (REDCAP) doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Par ailleurs, des tiers au D-SINE AFRICA (utilisateurs, prestataires externes, partenaires...) peuvent également avoir accès aux équipements informatiques et aux systèmes d'information et de communication de D-SINE AFRICA.

Or, l'utilisation d'équipements informatiques (hardware et software), de réseaux de communication et du système d'information fait peser un risque pour D-SINE AFRICA concernant le fonctionnement, la sécurité et l'intégrité de son système d'information et de communication, mais également concernant les données (à caractère personnel ou non, sensibles ou non) qui sont traitées dans le cadre de l'activité de D-SINE AFRICA.

Aussi, dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et des équipements informatiques, la présente charte pose des règles relatives à l'utilisation de ces ressources et ce notamment dans le respect des règles spécifiques aux professionnels de santé, de la recherche, ect

Cette charte a pour objectifs :

- de sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer ;
- d'informer les utilisateurs sur :
 - les usages permis des moyens informatiques mis à sa disposition ;
 - les règles de sécurité en vigueur ;
 - les mesures de contrôle prises par D-SINE AFRICA ;
 - les sanctions éventuellement encourues par les utilisateurs ;
- de formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

Ces règles s'inscrivent dans une démarche responsable afin de protéger d'une part le patrimoine informationnel et l'image de marque de D-SINE AFRICA, et d'autre part les libertés et la vie privée des personnes concernées que sont les utilisateurs et chercheur de D-SINE AFRICA et les tiers en lien avec les D-SINE AFRICA (utilisateurs suivis, prestataires externes, partenaires...).

Le Responsable des systèmes d'information (RSI) ou le Directeur des systèmes d'information (DSI), la Direction Générale (DG) et le Délégué à la protection des données personnelles (DPD) ou le DPO (Data Protection Officer) se tiennent à la disposition des utilisateurs qui souhaiteraient disposer d'informations ou de conseils complémentaires relatifs à l'usage des systèmes d'information et des équipements informatiques.

D-SINE AFRICA peut en outre identifier un Responsable des traitements au sein de la structure.

Définitions

« Equipements informatiques » : désigne l'ensemble des matériels, équipements, outils informatiques mis à disposition par le D-SINE AFRICA aux Utilisateurs. (Laptops, tablettes telephone disques amovibles clés USB ect...)

« Personnes concernées » : désigne les personnes physiques dont les données à caractère personnel sont traitées par D-SINE AFRICA ou par tout tiers via le système d'information, de communication et de collecte des données (REDCAP) de D-SINE AFRICA, ou via des Equipements informatiques.

« Utilisateurs » : désigne toute personne qui utilise les systèmes d'information du D-SINE AFRICA et les Equipements informatiques quel que soit son statut, et notamment les mandataires sociaux, les utilisateurs, les intérimaires, les stagiaires, les employés de sociétés prestataires, les visiteurs occasionnels, les utilisateurs suivis et de manière générale, à toute personne qui a obtenu un droit d'utilisation du système d'information du D-SINE AFRICA ou de ses Equipements informatiques.

Champ d'application

Personnes visées au sein de D-SINE AFRICA

Les obligations décrites dans la présente charte s'appliquent à toute personne qui utilise les systèmes d'information de D-SINE AFRICA. Il en est ainsi, notamment, des utilisateurs de D-SINE AFRICA, des stagiaires, des intérimaires, et de manière générale, de tout utilisateur ayant obtenu des droits personnels d'utilisation

La présente charte devra être annexée au contrat de prestations conclus avec des tiers concernant l'informatique.

Accès par des tiers aux systèmes d'information de D-SINE AFRICA

Tout utilisateur extérieur à D-SINE AFRICA ne peut avoir accès aux systèmes d'information de D-SINE AFRICA que moyennant une autorisation expresse préalable délivrée par la Hierarchie et s'engage, dès lors, à respecter l'ensemble des dispositions de la présente charte.

Moyens informatiques et de communication électronique concernés

La présente charte concerne l'ensemble des moyens informatiques et de communication électronique qui sont mis à la disposition des utilisateurs à des fins professionnelles exclusivement, ainsi que l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.

Les systèmes d'information et de communication et de collecte des données (REDCAP) de D-SINE AFRICA sont notamment constitués des éléments suivants :

- ordinateurs portables ou fixes,
- périphériques (y compris clés USB),
- réseaux informatiques (serveurs (Cloud), routeurs, connecteurs, bornes WIFI),
- photocopieurs,
- téléphones (fixes et portables) et smartphones,
- tablettes électroniques,
- logiciels,
- fichiers informatiques et bases de données,
- espaces de stockage individual,
- messagerie,
- connexions internet, intranet, extranet.

Dérogations possibles

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit au responsable des systèmes d'information (RSI). La décision finale est ensuite prise en concertation avec la hiérarchie qui se réserve le droit d'accepter ou de refuser les demandes de dérogation.

Utilisation des Systèmes d'Information et des outils de communication

Accès

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

Chaque utilisateur reçoit par SMS un droit d'accès individuel qui se matérialise par tout moyen logique ou physique (code utilisateur et mot de passe,).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'accès des utilisateurs. Ils ne doivent être communiqués à personne, ni au responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par le Responsable du Système d'information (RSI).

L'utilisateur s'engage à respecter les considérations d'efficacité d'un mot de passe, laquelle dépend du nombre de caractères alphanumériques (X caractères au moins, et autres spécificités....), de son originalité, de son renouvellement régulier par l'utilisateur (tous les Y mois,...).

Chaque utilisateur doit s'identifier personnellement et ne peut utiliser l'identité d'autrui (même avec l'accord de ce dernier).

Ce droit d'accès cesse automatiquement lors d'un départ ou à la fin d'un Projet (l'utilisateur quittant D-SINE AFRICA) et peut être modifié lors d'un changement d'affectation (changement de poste, mutation, etc.) ou s'il est constaté que l'utilisateur a enfreint l'une des obligations imposées par la présente charte.

La messagerie électronique :

▪ Principes généraux

Chaque Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le Responsable du Système d'information (RSI)

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam.

Les utilisateurs sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de

messages non sollicités et de ne pas engager la responsabilité civile ou pénale de D-SINE AFRICA et/ou de l'utilisateur.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie pendant une durée maximale de **2 an(s)**. Une limitation de la taille des messageries électroniques est mise en œuvre afin d'inciter l'utilisateur à réaliser un tri des messages régulièrement. Passé ce délai, ils sont automatiquement supprimés. Si l'utilisateur souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l'aide du Responsable du Système d'information (RSI) si nécessaire.

▪ **Envoi de messages électroniques**

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, de données à caractère personnel ou de données sensibles, ces vérifications doivent être renforcées ; en cas de besoin, un cryptage des messages pourra être aussi proposé par la direction informatique.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent dans ce cas être cryptés, conformément aux recommandations du responsable des systèmes d'information.

Les messages importants doivent être envoyés avec un accusé de réception ou signés électroniquement.

La forme des messages professionnels doit respecter les règles définies par la hiérarchie, pour ce qui concerne la mise en forme et surtout la signature des messages.

La signature des courriers électroniques fait l'objet d'une forme standardisée. Chaque utilisateur s'engage à respecter cette forme en évitant tout élément complémentaire.

▪ **Réception de messages électroniques**

L'utilisateur ne doit pas ouvrir, ni répondre à des messages électroniques tels que spam, messages électroniques répétés, ni les transférer lorsque ceux-ci sont reçus à son insu sur leur messagerie électronique professionnelle et ne présentent aucun rapport avec ses fonctions et ses attributions au sein de D-SINE AFRICA. Il s'engage, dans pareil cas, à les détruire immédiatement et à avertir le responsable des systèmes d'information en cas d'abus manifeste de fréquence ou de volume.

▪ **Absences de l'utilisateur**

L'utilisateur est informé et accepte qu'en cas d'absence prolongée ou pour la continuité des services, la direction des systèmes d'information se réserve le droit d'accéder à sa messagerie et à ses dossiers professionnels, et ce sans son consentement préalable.

En cas d'absence, l'utilisateur devra activer la fonction de délégation ou de notification d'absence afin de prévenir toute discontinuité dans le traitement des messages et permettre à ses interlocuteurs de prendre des mesures appropriées.

En cas d'urgence ou pour des raisons liées au besoin de maintenir un niveau de qualité de service, D-SINE AFRICA peut procéder à la destruction ou réinitialiser les codes d'accès d'un utilisateur.

La messagerie électronique de l'utilisateur est conservée sur le serveur de D-SINE AFRICA pendant une durée déterminée par le responsable des systèmes d'information.

▪ **Utilisation personnelle**

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention "Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon.

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso".

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

Internet / Intranet

Dans le cadre de leur activité, les utilisateurs doivent avoir accès à Internet.

Le Responsable du Système d'information (RSI), pour des raisons de sécurité, peut limiter ou prohiber l'accès à certains sites. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite ou autorisée sous réserve d'autorisation préalable du responsable des systèmes d'information. Un tel mode d'expression est susceptible d'engager la responsabilité du D-SINE AFRICA, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de D-SINE AFRICA, y compris sur Internet.

Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée.

En particulier, sont interdits :

- l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives.
- la création ou la mise à jour au moyen de l'infrastructure de D-SINE AFRICA tout site Internet, notamment des pages personnelles.
- la connexion à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'organisaton, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de D-SINE AFRICA ou engageant financièrement celle-ci.

La cessation de l'utilisation

Lors de son départ de D-SINE AFRICA, l'utilisateur doit respecter la procédure de départ et remettre l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis (ordinateur, périphériques, mobile, carte d'accès, moyen d'authentification à distance, badges, supports de stockage, etc.) en bon état

général de fonctionnement et ne conserver aucun matériel ou aucune donnée permettant d'accéder au système d'information. De plus, l'utilisateur s'interdit, avant son départ, de détruire des informations et des données professionnelles.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder [trois mois], le compte messagerie de l'utilisateur est supprimé le jour de son départ.

Dans le cas où le compte messagerie est toujours actif, même après le départ d'un utilisateur, une redirection des messages peut être mise en place par D-SINE AFRICA vers l'utilisateur ayant repris le poste de l'utilisateur ayant quitté D-SINE AFRICA ou toute autre personne occupant une fonction similaire. Ses identifiants sont également désactivés.

Sauf dérogation accordée au cas par cas par le responsable des systèmes d'information et qui ne peut en aucun cas excéder une durée de [trois mois], les éléments marqués « privé »

ou « personnel » doivent être supprimés par l'utilisateur au plus tard la veille de son départ de D-SINE AFRICA.

Accès au Système d'Information en dehors du Service (télétravail, en entreprise, centre mobile, ... accès au bureau distant)

Le présent article concerne l'utilisation des systèmes d'information de D-SINE AFRICA, de ses ressources, et des moyens de communication par l'utilisateur lorsque celui-ci est situé en-dehors du site physique de D-SINE AFRICA.

En premier lieu, il convient de préciser que l'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d'information de communication et de collecte des données (REDCAP) de D-SINE AFRICA à distance.

Par ailleurs, il est impératif que l'utilisateur informe préalablement le RSI des accès à distance qu'il mettra en place, afin d'en obtenir préalablement l'autorisation et que lui soient communiquées les consignes de sécurité et de confidentialité propres à sa situation.

D-SINE AFRICA veille à souscrire aux assurances nécessaires pour la protection des moyens informatiques et de communication électronique mis à disposition.

Tout accès à distance par du matériel informatique personnel est interdit sauf autorisation expresse et écrite de la part du Responsable du Système d'information (RSI).

Utilisation professionnelle

Les systèmes d'information mis à disposition des utilisateurs sont réservés à un usage professionnel exclusif. Tout usage des moyens informatiques et de communication électronique est réputé avoir été réalisé par le bénéficiaire de l'identification d'accès, ce à des fins professionnelles.

Par ailleurs et indépendamment des dérogations possibles précitées, une utilisation des systèmes d'information à des fins personnelles peut être résiduelle. Ainsi, tant dans la fréquence que dans la durée, elle ne peut être envisagée qu'en dehors du temps de travail et de manière limitée pendant le temps de travail, conformément à la Jurisprudence en la matière.

Les répertoires informatiques et échanges électroniques doivent alors porter la mention « privé » ou « personnel ». L'employeur se réserve le droit de limiter ou suspendre une telle utilisation, en cas d'abus.

Secret et confidentialité – transmission d'informations

Le respect de la confidentialité des données est une exigence essentielle.

La sauvegarde des intérêts du D-SINE AFRICA nécessite le respect d'une obligation générale et permanente de confidentialité et de secret professionnel, à l'égard des données disponibles mis à la disposition de l'utilisateur pour l'exercice de son activité professionnelle dans le cadre notamment de l'utilisation des systèmes d'information, mais aussi de tout traitement.

En conséquence, l'utilisateur s'engage au respect de la présente charte, comme des textes en vigueur et notamment à veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations, conformément aux règles d'éthique professionnelle ou de déontologie, le cas échéant.

Il est interdit d'utiliser des moyens de cryptologie autres que ceux expressément autorisés par D-SINE AFRICA.

Les administrateurs des systèmes informatiques sont tenus au secret professionnel et ils ne doivent pas divulguer des informations ayant un caractère nominatif, de quelque nature qu'elles soient et ce, quel que soit l'ordre hiérarchique. En aucun cas, les administrateurs ne sont contraints de divulguer ces informations sauf disposition réglementaire particulière en ce sens. En cas de non-respect de ces dispositions par les administrateurs, ceux-ci s'exposent à des sanctions indépendamment des circonstances susceptibles d'engager leur responsabilité.

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.

D-SINE AFRICA se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie, le droit d'accès de toute personne pour des raisons liées directement à la continuité et la sécurité des services.

Sécurité générale

Règles à respecter

▪ **Principes généraux**

Du fait de la collecte de données et du traitement de celles-ci réalisés, le D-SINE AFRICA s'engage, dans le cadre des dispositions légales et réglementaires qui s'imposent à mettre en œuvre toutes les mesures organisationnelles et techniques utiles afin de préserver la sécurité, l'intégrité et la confidentialité des Données, ainsi que la sécurité de son système d'information et de communication, sur le plan technologique et procédural, afin notamment d'empêcher toute modification, tout transfert et toute suppression non-autorisés des Données, et toute intrusion non-autorisée dans son système d'information ou son endommagement.

Toutefois, le premier risque reste le risque humain lié aux traitements et aux manipulations des Données par les Utilisateurs, et par l'utilisation par ces derniers du système d'information et de communication et des outils qui y sont liés.

Par conséquent, la mise en place d'outils de sécurité ne doit pas dispenser les utilisateurs de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au responsable des systèmes d'information.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le système d'information de D-SINE AFRICA.

▪ **Obligations de l'utilisateur**

L'utilisateur s'engage de respecter à

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ;
- détruire les messages du type « chaîne de solidarité » ;
- ne pas stocker et router des gadgets reçus ou trouvés sur Internet ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir /e responsable des systèmes d'information.
- modifier la configuration de son poste de travail informatique effectuée par la direction des systèmes d'information, que ce soit par adjonction, suppression ou modification, sauf exception après accord exprès de cette dernière ;
- mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage;
- utiliser [même avec leur accord) ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- ne pas sortir les Equipements informatiques de D-SINE AFRICA en dehors du site de D-SINE AFRICA, sauf accord du responsable du système d'information;
- ne pas télécharger de fichiers, en particulier médias, sans rapport avec l'activité professionnelle ou présentant un risque pour le système d'information ;

L'utilisateur est tenu **d'informer** sans délai sa hiérarchie de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication électronique.

Toute installation ou utilisation de logiciels non expressément autorisée par le responsable des systèmes d'information est interdite.

Dans le cadre de ses déplacements professionnels, peu importe leur durée ou leur fréquence, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information qu'il pourrait être amené à accéder, manipuler ou échanger.

En particulier, il est déconseillé d'utiliser les systèmes de connexion wifi dans les lieux publics.

Modalités de contrôle des systèmes d'information

L'utilisateur est informé que D-SINE AFRICA met en place des outils de traçabilité et de filtrage d'utilisation des systèmes d'information et de communication.

D-SINE AFRICA met en place :

- les journaux de connexion de l'ensemble des systèmes d'information ;
- des outils de filtrage notamment des contenus et des adresses Internet permettant d'analyser les conditions d'utilisation et d'interdire éventuellement tel ou tel protocole, ou encore de restreindre ou d'interdire l'accès à Internet ou à certaines catégories de sites Internet.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

L'utilisateur est informé que le responsable des systèmes d'information (qui doit veiller au fonctionnement normal et à la sécurité des réseaux et systèmes informatiques) est conduit

de par ses 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 leurs postes de travail

mais demeure soumis aux règles encadrant le secret professionnel le responsable des systèmes d'information dûment mandatée par le directeur peut contrôler les systèmes d'information, afin de vérifier que ce dernier respecte les clauses définies dans la présente charte.

En cas de suspicion de manquement grave aux dispositions de la présente charte, la direction pourra procéder à toutes les mesures d'investigation utile, dans le respect des règles en vigueur.

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

Le caractère « non professionnel » des répertoires informatiques clairement identifiés comme « privé » ou « personnel », ne fait pas obstacle à des modalités de contrôle dans les conditions précitées.

■ **Informations complémentaires**

L'utilisation des systèmes d'information implique le respect des droits de propriété intellectuelle de l'entreprise, de ses partenaires et, de tout tiers titulaire de tels droits. Dans le doute, l'utilisateur devra contacter le responsable des systèmes d'information.

Chaque utilisateur autorisé s'engage à :

- utiliser les progiciels dans les conditions de la licence souscrite ;
- ne pas reproduire ou utiliser les progiciels, bases de données, page web ou autre création protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits
- ne pas copier ou diffuser de textes, d'images, de photographies, d'œuvres musicales, audiovisuelles ou toute création copiée sur le réseau Internet.

L'utilisateur est informé que la contrefaçon est un délit passible de sanctions civiles et pénales.

La présente charte est communiquée individuellement à chaque salarié par voie électronique.

Le RSI peut fournir aux utilisateurs toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde, de sécurité et sur les droits des Personnes Concernées.

Il les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par le RSI ou DSI dans le cadre de la présente charte.

En cas de besoin, les utilisateurs pourront être formés par le RSI pour appliquer les règles d'utilisation du système d'information et de communication prévues.

Sanctions

Il est rappelé que la présente charte est document à portée juridique, et donc contraignante pour les Utilisateurs.

En effet, le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.

D-SINE AFRICA se réserve également le droit d'engager ou de faire engager des poursuites pénales et/ou civiles, indépendamment des sanctions disciplinaires mises en œuvre, notamment mais pas limitativement en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

Le responsable des systèmes d'information peut effacer ou isoler et conserver aux fins de preuve toute trace de logiciels, progiciels, programmes ou fichiers créés ou introduits dans le système d'Information de D-SINE AFRICA, en violation des droits des tiers, notamment de propriété intellectuelle, et dénoncer tout acte délictueux aux autorités, sans préjudice de l'application de sanctions dans le cadre de son statut.