

CHARTE UTILISATEUR

Utilisation du système d'information

Date de mise à jour : 30 avril 2024

Date d'entrée en vigueur : 24 août 2024

Version 3.0

Macro-Process : Ressources SI

Process : Cloud & Sécurité

Entité pilote : Direction des Systèmes d'Information / Département Technologies et Services

Entités associées : Direction des Ressources humaines et Direction juridique

DESCRIPTION :



La présente charte a pour objet de fixer les principes généraux (règles d'utilisation et de sécurité, responsabilités respectives de l'Agence et des utilisateurs) d'utilisation du système d'information mis à disposition des utilisateurs dans le cadre de leur activité professionnelle au sein de Business France.

SOMMAIRE

PREAMBULE.....	5
ARTICLE 1. CHAMP D'APPLICATION.....	5
ARTICLE 2. DEROGATION.....	6
ARTICLE 3. REGLES D'UTILISATION DU SYSTEME D'INFORMATION .	6
ARTICLE 4. UTILISATION PRIVEE RESIDUELLE	7
ARTICLE 5. CONDITIONS D'ACCES, ABSENCES ET DEPARTS DE L'UTILISATEUR.....	7
5.1 Conditions d'accès.....	7
5.2 - Gestion des absences	8
5.3 - Gestion des départs.....	9
5.4 - Equipement personnel de communication	9
ARTICLE 6. CONFIDENTIALITE ET SECURITE	10
ARTICLE 7. PROTECTION DE L'ACCES AU SYSTEME D'INFORMATION	10
ARTICLE 8. PLAN DE CONTINUITE D'ACTIVITE	11
ARTICLE 9. MOBILITE ET MATERIELS MIS A DISPOSITION PAR BUSINESS FRANCE	12
ARTICLE 10. OUTILS COLLABORATIFS ET PLATEFORMES DE COMMUNICATION COLLECTIVES	13
10.1 - Principes	13
10.2 - Forum	13
10.3 - Liste de diffusion.....	13
10.4 - Logiciel externe	14
10.5 - Services hébergés.....	14

SOMMAIRE

ARTICLE 11. RESEAUX SOCIAUX	14
Usage professionnel	14
Usage non professionnel	15
Signalement	15
ARTICLE 12. UTILISATION DE L'INTELLIGENCE ARTIFICIELLE	16
ARTICLE 13. DONNEES A CARACTERE PERSONNEL	16
13.1 - Devoirs des utilisateurs	16
13.2 - Droits des utilisateurs	17
ARTICLE 14. PROPRIETE INTELLECTUELLE	18
ARTICLE 15. CONTROLE DU SYSTEME D'INFORMATION	18
ARTICLE 16. VIDEOSURVEILLANCE	19
ARTICLE 17. CONTROLE DES CONSOMMATIONS DE TELEPHONIE FIXE ET MOBILE	20
ARTICLE 18. SAUVEGARDE ET ARCHIVAGE	20
ARTICLE 19. SANCTIONS	21
ARTICLE 20. ENTREE EN VIGUEUR	21

PREAMBULE

1. La présente charte a pour objet de fixer les principes généraux (règles d'utilisation et de sécurité, responsabilités respectives de l'Agence et des utilisateurs) d'utilisation du système d'information mis à disposition des utilisateurs dans le cadre de leur activité professionnelle.
2. L'utilisation du système d'information, au sein de Business France, suppose de la part des utilisateurs le respect d'un certain nombre de règles qui ont pour objectifs de :
 - Garantir la disponibilité des systèmes ;
 - Préserver l'intégrité du réseau, des données et de la sécurité des systèmes d'information ;
 - Définir les responsabilités respectives de Business France et des utilisateurs.
3. L'utilisation du système d'information suppose le respect des dispositions de la présente charte qui constitue un code de bonne conduite et de bon usage. Elle est une annexe au règlement intérieur de Business France.
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 Business France du système d'information.

ARTICLE 1. CHAMP D'APPLICATION

La présente charte est portée à la connaissance de tous les utilisateurs des systèmes d'information et illustre le comportement responsable que chaque utilisateur doit avoir afin de protéger le patrimoine confidentiel et l'image de marque de Business France.

Est considéré comme « utilisateur », toute personne, quel que soit son statut (salarié, stagiaire, consultant, prestataire, autre intervenant ou collaborateur extérieur etc...) permanent ou temporaire qui est amenée à mettre en œuvre, créer, consulter ou utiliser le système d'information de Business France.

Est désigné de façon générale sous le terme de « système d'information », l'ensemble des moyens informatiques et numériques, ainsi que les données sous la responsabilité ou en possession de Business France.

Est considéré comme « donnée », toute information, quelle que soit sa forme, détenue par Business France.

Est considéré comme « donnée à caractère personnel », toute information relative à une personne physique et la rendant identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Est considérée comme « donnée confidentielle », toute information sous la responsabilité de Business France, référencée comme telle par Business France.

Est considéré comme « administrateur », toute personne, salariée ou non de Business France, à laquelle est confiée explicitement et par écrit, sous la forme d'une lettre de mission, d'un

profil de poste annexé au contrat de travail ou d'un contrat de prestations de service, la responsabilité d'un système informatique, d'un réseau ou d'un sous-réseau administré par une entité de Business France.

ARTICLE 2. DEROGATION

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

ARTICLE 3. REGLES D'UTILISATION DU SYSTEME D'INFORMATION

- 3.1** Le système d'information mis à disposition des utilisateurs est réservé à un usage professionnel exclusif.
- 3.2** Le non-respect de tout ou partie des règles définies dans la présente charte pourra entraîner la suspension immédiate du droit d'utilisation de tout ou partie du système d'information.
- 3.3** En tout état de cause, les utilisateurs sont responsables du bon usage du système d'information au regard des textes légaux et réglementaires applicables.
- 3.4** Les modes de mise à disposition de contenus numériques comportent des risques inhérents à la technologie employée. Ces risques peuvent être causés par :
 - Un mauvais usage 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.
- 3.5** Toutes les données de Business France mises en ligne sur un site (interne ou externe), sous forme de carnets d'adresses, annuaires, photographies, logiciels, articles de presse, œuvres protégées, blog, chat ou toutes autres données de toutes natures, devront faire l'objet d'une autorisation préalable de Business France.
- 3.6** L'utilisateur ne doit se livrer en aucune circonstance, à une activité qui serait contraire au principe de la législation française et/ou à une quelconque des activités ci-dessous qui pourraient constituer des infractions de nature pénale, notamment de nature et d'ordre :
 - Violent, pornographique, pédophile, négationniste, extrémiste, raciste, xénophobe ;

- Contraires aux bonnes mœurs et/ou susceptible de porter atteinte au respect de la personne et de la dignité humaine de façon générale ;
- Contraires à la protection des mineurs ;
- Diffamatoires ou de manière générale illicites ;
- Susceptibles de mettre en cause la sécurité matérielle ou juridique de Business France ;

3.7 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.

ARTICLE 4. UTILISATION PRIVEE RESIDUELLE

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 et dossiers ne portant pas dans leur objet ou leur dénomination la mention « PRIVE » sont considérés comme de nature professionnelle.

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

5.1 Conditions d'accès

L'accès au système d'information implique que les utilisateurs justifient leur identité en début de session. Si l'identification à une application ou à une ressource s'effectue en cours de session, seul le moyen d'authentification mis à disposition par Business France doit être utilisé.

5.1.1 Chaque utilisateur reçoit un droit d'accès individuel, personnel et confidentiel qui se matérialise par tout moyen logique (accès aux applications du SI) ou physique (code utilisateur et mot de passe), et qu'il ne doit pas communiquer.

5.1.2 L'efficacité d'un mot de passe dépend du nombre de caractères alphanumériques (douze au moins), de son originalité et de son renouvellement régulier par l'utilisateur.

- 5.1.3** Chaque utilisateur doit s'identifier clairement et ne peut utiliser l'identité d'autrui.
- 5.1.4** Il appartient à l'utilisateur de vérifier la légitimité des pages ou outils sur lesquels il est invité à s'identifier (cf. hameçonnage ...)
- 5.1.5** Chaque utilisateur doit obligatoirement activer une méthode d'authentification forte (téléphone, clé de sécurité, ...), qui permet de sécuriser le SI contre les attaques de type hameçonnage. (*Procédure disponible sur l'intranet de l'entreprise*).
- 5.1.6** Ce droit d'accès cesse automatiquement lors d'un départ (l'utilisateur quittant Business France) ou lors d'un changement d'affectation (changement de poste, mutation, etc....) ou s'il est constaté que l'utilisateur a violé l'une des obligations imposées par la présente charte.
- 5.1.7** Le droit d'accès n'est conféré à l'utilisateur qu'aux fins d'une utilisation conforme à son activité professionnelle au sein de Business France et exclut toute autre utilisation.
- 5.1.8** L'utilisateur reconnaît que l'usage de son droit d'accès peut engager sa responsabilité.
- 5.1.9** 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.
- 5.1.10** 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

- 5.2.1** 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.
- 5.2.2** 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.
- 5.2.3** En cas d'absence de l'utilisateur, pour quelque raison que ce soit, l'autorité hiérarchique se réserve le droit, avec l'accord de la DRH, 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.

- 5.2.4** En cas d'absence prolongée, Business France 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

- 5.3.1** Lors de son départ de Business France, 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.
- 5.3.2** Par ailleurs, il appartient à l'utilisateur de détruire son répertoire et ses dossiers « PRIVE ».
- 5.3.3** Le répertoire « PRIVE » d'un utilisateur quittant Business France, s'il n'a pas été détruit par ce dernier, sera supprimé sans copie, ni prise de connaissance préalable du contenu par Business France, sauf s'il est présent ou s'il a été dûment informé ou en cas de risque ou d'évènement particulier.
- 5.3.4** L'utilisateur est informé que son compte sera fermé le lendemain de son départ contractuel, afin de lui permettre de vider sa messagerie. Il est de la responsabilité de l'utilisateur de faire suivre ses messages à caractère personnel en communiquant sa nouvelle adresse à ses interlocuteurs.
- 5.3.5** Lors du départ de l'utilisateur, aucun élément ne doit être protégé par un code d'accès ou un mécanisme de protection quelconque.
- 5.3.6** L'utilisateur s'engage en cas de cessation de ses fonctions à restituer intégralement les données, fichiers informatiques et tout support d'information appartenant à Business France et à ne pas les divulguer en externe.

5.4 – Equipement personnel de communication

- 5.4.1** Pour des raisons écologiques et pratiques, les utilisateurs ont la possibilité d'utiliser leurs appareils personnels pour se connecter aux réseaux de Business France. Cette pratique est acceptée, mais encadrée.
- 5.4.2** L'utilisateur est conscient que la connexion aux ressources de l'entreprise depuis son appareil personnel implique d'ajouter son appareil dans le système informatique de Business France. Cet ajout ne permet en aucun cas à Business France de prendre connaissance d'informations personnelles présentes sur l'appareil personnel de l'utilisateur.
- 5.4.3** Son accès depuis un appareil personnel pourra être bloqué à tout moment par la Direction des Systèmes d'Information si elle le juge nécessaire à la protection du SI.
- 5.4.4** L'utilisateur pourra demander, via le support, à supprimer son appareil du SI de Business France. Une telle demande coupera ses accès via son appareil personnel.
- 5.4.5** Des restrictions peuvent s'appliquer sur l'accès à certains fichiers et sur les fonctionnalités normalement disponibles sur un poste professionnel.

5.4.6 L'utilisation d'appareil personnel pour l'accès aux ressources du SI de Business France est soumise à plusieurs règles de sécurité qui évolueront au fil du temps. La Direction des Systèmes d'Information s'accorde donc le droit de modifier ces règles d'accès si elle le juge nécessaire.

ARTICLE 6. CONFIDENTIALITE ET SECURITE

6.1 La sauvegarde du patrimoine et des intérêts de Business France passe par le respect, par tous, d'une obligation générale et permanente de confidentialité et de discrétion, à l'égard des informations et documents disponibles.

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

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

- Habilitation de l'émetteur ;
- Echanges d'information basés sur le principe du « Besoin d'en connaître » ;
- Désignation d'un destinataire autorisé ;
- Respect d'une procédure sécurisée.

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.

6.3 Des mécanismes de classification de données en fonction du degré de confidentialité sont mis en place par Business France.

- L'utilisateur doit s'assurer de la bonne classification des documents qu'il manipule.
- Des restrictions peuvent être mises en place en fonction de la sensibilité du document. De ce fait, l'utilisateur ne doit pas réduire la sensibilité d'un document pour outrepasser les mesures de sécurité qui s'appliqueraient.

6.4 La Direction des Systèmes d'Information (DSI) met en place des solutions de sensibilisation à la sécurité informatique. Les utilisateurs sont vivement encouragés à participer à ces initiatives pour renforcer la sécurité de l'ensemble du système.

ARTICLE 7. PROTECTION DE L'ACCES AU SYSTEME D'INFORMATION

7.1 L'utilisateur doit signaler toute tentative de violation de son poste ou supports numériques en sa possession auprès de la Direction des systèmes d'information ([via l'outil de contact du support informatique](#)).

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

- 7.3** En particulier, l'utilisateur veille à verrouiller systématiquement son poste de travail en cas d'absence, même momentanée (touche Windows + L).
- 7.4** 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.
- 7.5** 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 [via l'outil de contact du support informatique](#).
- 7.6** 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 [via l'outil de contact du support informatique](#).
 - Agir sur instruction de cette dernière.
- 7.7** 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 ;
 - Modifier ou supprimer des données, notamment comptables ou financières.

ARTICLE 8. PLAN DE CONTINUITE D'ACTIVITE

- 8.1** L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, Business France 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.
- 8.2** 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.).

ARTICLE 9. MOBILITE ET MATERIELS MIS A DISPOSITION PAR BUSINESS FRANCE

- 9.1** 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.
- 9.2** Seuls les matériels nomades autorisés peuvent être connectés aux réseaux de Business France.
- 9.3** Les matériels nomades sont mis à la disposition des utilisateurs, selon les procédures définies par la Direction des systèmes d'information.
- 9.4** Lorsque ces matériels nomades sont utilisés à l'extérieur de Business France, l'utilisateur en assure la garde et la responsabilité.
- 9.5** L'utilisation des matériels nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcées.
- 9.6** Il doit notamment veiller à ce que des tiers ne puissent prendre possession de ces matériels nomades, les utiliser ou accéder à leurs contenus ; l'utilisateur doit veiller à mettre en œuvre les consignes suivantes définies par la Direction des systèmes d'information.
- Adopter la plus stricte discrétion sur Business France et ses activités au sein de celle-ci lorsqu'il est dans des lieux publics, et notamment ne pas travailler sur ou discuter d'éléments confidentiels, secrets, sensibles ou stratégiques en de tels lieux ;
 - Veiller à utiliser tous les moyens de prévention de vol (câble antivol, coffres d'hôtels) et de protection d'informations disponibles (chiffrement, écrans polarisés) et ne pas laisser ses affaires professionnelles sans surveillance, afin de réduire la probabilité d'un vol de matériel ou d'information et d'en limiter les conséquences ;
 - Alerter Business France dans les plus brefs délais de tout événement suspect (déplacement d'ordinateur portable ou d'objets personnels dans la chambre d'hôtel, fouille et saisie temporaire d'ordinateurs au contrôle des douanes, intérêt manifeste et questionnement sur Business France de la part de voyageurs tiers, etc.), ainsi qu'en cas de perte ou de vol de matériel.
- 9.7** L'utilisateur est, par ailleurs, averti du fait que les formalités douanières de certains pays étrangers (USA et Chine notamment) permettent, en toute légalité, aux agents assermentés de ces pays, de procéder à une saisie temporaire des matériels informatiques afin d'en examiner le contenu et d'en établir une copie intégrale. L'utilisateur doit se soumettre à ces formalités sans réserve.

Toutefois, afin de limiter les conséquences potentielles pour Business France, il est expressément recommandé aux utilisateurs de réduire au strict nécessaire la quantité d'informations confidentielles, secrètes, sensibles ou stratégiques présentes sur ces matériels lors de tels déplacements.

Dans certains cas, il sera préférable d'utiliser un support de stockage distant mis en place par Business France (OneDrive, accès aux serveurs de fichiers par tunnel chiffré) pour stocker de telles informations lors d'un déplacement.

ARTICLE 10. OUTILS COLLABORATIFS ET PLATEFORMES DE COMMUNICATION COLLECTIVES

10.1 – Principes

La mise en place des outils collaboratifs et plateformes de communication collectives, notamment blogs, chats, comptes d'entreprise sur les réseaux sociaux ne peut se faire que sur autorisation écrite et préalable de l'autorité hiérarchique.

10.2 – Forum

- 10.2.1** L'ouverture d'un forum professionnel interne à Business France, de type "News Group" par un utilisateur s'effectue sur demande motivée de l'utilisateur et sur autorisation écrite de sa hiérarchie.
- 10.2.2** Ces forums peuvent faire l'objet d'un contrôle par un modérateur désigné à cet effet.
- 10.2.3** 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.
- 10.2.4** La participation des utilisateurs à des forums externes à Business France est interdite, sauf autorisation expresse de leur hiérarchie.
- 10.2.5** L'utilisateur demeure responsable des messages qu'il rédige.

10.3 – Liste de diffusion

- 10.3.1** L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est réservée à un usage strictement professionnel.
- 10.3.2** En outre, l'utilisateur doit systématiquement vérifier lors de l'inscription qu'il existe une procédure de désabonnement.
- 10.3.3** 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.

10.4 – Logiciel externe

- 10.4.1** 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.
- 10.4.2** Le fait pour un utilisateur d'installer un logiciel ou progiciel, même gratuit, sans autorisation préalable de sa hiérarchie est fautif et est susceptible d'engager la responsabilité personnelle de l'utilisateur.

10.5 – Services hébergés

L'utilisation de services hébergés est interdite sauf autorisation de la Direction des systèmes d'information.

ARTICLE 11. RESEAUX SOCIAUX

- 11.1** Business France considère que les réseaux sociaux d'entreprise, les web TV d'entreprise et les services de type podcast dédiés à ses salariés permettent à ces derniers de partager des informations utiles au développement des produits, à l'amélioration du service fourni et à l'innovation.
- 11.2** Par ailleurs, Business France estime que les réseaux sociaux extérieurs à l'entreprise occupent une place grandissante dans la vie des affaires. Ces réseaux permettent aux utilisateurs de créer de nouvelles relations avec ses clients et partenaires et d'optimiser en partie la communication commerciale autour de ses produits.
- 11.3** Cependant, l'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en termes de sécurité, d'image (notamment diffusion de fausses informations), de fraude, de propriété intellectuelle d'intelligence économique et de concurrence déloyale. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

Usage professionnel

- 11.4** Dans le cadre de la sphère professionnelle, l'utilisateur doit obtenir au préalable l'autorisation de la Direction de la Communication et des Affaires Publiques (DCAP) avant de créer un compte ou une page sur un réseau social au nom de Business France. Il doit également obtenir l'autorisation de son supérieur hiérarchique pour réaliser les missions confiées par Business France via un réseau social.
- 11.5** Si l'autorisation a été donnée, l'utilisateur doit se conformer aux règles et instructions édictées par son supérieur hiérarchique, ce dernier étant seul compétent pour déterminer les conditions d'utilisation du réseau social.
- 11.6** De plus, l'utilisateur devra :
- S'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein de Business France ;

- Répondre aux contributions des tiers avec pertinence, exactitude, en s'assurant de ne pas nuire à l'image de Business France ;
- Suivre les recommandations de la DCAP qui mettent à disposition des collaborateurs des outils pour les aider à gérer leurs comptes personnels (logo, contenus intéressants à partager, formations et bonnes pratiques, etc.) [Guide de bonnes pratiques Social Media DCAP](#)
- Respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle, en particulier sur l'utilisation d'images ou de vidéos) ;
- S'abstenir de diffuser toute information confidentielle ou toute information commerciale sensible relative à Business France ou à ses concurrents ;
- Veiller à la sécurité d'accès à son compte afin d'éviter toute usurpation d'identité qui pourrait être préjudiciable à l'image de l'agence et pour cela suivre les recommandations de la Direction des Systèmes d'information.
- S'abstenir de favoriser des actes de concurrence de la part de tiers.

11.7 En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra consulter son supérieur hiérarchique et la DCAP qui pourra le conseiller.

11.8 L'autorisation donnée pourra être retirée, modifiée ou suspendue par le supérieur hiérarchique dès lors que l'intérêt de Business France le justifie.

11.9 L'utilisateur devra prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour le système d'information de Business France, notamment en veillant à mettre en place les protections nécessaires à l'utilisation de son compte personnel pour être conforme aux articles 5, 6 et 7 de la présente Charte.

Usage non professionnel

11.10 Dans le cadre de la sphère non professionnelle et hors des murs de Business France, l'utilisateur est bien évidemment libre d'utiliser les réseaux sociaux, cependant il s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations confidentielles, des informations commerciales sensibles relatives à ses projets professionnels, l'Agence ou à ses concurrents, des informations relatives aux conditions de travail, à l'organisation générale, au calendrier d'événements, à la rémunération, etc..

11.11 L'utilisateur n'est autorisé à faire mention de son appartenance à Business France que sur les réseaux sociaux à caractère professionnel (notamment LinkedIn et X), et ce uniquement tant que l'utilisateur fait partie des effectifs de Business France.

Signalement

11.12 Qu'il utilise les réseaux sociaux à titre professionnel ou non professionnel, l'utilisateur pourra informer Business France d'un agissement de tiers susceptible de porter atteinte à la réputation de Business France ou à un droit de Business France (notamment de propriété intellectuelle) dont il aurait connaissance.

ARTICLE 12. UTILISATION DE L'INTELLIGENCE ARTIFICIELLE

- 12.1 Face aux besoins en outils d'intelligence artificielle pour certains métiers, l'Agence a mis à disposition des collaborateurs un outil d'intelligence artificielle intégré aux outils et applications bureautiques de l'Agence.
- 12.2 Afin de préserver les données de l'Agence, les utilisateurs doivent privilégier l'utilisation de Copilot. Le recours à d'autres outils d'IA génératives est toléré, dès lors que ne doivent pas être chargés dans ces outils des données propriété de l'Agence ou de ses clients, ou de données susceptibles de les identifier. Toute utilisation abusive d'outils externes relèverait alors de sanctions (comme précisé à l'article 19).
- 12.3 Les utilisateurs doivent être conscients que les réponses générées par l'intelligence artificielle peuvent être sujettes à des erreurs et de reproduire des biais. Il est de la responsabilité des utilisateurs de vérifier, corriger et valider les réponses avant de les partager en interne ou en externe.
- 12.4 Les utilisateurs devront veiller à ce que les productions issues de l'utilisation de l'outil d'intelligence artificielle respectent le droit de la propriété intellectuelle et ne contiennent aucun contenu discriminatoire ou offensant qui ne respecte pas les droits et libertés fondamentales.
- 12.5 La Direction des Systèmes d'Information se réserve le droit de surveiller de la bonne utilisation des outils d'IA, et le cas échéant de restreindre l'accès à des outils externes d'IA, pouvant mettre l'Agence en risque.

ARTICLE 13. DONNEES A CARACTERE PERSONNEL

13.1 – Devoirs des utilisateurs

- 13.1.1** Les utilisateurs sont informés de la nécessité de respecter les dispositions légales et réglementaires en matière de traitement automatisé ou non de données à caractère personnel.

Les salariés de l'Agence peuvent consulter la formation dispensée par Business France sur ce sujet (modules d'e-learning dans MyTalent + support disponible dans le référentiel documentaire / dossiers les essentiels de Business France / les essentiels juridiques / dispositif RGPD).

- 13.1.2** 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 qui feront l'objet des formalités préalables susvisées.

- 13.1.3** 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.

13.1.4 L'utilisateur veille, en cas d'opération de prospection directe par courrier électronique, à respecter les dispositions légales et réglementaires en vigueur.

13.1.5 Un Délégué à la Protection des Données a été nommé par Business France. Il tient à jour le registre des traitements de l'Agence et se porte fort de la conformité de l'Agence avec les exigences juridiques dédiées à la protection des données. Le DPO doit être saisi par tout utilisateur qui aurait une question sur ce sujet à l'adresse : rgpd-interne@businessfrance.fr. Tout collaborateur peut exercer ses droits sur le site suivant : <https://dpo.businessfrance.fr>.

13.2 – Droits des utilisateurs

13.2.1. Business France s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite.

13.2.2. 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.

13.2.3 Conformément à la loi « Informatique et Libertés » modifiée et au Règlement sur la Protection des Données (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et relève de la vie privée et du secret professionnel, 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, ou de la Direction administrative et financière dans tous les autres cas et notamment s'agissant des prestataires extérieurs.

La Charte des données personnelles des collaborateurs Business France est accessible sur [MyNet](#).

ARTICLE 14. PROPRIETE INTELLECTUELLE

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

14.2 En conséquence, chaque utilisateur doit :

- Respecter les conditions de licence souscrite par Business France ;
- Ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels Business France ne posséderait pas un droit d'usage ;
- Ne pas reproduire et utiliser les bases de données, pages web ou autres créations de Business France 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 Business France 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.

14.3 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 Direction des systèmes d'information.

ARTICLE 15. CONTROLE DU SYSTEME D'INFORMATION

15.1 La Direction des systèmes d'information a la charge de la qualité et de la sécurité du système d'information fournis aux utilisateurs. Par conséquent, et conformément à la PSSI (Politique des Systèmes d'Information) des contrôles sont mis en place, au titre de la sécurité 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 textes légaux et réglementaires en vigueur.

15.2 A ce titre, les utilisateurs sont informés que les administrateurs SI devant veiller au fonctionnement normal et à la sécurité des réseaux et systèmes informatiques, sont conduits, 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 dans le cadre de leurs fonctions. Néanmoins, ces administrateurs sont tenus à une obligation de discrétion et ne peuvent utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

En outre, Business France se réserve notamment le droit :

- De vérifier le trafic informatique entrant et sortant, 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 ;
- De conserver des fichiers de journalisation des traces de connexion globales ;
- De transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

15.3 En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts de l'Agence et/ou la sécurité du système d'information 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.

15.4 En outre, en cas d'incident, Business France se réserve le droit de :

- Surveiller le contenu des informations qui transitent sur le système d'information ;
- 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 de Business France.

15.5 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 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.

ARTICLE 16. VIDEOSURVEILLANCE

16.1 Les utilisateurs sont informés de la mise en place d'un système de vidéosurveillance dans les locaux de Business France.

16.2 La vidéosurveillance dite de « sécurité privée » est régie par :

- Les principes directeurs de la loi « Informatique et libertés » modifiée et du Règlement sur la Protection des Données (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et relève de la vie privée et du secret professionnel, dans la mesure où les activités de vidéosurveillance ne sont pas visées en tant que telles, à la différence, par exemple, des technologies de biométrie ;
- La délibération 94-056 du 21 juin 1994 portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et les lieux recevant le public. Cette disposition reste d'actualité, sous réserve des prescriptions de la loi 95-73 d'orientation et programmation relative à la sécurité du 21 janvier 1995 et de la loi Informatique et libertés du 6 août 2008 modifiée.

16.3 Ces dispositions visent :

- La prise de vue avec ou sans enregistrement ;
- La connexion avec des fichiers nominatifs.

16.4 Il est enfin rappelé que l'enlèvement ou la neutralisation des caméras de surveillance sans justificatif est strictement interdit.

ARTICLE 17. CONTROLE DES CONSOMMATIONS DE TELEPHONIE FIXE ET MOBILE

17.1 Les utilisateurs sont informés que Business France a mis en place un système de gestion de la téléphonie qui enregistre, à partir de chacun des postes téléphoniques fixes, les éléments de la communication (date, heure, durée, coût et numéros appelés), ainsi que pour les moyens informatiques et de communication électronique nomades (téléphone portable, tablette, etc.).

17.2 L'enregistrement en revanche des conversations téléphoniques est interdit sauf à en informer préalablement l'utilisateur, conformément à la loi dite « Informatique et libertés » modifiée.

ARTICLE 18. SAUVEGARDE ET ARCHIVAGE

Business France met à disposition des utilisateurs des espaces dédiés aux sauvegardes et à l'archivage sur des zones sécurisées.

Par conséquent Business France recommande à l'ensemble des collaborateurs le stockage et l'archivage de leur données sur les espaces prévus à ces effets (OneDrive)

Cet espace permet aux collaborateurs :

- Le Stockage de fichiers : OneDrive permet de sauvegarder des fichiers et des documents tels que des photos, des vidéos, des présentations, des feuilles de calcul, des fichiers audios, etc. dans le cloud.
- Le Partage de fichiers : Vous pouvez partager des fichiers et des dossiers stockés sur OneDrive avec d'autres personnes, que ce soit en leur envoyant un lien pour accéder aux fichiers ou en les invitant à collaborer directement sur les documents.
- La Collaboration en temps réel : OneDrive intègre des fonctionnalités de collaboration en temps réel, ce qui signifie que plusieurs personnes peuvent travailler ensemble sur un même document simultanément. Les modifications sont synchronisées en temps réel.
- La Synchronisation automatique : OneDrive est configuré pour synchroniser automatiquement les fichiers entre votre ordinateur et le cloud. Cela permet d'assurer que vos fichiers sont toujours sauvegardés et accessibles, même en cas de perte ou de panne de votre appareil.

ARTICLE 19. SANCTIONS

- 19.1** 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.
- 19.2** Les sanctions qui seraient prises par l'employeur ne sont pas exclusives d'éventuelles poursuites judiciaires à l'encontre des intéressés.
- 19.3.** En outre, l'utilisateur s'expose à des sanctions concernant son droit d'utiliser les moyens informatiques et de communication électronique mis à sa disposition.
- 19.4.** Ces sanctions peuvent consister, notamment, dans le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie de ces moyens. Il peut, le cas échéant, être également exclu des espaces collaboratifs de travail.

ARTICLE 20. ENTREE EN VIGUEUR

- 20.1** 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.
- 20.2** 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 Business France du fait de l'évolution de ces dernières, serait nulle de plein droit.