

Charte Utilisateurs

Sur le bon usage des outils numériques du Groupe



TABLE DES MATIÈRES

INTRODUCTION	4
1 CHAMP D'APPLICATION DE LA CHARTE.....	5
1.1 Définition du système d'information.....	5
1.2 Définition de l'Utilisateur	5
1.3 Définition d'outil professionnel.....	5
1.4 Définition d'outil numérique personnel.....	5
2 CONDITIONS D'USAGE DES OUTILS INFORMATIQUES.....	6
2.1 Responsabilité	6
2.2 Accessibilité.....	6
2.3 Usage pour des besoins privés du SI du Groupe	6
2.4 Accès au SI du Groupe à travers des moyens privés	7
2.5 Le respect du droit de propriété.....	7
2.6 Probité	8
3 RÈGLES GÉNÉRALES DE SÉCURITÉ	8
4 RÈGLES DE COMMUNICATION NUMÉRIQUE	9
4.1 Usage des services Internet et Intranet.....	9
4.2 Usage de la messagerie électronique.....	10
4.2.1 Règles générales d'usage de la messagerie électronique.....	10
4.2.2 Usage de la messagerie électronique et vie privée.....	11
4.2.3 Sauvegarde du contenu de la messagerie électronique.....	11
4.2.4 Absence de l'utilisateur	11
4.2.5 Accès à la messagerie de l'Utilisateur après un départ définitif	12
4.2.6 Messagerie électronique et délégations de signature	12
4.3 Le nomadisme	12
4.4 Les moyens de communication par visio-conférence	12
5 PROTECTION DES DONNÉES PERSONNELLES	13
5.1 Respect des règles de protection des données personnelles	13
5.2 Données personnelles sur les Utilisateurs du SI du Groupe.....	14
6 ANALYSE ET CONTRÔLE DE L'UTILISATION DU SI	14
6.1 Contrôles de l'utilisation des outils professionnels.....	14
6.2 Le système automatique de filtrage	15
6.3 Accès aux postes de travail par le PSU	15

7	DU BON USAGE DU SYSTÈME D'INFORMATION	15
7.1	Généralités	15
7.2	Arrivants, mobilités et départs	15
7.3	Dossiers réseaux	16
7.3.1	Dossiers partagés	16
7.3.2	Dossier dit « personnel »	16
7.4	Poste de travail	17
7.5	Impressions et imprimantes	17
7.6	Applications et logiciels	17
7.7	Responsabilité environnementale	18
7.8	Équipements liés à la fonction	18
7.9	Archivage et continuité d'activité	18
8	OBLIGATIONS DES UTILISATEURS	18
9	DÉONTOLOGIE DES ADMINISTRATEURS DU SI	19
10	PORTÉE DISCIPLINAIRE DE LA CHARTE	19
11	ANNEXE I : LES DISPOSITIFS DE SÉCURITÉ DU SI DU GROUPE	20
11.1	Pour la connexion nomade :	20
11.2	Pour le chiffrement des postes de travail :	20
11.3	La protection des postes de travail :	20
11.4	La sensibilisation des Utilisateurs :	21
12	ANNEXE II : LE CHOIX D'UN MOT DE PASSE	22

INTRODUCTION

L'utilisation des outils informatiques, logiciels et matériels, reliés au réseau informatique du Groupe suppose le respect des règles assurant la sécurité du système d'information. Ces règles sont mises en œuvre dans le cadre des règlements en vigueur, du règlement intérieur et des règles de sécurité internes au Groupe (Politique de Sécurité des Systèmes d'Information ou PSSI, publiée au MOP sous la référence CIR-R0054 et Politique de confidentialité de l'information, publiée au MOP sous la référence cir-R8006).

Dans ce contexte, la présente charte définit les droits et obligations des Utilisateurs du système d'information du Groupe. Elle a notamment pour objet de :

- protéger le patrimoine du Groupe,
- rappeler la responsabilité et les droits des Utilisateurs face à la réglementation et aux règles en vigueur,
- rappeler les bons usages d'utilisation du SI, sur lesquels repose le bon fonctionnement général du Groupe.

Les garanties dont bénéficie chacun des salariés du Groupe en matière de droit à la déconnexion font l'objet d'une Charte dédiée. L'application du présent document est mise en œuvre dans le respect des dispositions de cette Charte du droit à la déconnexion afin d'assurer le respect de l'équilibre entre vie personnelle et vie professionnelle.

Des dispositions spécifiques concernant l'utilisation de la messagerie professionnelle par les organisations syndicales sont prévues par accord distinct (cf. accord sur le fonctionnement du CSE)

1 CHAMP D'APPLICATION DE LA CHARTE

Les obligations définies dans cette charte s'appliquent à tout accès au système d'information, aussi bien depuis les locaux du Groupe qu'à distance (au moyen de l'informatique « nomade » : assistants personnels, ordinateurs portables professionnels ou non, smartphones professionnels et personnels avec accès aux applications professionnelles du Groupe via le container sécurisé, ...). Elle encadre aussi l'utilisation de toute technologie pouvant être déployée à l'avenir sur le système d'information du Groupe.

La charte d'utilisation du SI est d'application obligatoire : les règles décrites dans ce document s'imposent à tous les Utilisateurs du SI du Groupe, quels que soient leur statut et leur situation géographique. **La présente Charte constitue une adjonction au règlement intérieur de l'AFD.**

Le respect de la présente charte doit être également une exigence contractuelle vis-à-vis de tout tiers autorisé à accéder au SI du Groupe.

1.1 Définition du système d'information

On entend par système d'information le matériel informatique, les logiciels, les réseaux de communication, les données papier et les informations numériques pouvant être directement ou indirectement utilisés par les Utilisateurs.

1.2 Définition de l'Utilisateur

On entend par Utilisateur toute personne ayant accès aux ressources du système d'information du Groupe, quelle que soit la nature du lien contractuel ou conventionnel qui la lie à ce dernier. De manière plus générale, toute personne qui se sert, de façon permanente ou temporaire, des outils informatiques du Groupe est soumise à cette charte.

1.3 Définition d'outil professionnel

On entend par outil professionnel, tout objet ou logiciel mis à disposition d'un Utilisateur par le Groupe. Cette mise à disposition peut être physique (attribution d'un ordinateur, d'un téléphone ...) ou numérique (accès au système d'information via Internet par exemple).

1.4 Définition d'outil numérique personnel

On entend par outil numérique personnel, tout objet numérique propriété d'un Utilisateur, destiné à ses usages personnels et dont l'administration n'est pas effectuée par le Groupe.

2 CONDITIONS D'USAGE DES OUTILS INFORMATIQUES

2.1 Responsabilité

Les outils informatiques sont mis à la disposition des Utilisateurs pour un usage professionnel, conformément aux besoins liés à leur mission et à leur emploi tels que définis par le Groupe. Ils ne doivent pas être détournés à des fins personnelles, sauf tolérance d'usage.

Tout Utilisateur est responsable de l'usage qu'il fait des ressources du système d'information et doit respecter la réglementation et les règles internes en vigueur.

2.2 Accessibilité

L'accès aux ressources du SI du Groupe est soumis à autorisation. Cette dernière est strictement personnelle et peut être retirée à tout moment. Des droits d'accès sont modifiés ou supprimés en cas de changement de fonction ou de cessation, même provisoire, d'activité.

L'accès sans autorisation à un système d'information privé, tel que celui du Groupe, constitue un délit.

2.3 Usage pour des besoins privés du SI du Groupe

Un usage privé des outils professionnels mis à la disposition des Utilisateurs est toléré, s'il ne nuit pas au bon fonctionnement du SI. Toutefois, **toute information présente sur le SI du Groupe est réputée liée à son activité**, à l'exclusion des données explicitement désignées par l'Utilisateur comme relevant de sa vie privée. Ceci est aussi applicable aux smartphones professionnels fournis par le Groupe.

Il appartient à l'Utilisateur de procéder au stockage éventuel de ses données à caractère privé dans un espace créé par ses propres soins **explicitement** prévu à cet effet (espace dénommé « privé » ou « personnel »). **Le Groupe ne peut être tenue responsable de la pérennité du stockage de ces informations.**

Ces données strictement privées **ne peuvent être stockées sur les emplacements disques présents sur le réseau (les dossiers partagés) que de façon limitée et transitoire**. Seul le stockage local peut être utilisé pour conserver de façon pérenne des données privées. Ceci s'applique aux postes de travail comme aux smartphone professionnels.

Le Groupe s'engage à ne pas visualiser les données clairement identifiées comme « personnelles » ou « privées » sur les espaces. Les fichiers et dossiers ainsi désignés pourront par conséquent uniquement être consultés en présence de l'Utilisateur ou celui-ci dûment appelé, ou encore, en cas de risque ou évènement particulier, par la Direction ou son représentant, si le contrôle est justifié et proportionné au but recherché.

En revanche, il est strictement interdit d'identifier indûment des données traitées dans le cadre professionnel comme relevant de dossiers personnels de l'Utilisateur.

2.4 Accès au SI du Groupe à travers des moyens privés

Des applications du Groupe peuvent être mises à disposition des Utilisateurs à travers des logiciels chargés sur leurs appareils numériques privés. **Cette mise à disposition n'est possible que sur la base du volontariat.** Elle est soumise à autorisation et à certaines règles de sécurité en fonction de la nature du support numérique privé concerné.

À ce jour, le Groupe permet seulement deux types de mise à disposition sur les supports privés :

- l'accès au portail extranet (extranet.afd.fr) depuis un ordinateur ou un smartphone privé,
- l'installation de la messagerie pushmail du Groupe sur un smartphone personnel.

Les Utilisateurs sont informés que cette mise à disposition entraîne la capture d'informations techniques liées au matériel privé utilisé pour accéder aux outils professionnels. Le Groupe s'engage à n'accéder à aucune autre information privée et à assurer la protection des informations techniques indispensables aux fonctionnements des outils fournis.

En conséquence, le Groupe ne pourra pas effectuer le support de l'outil mis à disposition si une intervention est nécessaire sur l'appareil privé de l'Utilisateur.

Des outils informatiques professionnels sont parfois accessibles depuis l'Internet. Les Utilisateurs doivent alors s'interdire d'y accéder en dehors des moyens autorisés par le Groupe. Ils s'interdisent en particulier de stocker leurs secrets d'authentification sur du matériel n'appartenant pas au Groupe. Sauf mention explicite dans les conditions d'usage de l'outil, les seuls moyens d'accès autorisés sont ceux mis à la disposition par le groupe.

Dans l'hypothèse où les Utilisateurs recourent à des outils personnels pour accéder au SI du Groupe, ils ne doivent pas conserver sur leurs outils numériques personnels des données professionnelles.

2.5 Le respect du droit de propriété

Les Utilisateurs du SI du Groupe doivent respecter les dispositions du code de la propriété intellectuelle. Ils doivent notamment **ne pas reproduire, copier, diffuser, modifier ou utiliser des supports soumis au droit de la propriété intellectuelle** sans avoir reçu l'autorisation du ou des titulaires des droits. Ceci inclut :

- les logiciels, les bases de données ou les pages web, ...
- les textes, images, photographies ou autres créations intellectuelles.

Toute production d'un Utilisateur réalisée dans le cadre de ses fonctions et/ou grâce aux ressources mises à sa disposition par le Groupe appartient au Groupe.

2.6 Probité

Il est interdit pour tout Utilisateur de consulter, stocker, diffuser ou relayer via les outils professionnels des contenus pornographiques ou illégaux, en ce compris des contenus pédopornographiques, diffamatoires, haineux, homophobes, racistes, antisémites ou constitutifs d'apologie du terrorisme.

3 RÈGLES GÉNÉRALES DE SÉCURITÉ

Outre la réglementation applicable et les dispositions de la politique de sécurité des systèmes d'information, l'usage des outils informatiques doit être conforme à la présente charte. Chacun contribue, à son niveau, à la sécurité générale du système d'information du Groupe.

En particulier, tout Utilisateur :

- est tenu d'appliquer les règles, procédures et consignes de sécurité de l'établissement ;
- est responsable de la confidentialité des informations qu'il produit et détient.

Il s'engage à :

- signaler au département Sécurité (SEC) toute anomalie de sécurité, perte ou vol qu'il peut constater, y compris de son smartphone personnel sur lequel seraient installés des outils numériques du Groupe ;
- ne pas installer, sur les outils professionnels, de logiciels susceptibles de contourner, d'affaiblir ou de perturber les dispositifs de sécurité ou de performance du SI ;
- choisir des mots de passe sûrs, correspondant a minima aux critères dans cette charte (cf. annexe III) et **les garder secrets sans les communiquer à un tiers** (y compris aux services en charge du support informatique) ;
- **procéder régulièrement au changement de ses mots de passe** ou si, pour quelque raison que ce soit, leur confidentialité a été compromise ;
- **ne pas utiliser ou essayer d'utiliser les accès d'un autre Utilisateur**, même avec son accord, ni masquer sa véritable identité ou usurper celle d'autrui ;
- ne jamais essayer de désactiver les logiciels de protection installés sur son poste de travail ;
- **ne pas débrider¹ son smartphone** professionnel ou son smartphone personnel si un outil professionnel y est installé ;
- autoriser le déploiement, sur son smartphone personnel, des paramètres de sécurité professionnels s'il souhaite bénéficier de l'outil pushmail du Groupe² ;

¹ Le terme « jailbreak » est aussi utilisé pour décrire l'action de débridage.

² Le paramétrage de sécurité applicable aux smartphones personnels est étudié pour être le moins contraignant possible.

- **verrouiller l'accès au smartphone** par mot de passe ou biométrie ;

L'utilisation de la biométrie n'est pas exigée par le Groupe et constitue une démarche volontaire individuelle. Le Groupe n'accède pas à vos données biométriques, stockées localement sur votre smartphone professionnel.

- utiliser uniquement les outils mis à disposition ou approuvés par le Groupe pour stocker les données professionnelles ;
- Respecter les bonnes pratiques de sécurité dans l'usage des ports USB, comprenant notamment l'analyse préalable de la clé USB par l'anti-virus avant ouverture des documents stockés et sécurisation des informations stockées à hauteur du niveau de confidentialité (pas de données personnelles ou couvertes par le secret bancaire sur des clés USB non chiffrées par exemple).

Il veille à :

- verrouiller son compte professionnel lors de chaque absence, même de courte durée ;
- vérifier que son ordinateur est attaché à un point fixe par un câble antivol lorsqu'il est à son poste de travail habituel ou, pour les portables, que le dock est bien verrouillé (clef à conserver en sûreté) ;
- ne pas laisser son équipement portable ou son smartphone sans surveillance si celui-ci n'est pas physiquement sécurisé ;
- ne pas faire réparer ses outils professionnels et notamment son équipement portable ou son smartphone professionnel par un intervenant non approuvé formellement par le Groupe. Le PSU doit être sollicité pour faire effectuer les opérations de maintenance par un prestataire approuvé par le Groupe.

4 RÈGLES DE COMMUNICATION NUMÉRIQUE

Le terme « outils de communication numérique » désigne les services de messagerie, l'Intranet et l'Internet et toutes les applications associées y compris les réseaux sociaux.

Le terme « messagerie électronique » désigne tous les moyens permettant d'échanger des messages électroniques à travers le système d'information du Groupe y compris vers les tiers (courriels, messagerie instantanée, Pushmail, webphone type Skype ou visioconférence ...).

4.1 Usage des services Internet et Intranet

L'usage des services Internet et Intranet fournis par le Groupe est réglementé. L'utilisateur s'astreint à :

- ne pas engager financièrement le Groupe, pour ses besoins personnels, par la consultation de sites payants ;
- ne pas utiliser Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives ;
- faire preuve de correction et de discrétion à l'égard de ses interlocuteurs lors de ses échanges via Internet ou Intranet ;

- ne pas dénigrer, injurier, ni diffamer le Groupe publiquement, notamment sur les réseaux sociaux ;
- respecter les lois relatives à l'interdiction d'accès aux publications à caractères injurieux, raciste, sexiste, diffamatoire ou pédopornographique ;
- ne pas enregistrer de document propriété du Groupe sur un espace de stockage ou de transfert externe non homologué par le Groupe, sauf autorisation ou droits appropriés liés à l'exercice de l'activité professionnelle et sauf si ce document est identifié comme « PUBLIC ».

4.2 Usage de la messagerie électronique

4.2.1 Règles générales d'usage de la messagerie électronique

L'usage de la messagerie électronique est réglementé. L'Utilisateur s'engage à :

- **toujours rester vigilant vis-à-vis des messages reçus.** Un message paraissant suspect (expéditeur inconnu ou suspect, objet ou fichier joint suspect...) ne doit pas être ouvert et aucune réponse ne doit être envoyée suite à la réception d'un SPAM (courrier non désiré). Les messages suspects doivent systématiquement être signalés en les transférant à l'adresse #message_douteux@afd.fr ;
- **ne pas utiliser directement le compte de messagerie d'un tiers.** L'accès à une autre boîte aux lettres que la sienne ne doit se faire qu'avec l'aval explicite et formel du propriétaire et exclusivement par le biais du mécanisme de délégation prévu dans l'outil de messagerie ;
- **signaler tout incident de sécurité** qu'il pourrait constater lors de l'utilisation de sa messagerie (virus, tentative d'intrusion, usurpation d'identité ...), et ce dans les meilleurs délais ;
- ne pas diffuser, par le biais de la messagerie des informations ou données dont le contenu présenterait un caractère illégal, diffamatoire ou injurieux. Ceci s'applique tant aux messages qu'aux pièces jointes qui peuvent leur être associées, quelle que soit leur forme (textuelle, sonore, audiovisuelle ou multimédia) ;
- ne pas utiliser la messagerie interne comme vecteur d'échange, de vente, de recherche de biens (les communications générales et les petites annonces peuvent transiter par Gaïa à travers des supports mieux adaptés) ;
- veiller à limiter la diffusion des messages aux seuls destinataires concernés afin d'éviter l'engorgement de la messagerie et la dégradation du service ;
- ne pas utiliser les listes de diffusion « tout le personnel » et « siège tout le personnel », même en réponse, sauf après autorisation de sa hiérarchie, du service communication ou de la direction générale ;
- **limiter autant que possible le nombre des messages transmis** et éviter d'utiliser systématiquement les envois automatiques de messages tels que les accusés de lecture ou de réception afin de limiter une multiplication non maîtrisée des courriels ;
- veiller à limiter l'usage des boîtes aux lettres génériques aux stricts besoins de service et s'assurer régulièrement que les droits d'accès à ces boîtes sont régulièrement mis à jour.

4.2.2 Usage de la messagerie électronique et vie privée

L'usage de la messagerie électronique professionnelle est réservé à des fins professionnelles. En conséquence, **l'usage privé abusif de la messagerie électronique professionnelle est interdit.**

L'abus est caractérisé en cas d'entrave à l'accomplissement du travail de l'Utilisateur, notamment eu égard à l'importance et à la régularité de l'utilisation personnelle, à l'amointrissement des conditions d'accès ou à l'entrave au trafic normal des messages électroniques professionnels, et ce en termes de volume et de taille des courriers échangés et de format des pièces jointes.

Il est rappelé aux Utilisateurs que les messages envoyés ou reçus à l'aide de leur messagerie électronique professionnelle sont présumés être à caractère professionnel. En conséquence, le Groupe a la possibilité de les consulter en présence ou en l'absence de l'Utilisateur, pour quelque cause que ce soit. L'Utilisateur commettrait une faute en faisant obstacle de manière directe ou indirecte à l'accès à sa messagerie électronique professionnelle.

S'il souhaite identifier un message comme personnel, il revient alors à l'Utilisateur d'indiquer la mention « **PERSONNEL** » ou « **PRIVE** » dans l'objet du message ou de les stocker dans un dossier de messagerie nommé « **PERSONNEL** » ou « **PRIVE** ».

Les messages ainsi désignés pourront uniquement être consultés en présence de l'Utilisateur ou celui-ci dûment appelé, ou encore en cas de risque ou événement particulier, par la Direction ou son représentant, si le contrôle est justifié et proportionné au but recherché.

Il est strictement interdit d'identifier comme « PERSONNEL » un message qui aurait en réalité une nature professionnelle.

4.2.3 Sauvegarde du contenu de la messagerie électronique

L'ensemble des messages reçus par les Utilisateurs sur leur messagerie électronique professionnelle et envoyés depuis celle-ci sont sauvegardés par le Groupe, qui peut donc y avoir accès même après suppression éventuelle pendant 12 mois. Ceci s'applique également aux conversations par messagerie instantanée.

Cette sauvegarde pourra permettre au Groupe de contrôler à posteriori le contenu des emails envoyés afin de vérifier que celui-ci est conforme à la présente Charte, ainsi qu'à l'obligation de loyauté des Utilisateurs qui sont soumis à cette obligation en vertu de leur contrat.

4.2.4 Absence de l'utilisateur

En cas d'absence, il appartient à chaque Utilisateur de mettre en place un message automatique en précisant la durée d'absence et les interlocuteurs à qui s'adresser durant cette période. À défaut, le supérieur hiérarchique pourra obtenir de la DSI la mise en place d'un tel message pour la période indiquée.

Par exception, les Utilisateurs occupant des fonctions sensibles sont dispensés de cette notification si elle peut favoriser des tentatives de fraude ou mettre en risque les personnes ou les activités du Groupe.

En cas d'absence de longue durée, le supérieur hiérarchique de l'Utilisateur, pourra demander à la DSI, après accord de la Direction, le transfert des messages reçus par l'Utilisateur absent.

4.2.5 Accès à la messagerie de l'Utilisateur après un départ définitif

La messagerie professionnelle d'un Utilisateur est fermée à compter de son départ effectif. Pour assurer la continuité du service, elle restera néanmoins accessible à l'un des responsables de l'ancien Utilisateur, sur demande à la DSI et après approbation par la Direction, pendant un délai maximum de quatre mois.

Il conviendra ainsi que l'Utilisateur trie sa messagerie avant son départ effectif et supprime l'ensemble des courriers électroniques personnels envoyés ou reçus. A l'expiration des quatre mois, l'adresse électronique du salarié sera supprimée.

4.2.6 Messagerie électronique et délégations de signature

L'Utilisateur s'engage à porter une attention toute particulière à la rédaction et à la diffusion des messages électroniques. Le message électronique peut être reconnu comme une preuve valable pour établir un fait ou un acte juridique. Les règles relatives aux délégations de signatures devront être respectées.

4.3 Le nomadisme

Le Groupe dote ses agents, ou même certains intervenants externes, de matériels et logiciels capables de se connecter à distance à son réseau.

En particulier, le Groupe donne la possibilité à ses agents, sur la base du volontariat, d'accéder à certaines applications professionnelles à travers leur smartphone personnel. Cet accès est uniquement autorisé à travers l'outil « pushmail » sécurisé du Groupe. Il est fourni uniquement sur les smartphones qui sont conformes aux règles de sécurité du Groupe et si l'Utilisateur accepte l'application de ces règles sur son smartphone.

L'utilisation de ces outils doit se faire dans le respect des principes de sécurité suivants :

- seuls les moyens de connexion prévus ou autorisés par le Groupe doivent être utilisés ;
- une fois connecté au système d'information du Groupe, l'Utilisateur est soumis aux mêmes règles de sécurité qu'en interne ;
- **le matériel nomade est sous la responsabilité de son Utilisateur.** Ce dernier doit donc être vigilant afin d'en assurer la sécurité ;
- tout accès aux services à distance du Groupe ne doit être initié qu'avec un ordinateur présentant des garanties de sécurité suffisantes, notamment en termes de protection antivirale.

4.4 Les moyens de communication par visio-conférence

L'usage des moyens de communication par visio-conférence doit s'inscrire dans le strict respect des règles générales de la présente charte.

A cet égard, l'Utilisateur devra recourir uniquement aux outils mis à sa disposition ou explicitement autorisés par le Groupe.

Dans le cadre des échanges via les outils de visio-conférence, il est par principe interdit d'enregistrer les échanges, sauf si cet enregistrement est nécessaire pour les activités professionnelles et sous réserve du respect des principes de la protection des données personnelles, rappelés à l'article 5 de la présente Charte. Dans le cas d'un enregistrement, les Utilisateurs s'assureront en particulier que toutes les personnes concernées par l'enregistrement sont informées au préalable et ont donné leur accord.

5 PROTECTION DES DONNÉES PERSONNELLES

5.1 Respect des règles de protection des données personnelles

Conformément au Règlement Général sur la Protection des Données³, les données à caractère personnel doivent être :

- traitées de manière licite et loyale et d'une manière compréhensible pour la personne concernée ;
- collectées à des fins déterminées, claires et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- pertinentes eu égard aux finalités poursuivies ;
- correctes et, le cas échéant, à jour;
- conservées sous une forme permettant l'identification des personnes concernées uniquement pendant la durée nécessaire aux finalités pour lesquelles elles sont traitées ;
- traitées de manière à garantir un niveau de sécurité suffisant au regard des enjeux et risques résultant du traitement des données personnelles.

Le groupe s'est engagée dans une démarche de conformité à ces grands principes, qui se traduiront dans des règles et procédures internes, complétées d'instructions éventuellement plus précises à l'attention des Utilisateurs. Ces derniers doivent respecter lesdites règles et instructions dans le cadre de l'utilisation des outils professionnels. Ils sont invités par ailleurs à contacter la Déléguée à la protection des données si :

- Ils constatent que les règles et instructions ne sont pas conformes aux principes résultant du RGPD ;
- Ils identifient une possible violation de données, laquelle est constituée par une perte de confidentialité, de disponibilité ou d'intégrité impactant des données personnelles.

³ RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

5.2 Données personnelles sur les Utilisateurs du SI du Groupe

L'administration et le contrôle de l'usage des outils mis à disposition par le Groupe résultent en des traitements de données personnelles dont les finalités et modalités sont rappelées à l'article 7 de la présente Charte. Le fondement juridique du traitement de ces données est l'intérêt légitime du groupe à assurer la sécurité de son système d'information. Seul le personnel dûment habilité en raison de ses missions accède aux données.

Le Groupe, agissant en tant que responsable de traitement, s'engage à ce que les données qui concernent les Utilisateurs soient collectées et traitées de manière loyale et sécurisées, dans le strict respect des prescriptions légales en vigueur.

Les Utilisateurs disposent en particulier de plusieurs droits concernant les données personnelles les concernant, savoir d'un droit d'accès, de rectification, d'opposition, d'effacement et de limitation des traitements relatifs à leurs données personnelles ainsi que d'un droit à ne pas faire l'objet d'une décision automatisée. Pour exercer ces droits ou obtenir toute autre information relative aux traitements de ces données, les Utilisateurs peuvent contacter la Déléguée à la Protection des Données (DPD) de l'AFD à l'adresse suivante : informatique.libertés@afd.fr

6 ANALYSE ET CONTRÔLE DE L'UTILISATION DU SI

6.1 Contrôles de l'utilisation des outils professionnels

L'utilisation des ressources du système d'information ainsi que **les échanges réseaux sont analysés et contrôlés** dans le respect de la réglementation applicable. Le Groupe se réserve la possibilité de réaliser un contrôle des connexions et modalités d'utilisation du SI, susceptible de concerner notamment :

- Les accès aux sites internet, en particulier les sites de contenu contraire aux lois et règlements en vigueur. Dans ce contexte, le Groupe a la possibilité, en cas d'incident, d'identifier individuellement les Utilisateurs qui se seraient connectés et maintenus sur de tels sites. Dans la mesure où les connexions Internet sont présumées à caractère professionnel, elles sont susceptibles d'être contrôlées par le Groupe, même hors la présence de l'Utilisateur ;
- L'installation d'outils sur le poste de travail de l'Utilisateur, au moyen d'inventaires à distance réguliers, afin d'identifier le téléchargement et l'installation de logiciels non fournis et non autorisés par le Groupe ;
- Les journaux de bord traitant des données figurant sur les postes individuels, sur le réseau et sur les outils de communication électronique, le niveau de détail des données collectées étant proportionné aux enjeux de sécurité encourus. Ces journaux sont conservés pendant un an maximum, conformément à la PSSI du Groupe ;
- Le contrôle de l'utilisation de la messagerie électronique, dans les conditions définies à l'article 4.2 de la présente Charte.

De tels contrôles sont mis en œuvre afin de garantir la sécurité de l'information, de prévenir l'utilisation frauduleuse ou malveillante des outils mis à disposition et de limiter

la responsabilité du Groupe du fait d'un Utilisateur. Ces informations sont susceptibles d'être utilisées dans le cadre de procédures disciplinaires et/ou judiciaires.

En cas de risque ou d'événement particulier, notamment de sécurité, le Groupe pourra, à tout moment et sans préavis, accéder aux ressources informatiques mises à la disposition d'un Utilisateur du SI du Groupe. Tenus au secret professionnel, les administrateurs ne peuvent divulguer les informations qu'ils auraient été amenés à connaître dans le cadre de leur fonction.

6.2 Le système automatique de filtrage

Afin de réduire les flux d'information, d'assurer la sécurité et la confidentialité des informations, le Groupe met en place un système automatique de filtrage des sites internet, d'élimination des courriels non sollicités, de blocage de certains protocoles ainsi que toute autre mesure destinée à assurer la sécurité du SI.

6.3 Accès aux postes de travail par le PSU

Sauf cas d'urgence mettant en cause l'intégrité et la bonne marche des systèmes, **la prise de contrôle à distance** de la session d'un Utilisateur par un administrateur ou un intervenant du PSU **ne peut se faire qu'après en avoir informé celui-ci et obtenu son accord préalable**. Il appartient à l'Utilisateur de ne pas laisser en évidence sur le poste de travail des documents susceptibles de contenir des informations confidentielles lors de l'intervention du PSU.

En cas d'utilisation d'un outil professionnel sur du matériel privé, il est précisé que le Groupe n'a de visibilité que sur les données isolées sur l'outil professionnel et ne peut, en aucun cas, prendre le contrôle à distance du matériel personnel, même sur demande de l'Utilisateur.

7 DU BON USAGE DU SYSTÈME D'INFORMATION

7.1 Généralités

Le point d'entrée de toutes les demandes et incidents relatifs au système d'information et aux équipements associés est le PSU : 3434 ou psu@afd.fr.

7.2 Arrivants, mobilités et départs

Les formulaires à remplir sont accessibles dans l'outil GALATA accessible depuis GAIA.

Les demandes de création de compte et d'installation de poste de travail sont à adresser à PSU en utilisant l'outil GALATA. Il en est de même pour les demandes de prise en compte dans le SI des mobilités, changements d'affectation, déménagements, changements de statuts et changements de service.

Chaque Utilisateur du SI doit restituer, avant tout départ, l'intégralité du matériel mis à sa disposition par le Groupe. Il ne pourra pas conserver le numéro de téléphone portable professionnel que lui a éventuellement fourni le Groupe.

Tout départ définitif d'un Utilisateur doit impérativement être signalé au PSU selon les mêmes modalités.

Les informations contenues sur le poste de travail, le disque P et la messagerie d'une personne sont conservées pendant une durée de 4 mois après son départ définitif du Groupe. Elles sont ensuite supprimées définitivement. Pendant cette période, la personne pourra demander au Groupe la restitution des informations « personnelles » contenues sur ces emplacements. Les données professionnelles ne pourront pas être restituées. Cette demande doit être adressée à DSI par l'intermédiaire de DRH.

Avant leur départ, les Utilisateurs s'astreindront à un tri sur leur messagerie professionnelle, tel que décrit dans l'article 4.2.5. Ce tri devra aussi être effectué sur leur poste de travail et sur leur disque P avant leur départ effectif afin de supprimer l'ensemble des documents personnels stockés. A l'expiration des quatre mois, l'espace de stockage réseau de l'Utilisateur sera supprimé et son poste de travail recyclé.

7.3 Dossiers réseaux

Les dossiers réseaux font l'objet d'une sauvegarde automatique et quotidienne. Il appartient à l'Utilisateur de supprimer régulièrement les documents périmés stockés dans ces derniers ou de procéder à leur archivage, conformément à la politique d'archivage et en appliquant les durées de conservation définies pour les documents.

7.3.1 Dossiers partagés

Les dossiers partagés constituent un espace de stockage permettant le partage de données professionnelles entre agents d'une même structure (lecteur S) ou entre tous les agents et intervenants externes possédant un poste de travail mis à leur disposition par le Groupe et collaborant autour d'un même sujet (lecteur I). Il est précisé que les accès au :

- lecteur S sont réservés aux agents de la structure concernée ;
- lecteur I sont attribués selon les besoins par les correspondants informatiques des départements ;
- lecteur Q réservé aux documents de portée générale accessible à l'ensemble des Utilisateurs.

7.3.2 Dossier dit « personnel »

Le lecteur « P » dit « personnel » permet de stocker des **données individuelles à usage professionnel**. Il ne constitue pas un espace « privé » et ne saurait être utilisé pour les documents, photos, archives de messagerie ou autres éléments non professionnels.

Si certaines informations privées sont malgré tout stockées sur cet emplacement, il est nécessaire de le signaler en les positionnant dans un dossier nommé « privé » ou « personnel ».

Afin d'éviter les surcharges de l'infrastructure de stockage de l'entreprise, une limite de stockage sur le disque « P: » peut être mise en place sur décision du Groupe. Cette limite est fixée par la DSI en fonction des besoins. La DSI peut aussi demander aux Utilisateurs de supprimer certains fichiers de leur lecteur P en cas de surcharge du stockage.

7.4 Poste de travail

Chaque Utilisateur du SI dispose d'un poste de travail fourni par le Groupe. Ce poste de travail permet d'accéder aux logiciels, aux applications et aux ressources partagées mises à disposition de chacun par le Groupe. Il permet de stocker des données individuelles à usage professionnel. Il ne constitue pas un espace « privé ».

Si certaines informations privées sont malgré tout stockées sur le poste, il est nécessaire de le signaler en les positionnant dans un dossier nommé « PRIVE » ou « PERSONNEL ».

Afin de permettre aux Utilisateurs de sauvegarder leurs informations présentes sur le poste de travail, le Groupe met à disposition des agents, sur demande au PSU, un support amovible sur lequel ils peuvent copier leurs données les plus importantes. **Cette sauvegarde doit impérativement être conservée sous clef dans les locaux professionnels du Groupe ou chiffrée grâce à l'outil Bitlocker installé sur tous les postes de travail.**

Afin d'assurer la confidentialité des informations affichées sur l'écran du poste de travail, en particulier lors des déplacements professionnels, le Groupe met à la disposition des Utilisateurs des filtres de confidentialité sur simple demande au PSU.

7.5 Impressions et imprimantes

Le dispositif de référence pour les impressions est constitué par les copieurs multifonctions (scan, impression, copie) placés dans les espaces communs.

Les demandes d'imprimantes complémentaires (réseau ou personnelles) ne sont prises en compte qu'en cas d'absolue nécessité. Ces équipements ont un coût de fonctionnement conséquent et ont un impact négatif sur l'environnement.

En cohérence avec l'approche RSE, les Utilisateurs veillent à n'imprimer qu'en cas de nécessité. Il convient de privilégier les impressions en noir et blanc et recto/verso.

7.6 Applications et logiciels

Toute demande d'accès ou d'installation d'une application métier ou d'un logiciel fait l'objet d'une demande à PSU. Le responsable hiérarchique est garant de la légitimité de cette demande. Ces demandes suivent un circuit d'habilitation ou de demande de service adapté en fonction de la sensibilité et du coût.

Il est rappelé qu'applications et logiciels sont mis à disposition dans le cadre d'une affectation et sont donc désinstallés en cas de mobilité ne justifiant plus de l'usage de ces outils. Ces installations sont coûteuses (licences facturées annuellement) et soumises à des règles de sécurité : chacun se doit de **signaler à PSU s'il n'en a plus l'usage** dans le cadre de ses fonctions.

7.7 Responsabilité environnementale

Par des solutions technologiques et des pratiques plus sobres, notre écosystème numérique converge avec les engagements 100 % accord de Paris et 100 % lien social du Groupe.

En ce sens, l'utilisateur s'engage à aligner ses pratiques numériques :

- avec la trajectoire en faveur du climat de l'entreprise, sur les bases notamment mentionnées dans le support de communication interne repris en pièce jointe ;
- avec la trajectoire sociale de l'entreprise, en particulier en matière de qualité de vie au travail, à travers, notamment, des communications électroniques respectueuses de ses interlocuteurs, ainsi que de leur équilibre vie professionnelle / vie personnelle.

7.8 Équipements liés à la fonction

Certains équipements sont attribués dans le cadre d'une affectation (hiérarchique et géographique) ou d'une fonction spécifique. C'est le cas par exemple des smartphones équipés de la fonction « pushmail » et des tablettes. Ils doivent être restitués à PSU (au siège) ou au CIL (dans le réseau) en cas de changement de fonction ou de localisation ou de départ.

7.9 Archivage et continuité d'activité

Dans la mesure où l'écrit électronique peut constituer une preuve et afin d'assurer la continuité de service, l'Utilisateur doit prendre toute mesure pour conserver les documents électroniques dans de bonnes conditions, conformément à la politique d'archivage et aux règles d'usage de son service, en classant de façon intelligible ces documents et en les enregistrant dans des espaces numériques dédiés (serveurs partagés, GED, système d'archivage électronique).

Cette considération vaut également pour les messages électroniques engageants et les documents de référence qui transitent par messagerie.

8 OBLIGATIONS DES UTILISATEURS

En complément de la présente charte, l'Utilisateur devra appliquer les directives de la Politique de Sécurité du Système d'Information (PSSI) du Groupe.

Toute violation des règles d'usage des outils informatiques et de communication électronique constitue un manquement aux obligations professionnelles d'un Utilisateur du SI. Tout Utilisateur pourrait personnellement être mis en cause en cas de manquement avéré.

Toute violation de la réglementation en vigueur engage **directement la responsabilité personnelle, civile ou pénale** des Utilisateurs qui les commettent.

9 DÉONTOLOGIE DES ADMINISTRATEURS DU SI

Les administrateurs du SI ont pour mission d'assurer le fonctionnement normal et la sécurité des réseaux et systèmes et doivent veiller à ce titre au respect des règles d'utilisation. Même s'ils sont soumis, comme tout Utilisateur, au respect de la présente charte, ils peuvent être amenés dans le cadre de leur activité normale ou pour assurer la sécurité du SI à avoir accès à des informations sensibles du Groupe ou des Utilisateurs.

Dans ce cadre très particulier, ils s'engagent à :

- **respecter la confidentialité attachée aux données** qu'ils peuvent avoir à connaître en raison de leurs privilèges d'administration sur le SI ou lors d'opérations normales d'administration technique ;
- **n'effectuer que les actions techniques strictement nécessaires** pour répondre à la demande légitime d'un métier ou d'un Utilisateur pour rétablir le service nominal en cas de dysfonctionnement ;
- **n'attribuer que les droits d'accès demandés conformément aux processus d'habilitation** en vigueur ;
- **n'effectuer aucune modification des données ou traitements allant à l'encontre du fonctionnement habituel du système informatique** dont ils ont la charge, même si leurs privilèges d'accès au SI le permettent ;
- **n'accéder qu'aux données présentes sur l'espace de stockage professionnel** sécurisé des outils Groupe déployés sur du matériel privé.

Toute violation de ces règles de déontologie constitue un manquement aux obligations professionnelles.

10 PORTÉE DISCIPLINAIRE DE LA CHARTE

Il est précisé aux Utilisateurs que la présente Charte constitue une annexe au Règlement intérieur. Tout manquement, tout abus ou toute utilisation non conforme à la présente Charte peut donc faire l'objet de sanctions disciplinaires à l'encontre des Utilisateurs, telles que prévues par le Règlement intérieur et le Statut de l'AFD.

11 ANNEXE I : LES DISPOSITIFS DE SÉCURITÉ DU SI DU GROUPE

Le Groupe met à la disposition des Utilisateurs de son système d'information un certain nombre d'outils de sécurité dont les principaux sont listés ci-dessous.

11.1 Pour la connexion nomade :

- Connexion chiffrée à la messagerie via un navigateur Internet et le portail OWA (Outlook Web Access). <https://extranet.afd.fr>.
- Connexion à la messagerie via PUSHMAIL sur Smartphone. Sur smartphone professionnel et sur smartphone personnel sur la base du volontariat et sous réserve d'éligibilité avec les règles de sécurité du Groupe.
- Connexion sécurisée au réseau interne du Groupe positionnée sur les ordinateurs portables.
- Détection des smartphones débridés pour verrouiller l'accès au stockage professionnel (via l'accès BlackBerry)

11.2 Pour le chiffrement des postes de travail :

- Une solution de chiffrement du disque dur est déployée sur tous les ordinateurs portables du Groupe.
- Un logiciel de chiffrement peut être utilisé de manière plus ciblée (se renseigner auprès du département Sécurité).

11.3 La protection des postes de travail :

- Une configuration sécurisée du système d'exploitation est déployée sur les postes en fonction de leur sensibilité
- Un dispositif de chiffrement des flux nomades (VPN) est déployé sur les ordinateurs portables
- Un antivirus est déployé sur tous les postes du Groupe
- Un pare-feu personnel est déployé sur tous les postes du Groupe
- Un antivirus spécifique est positionné sur les serveurs de messagerie du Groupe
- Un filtre de courriels indésirables (SPAM) est placé sur les serveurs de messagerie du Groupe
- Un filtre de courriels indésirables est fourni par Outlook sur chaque poste, il permet à chaque Utilisateur de créer lui-même des filtres particuliers adaptés à son usage
- Un filtre d'URL, bloquant les accès Internet illégaux ou dangereux pour le SI est mis en place sur l'infrastructure d'accès au Web.
- Une chaîne de filtrage des flux réseau est implantée sur le SI.

11.4 La sensibilisation des Utilisateurs :

- Les modules de e-learning portant sur la sécurité du SI accessibles sur le site e-formation : <https://eformation.afd.fr/>
- Le cycle de conférences sensibilisation cyber-sécurité, organisé avec l'appui du ministère de l'intérieur.
- Des campagnes de sensibilisation spécifiques sont mise en place au bénéfice des agents en fonction de leur activité opérationnelle.

12 ANNEXE II : LE CHOIX D'UN MOT DE PASSE

Lors du choix d'un mot de passe, il convient de respecter certaines règles afin de le rendre le plus fiable possible. Il doit être **facile à retenir et difficile à deviner**. Pour construire un mot de passe « fort », sa composition doit s'appuyer sur les principes ci-après :

- Il doit avoir une longueur minimale de 8 caractères. Plus le mot sera long, plus il faudra de temps pour en venir à bout.
- Il convient d'éviter tout mot qui peut se trouver dans un dictionnaire. De même, les noms propres doivent être écartés ainsi que toute information familiale ou personnelle (il ne faut surtout pas choisir un surnom ou une date de naissance par exemple).
- Il est indispensable d'intégrer dans son mot de passe des caractères « exotiques ». Un bon mot de passe est un mélange de majuscules, minuscules, chiffres et caractères spéciaux tels que « #, ;! ?@ »

En appliquant ces trois principes, le mot de passe choisi sera très difficile à deviner mais pas forcément facile à retenir.

Pour pallier ce problème, certains moyens mnémotechniques existent (cette liste n'est bien sûr pas exhaustive et chacun pourra trouver ses propres méthodes) :

- La transposition : En remplaçant certaines lettres par des chiffres, on peut avoir à ne retenir qu'un mot (ou une phrase) simple.
- Exemple : « attention! » devient « **4#3N#1oN!** ».
- Les premières lettres : A partir d'une phrase, on peut constituer un mot de passe où les lettres utilisées seront, par exemple, la première lettre de chaque mot de la phrase. On peut ensuite faire suivre ces lettres par le nombre de mots qu'il y a dans la phrase.
- Exemple : « A brebis tondue, Dieu mesure le vent. » devient « **Abt,Dmlv7.** ».
- La phonétique : Il s'agit d'écrire une phrase comme on l'entend.
- Exemple : « J'ai deux beaux-frères... » devient « **Jé2bofrair...** ».

Les règles mises en œuvre sur le SI du Groupe prévoient actuellement que le mot de passe d'un Utilisateur doit, à minima, satisfaire les exigences suivantes :

- 1) être constitué d'un minimum de 8 caractères ;
- 2) être constitué d'au moins deux types de caractères parmi les groupes suivants :
 - minuscules
 - majuscules
 - chiffres
 - caractères spéciaux (« , ;#@ etc...)
- 3) avoir une durée de vie maximum de 3 mois ;
- 4) ne pas être semblable à l'un des quatre mots de passe précédents.

Niveau de confidentialité

PUBLIC	RESTREINT	CONFIDENTIEL	STRICTEMENT CONFIDENTIEL
☐	☒	☐	☐

Historique des modifications

Version	Date	État du document	Valideur
5.12	03/12/15	Version valide jusqu'au 7 février 2021	DGL
6.7	11/12/20	Projet d'évolution relu DRH, DCO, EJS, EVA, SEC	R. FALUOMI
6.92	18/12/20	Projet d'évolution de la Charte finalisé pour le CSEC	R. FALUOMI
6.92B	01/03/20	Projet de Charte Utilisateurs modifié pour le CSEC	R. FALUOMI
6.93	25/04/21	Charte Utilisateurs validée	R. RIOUX