

Groupe Socfin - Charte d'utilisation des outils informatiques et de la boîte e-mail professionnelle

Département	Date effective	Version	Date révision
Informatique	Mai 2025	1.0	/

1. Introduction

Le but de la présente charte est de définir les droits et les devoirs des utilisateurs à propos des moyens de communication (Internet, messagerie électronique, téléphonie) et des postes de travail informatiques mis à leur disposition dans le cadre professionnel, de prévenir une utilisation abusive de ces derniers et de régler les conséquences d'éventuels abus.

Elle s'applique à tous les utilisateurs.

Elle vise à garantir la sécurité, l'efficacité et le respect des bonnes pratiques en matière d'usage des technologies de l'information.

2. Champ d'application

Cette charte s'applique à tous les employés, stagiaires, prestataires et toute autre personne ayant accès aux outils informatiques de Socfin ou de ses filiales.

3. Utilisation des outils informatiques

3.1 Utilisation professionnelle

Les outils informatiques doivent être utilisés à des fins professionnelles. Toute utilisation personnelle doit être occasionnelle et ne doit pas interférer avec les responsabilités professionnelles.

3.2 Sécurité des systèmes

- Sécurisez vos appareils électroniques, en particulier le matériel portable (ordinateur portable, tablette, téléphone) lorsque vous vous absentez de votre poste de travail ou lors de déplacements ;
- Seules les personnes autorisées ont accès aux serveurs et autres installations informatiques ;
- Ne partagez pas vos identifiants et mots de passe ;
- Choisir des mots de passe comportant au moins 8 caractères (lettres majuscules et minuscules, chiffres et symboles) ;
- Il est recommandé de changer le mot de passe tous les 90 jours ;
- Ne pas enregistrer les mots de passe non codés dans un agenda, portefeuille ou communiquer ceux-ci par e-mail, messages ou autre plateforme publique ;
- Utiliser un logiciel de gestion de mot de passe ;
- Verrouillez votre poste de travail lorsque vous quittez votre place de travail (bouton Windows+L) ;

- Signalez immédiatement toute activité suspecte ou toute tentative d'accès non autorisé à votre hiérarchie et au Département Informatique par le biais d'un JIRA.

3.3 Installation de logiciels

L'installation d'un logiciel doit être validé explicitement par le Département Informatique du Groupe.

Il est notamment interdit de :

- Modifier la configuration matérielle du poste de travail en retirant ou en installant de nouveaux composants (par exemple : graveur, disque supplémentaire, lecteur DVD, CD-ROM, modem, imprimante, etc.) ;
- Connecter au poste de travail ou sur le réseau des appareils électroniques sans autorisation (agendas électroniques, téléphones portables, PC portables, matériel USB, appareils multimédia, appareils photos, vidéo, MP3, etc.) ;
- Modifier la configuration logicielle du poste de travail en retirant des programmes ou en installant des programmes téléchargés depuis Internet ou reçus par courrier électronique ou en provenance de toute autre source.

Il est important de noter que les développements informatiques sont sujets à l'approbation du Département IT du Groupe.

3.4 Respect de la législation

Ne consultez, ni ne stockez ou ne diffusez des informations qui, sous quelque forme que ce soit, constituent notamment une participation à un acte illicite ou qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, incitent à la haine raciale ou constituent une apologie du crime ou de la violence.

L'utilisation des outils informatiques doit être conforme aux lois en vigueur, notamment celles relatives à la propriété intellectuelle, la protection des données personnelles et la cybercriminalité.

4. Utilisation de la boîte e-mail professionnelle

4.1 Communication professionnelle

L'utilisation du courrier électronique comme instrument de communication est réservée aux besoins professionnels.

L'envoi d'e-mails personnels doit rester exceptionnel et doivent être clairement marqués comme étant privés.

4.2 Confidentialité

- Les informations confidentielles doivent être protégées, le Département IT sera en charge de trouver des solutions adéquates en fonction du contexte, des data, etc. ;
- Utilisez le cryptage pour les envois sensibles (voir Département IT) ;
- Ne partagez pas de données confidentielles à des adresses e-mail non professionnelles ;

- Pour des raisons de confidentialité et de sécurité, il est fortement conseillé de ne pas transférer des courriers électroniques à caractère professionnel de son adresse professionnelle à son adresse privée ;
- Vérifiez la validité des adresses e-mail avant de transférer des données sensibles ou confidentielles.

4.3 Gestion des e-mails

- Sauvegardez les pièces jointes volumineuses et éliminez celles-ci de votre boîte e-mail ;
- Évitez de saturer les boîtes e-mail de vos collègues avec des pièces jointes volumineuses ou non-essentiels.

4.4 Contenu des e-mails

- Soyez attentif au fait qu'un courrier électronique peut se transmettre très rapidement et qu'il y a lieu d'être très prudent avec les informations qu'il véhicule, ceci spécialement pour des fichiers attachés à caractère confidentiel.
- Ne diffusez pas de contenus offensants, discriminatoires ou illégaux.

4.5 Signature des e-mails professionnels

Les signatures de courrier électronique doivent être établies conformément aux normes de communication et de logo de Socfin. Les employés doivent s'abstenir d'ajouter à leur signature des éléments qui ne reflètent pas l'image professionnelle de Socfin.

4.6 Accès aux boîtes e-mail par la Direction ou des personnes tierces

Socfin et les prestataires de Département Informatique se réservent le droit d'accéder à la messagerie professionnelle des employés à tout moment et sans préavis, dans le cadre de ses activités de gestion et de sécurité et si la loi le permet. L'accès à la boîte e-mail est toutefois uniquement en lecture.

4.7 Messages à caractère confidentiel ou privé

Les mentions suivantes doivent être utilisées dans les éléments d'adressage, concernant la confidentialité ou le caractère privé/personnel d'un courrier électronique :

- **CONFIDENTIEL** : un courrier électronique dont les éléments d'adressage contiennent ce mot ne peut être ouvert que par les personnes ayant un accès explicite à la boîte aux lettres. Le traitement de l'information doit être traité de la même manière qu'un courrier confidentiel papier.
- **PRIVE** ou **PERSONNEL** : un courrier électronique dont les éléments d'adressage contiennent un de ces mots ne peut être ouvert que par la personne à qui le courrier électronique est destiné (dont le nom figure dans le texte ou fait partie de la désignation de la boîte aux lettres). Il ne doit contenir aucune information professionnelle.

Sans aucune précision, le courrier électronique pourra être lu par des tierces personnes.

L'utilisateur doit informer les personnes susceptibles d'envoyer un message à caractère privé ou confidentiel de l'indiquer dans le titre du message.

Les employés ont la responsabilité d'éliminer les messages à caractère privé de leur boîte e-mail de manière régulière.

Toutefois, même les e-mails marqués comme privés et confidentiels peuvent être consultés par la Direction dans des cas de soupçon d'actes malveillants envers les intérêts de l'entreprise ou contraires à la législation.

4.8 Sécurité

Les employés doivent toujours être vigilants afin de détecter les courriels contenant des logiciels malveillants ou des tentatives d'hameçonnage.

Nous demandons aux employés :

- D'éviter d'ouvrir les pièces jointes et de cliquer sur les liens lorsque le contenu n'est pas expliqué de manière adéquate (par exemple : « Regardez cette vidéo, elle est incroyable ») ;
- De se méfier des titres « clickbait » (appâts à clics) ;
- De vérifier les courriels et les noms des expéditeurs inconnus pour s'assurer qu'ils sont légitimes ;
- De rechercher les incohérences ou les signaux d'alerte stylistiques (par exemple : fautes de grammaire, majuscules, nombre excessif de points d'exclamation).

Si un employé n'est pas sûr qu'un courriel qu'il a reçu est sûr, il ne doit pas l'ouvrir et en référer à son Département Informatique.

5. Internet et réseaux sociaux

5.1 Navigation sur Internet

L'accès à Internet doit être utilisé de manière responsable.

Les sites à caractère illégal ou inapproprié sont strictement interdits.

Internet doit être utilisé pour la recherche et la diffusion d'informations à but professionnel.

Une utilisation privée est admise en dehors du temps de travail, dans la mesure où elle est limitée à un volume (temps et données) raisonnable et qu'elle respecte le devoir de fidélité.

L'employeur se réserve le droit de bloquer, sans préavis, l'accès à certaines catégories de sites Internet, notamment :

- Sites de messagerie non professionnelle, y compris site de messagerie instantanée (« chat ») ;
- Sites de transactions financières (notamment les sites boursiers) ou ceux payants ;
- Sites de jeux et de paris ;
- Sites à caractère érotique, violent, raciste ou contraire aux mœurs de quelque manière que ce soit ;
- Sites qui sollicitent trop fortement les systèmes d'information (par exemple : connexion à des sites de vidéo ou radiophoniques).

5.2 Réseaux sociaux

L'utilisation des réseaux sociaux pendant les heures de travail doit être limitée.

Toute communication faite au nom de l'entreprise sur les réseaux sociaux doit être approuvée par la Direction.

6. Téléphonie

Les moyens de téléphonie (téléphones fixes, mobiles, messageries vocales, etc.) sont mis à disposition pour un usage professionnel, y compris pour un accès à la boîte vocale ou l'internet.

L'utilisation personnelle doit rester exceptionnelle et ne doit en aucun cas perturber l'activité professionnelle.

6.1 Utilisation des téléphones mobiles

Les téléphones mobiles fournis par l'organisation doivent être utilisés principalement pour des communications professionnelles.

Les applications et les services installés sur les téléphones mobiles doivent être approuvés par le Département Informatique.

Les employés sont responsables de la bonne garde et de l'entretien des téléphones mobiles mis à leur disposition.

Soyez attentif aux charges élevées pour l'utilisation de données mobiles à l'étranger.

6.2 Confidentialité et sécurité

Protéger les informations confidentielles pendant les appels téléphoniques.

Ne pas divulguer d'informations sensibles ou confidentielles par téléphone sans les précautions nécessaires.

Les téléphones doivent être protégés par un mot de passe ou une méthode d'authentification sécurisée.

7. Protection des données

7.1 Données personnelles

Respectez la confidentialité des données personnelles des employés et des clients (voir Politique de protection des données personnelles).

Toute collecte ou traitement de ces données doit être conforme au Règlement Général sur la Protection des Données (RGPD).

7.2 Sauvegarde des données

Les données stockées sur les postes (ordinateurs, téléphones, etc.) ne sont pas sauvegardées par le Service IT ; la perte/vol/casse de ces matériels entraîne de facto la perte des données stockées sur ces matériels et constitue ainsi un préjudice pour l'entreprise.

Il est donc fortement recommandé d'enregistrer vos données uniquement sur les serveurs ou applications mis à disposition par l'entreprise.

8. Contrôles et sanctions

8.1 Contrôles

L'entreprise se réserve le droit de contrôler l'utilisation des outils informatiques et de la boîte e-mail professionnelle afin de s'assurer du respect de cette charte.

8.2 Sanctions

Tout manquement à cette charte pourra entraîner des sanctions disciplinaires pouvant aller jusqu'au licenciement, selon la gravité des faits.

9. Evolution de la charte

Cette charte peut être modifiée en fonction des évolutions législatives et technologiques. Les utilisateurs seront informés de toute mise à jour.

10. Acceptation de la charte

En utilisant les outils informatiques et la boîte e-mail professionnelle de l'entreprise, chaque utilisateur accepte automatiquement les termes de cette charte.

Pour toute question ou clarification concernant cette charte, veuillez contacter le Département Informatique, les ressources humaines ou bien encore le département conformité.

Cette charte a pour but de fournir un cadre clair et précis pour l'utilisation des outils informatiques au sein de l'entreprise, favorisant ainsi un environnement de travail sécurisé et professionnel.

Annexe 1 - Lignes directrices de Socfin sur l'utilisation des médias sociaux

Résumé et objectif de la ligne directrice

Le guide d'utilisation des médias sociaux de Socfin fournit un cadre pour l'utilisation des médias sociaux. Les médias sociaux sont un lieu où les gens échangent des informations, des opinions et des expériences pour apprendre, se développer et s'amuser. Que vous gériez un compte d'entreprise ou que vous utilisiez votre propre compte, vous devez éviter de nuire à notre organisation de quelque manière que ce soit. Cette ligne directrice fournit des conseils pratiques pour éviter les problèmes qui pourraient résulter d'une utilisation imprudente des médias sociaux sur le lieu de travail.

Champ d'application

Il est attendu de tous nos employés permanents ou contractuels, partenaires, prestataires, stagiaires qu'ils respectent cette ligne de conduite.

Par « médias sociaux », nous entendons toute une série de communautés en ligne telles que les blogs, les réseaux sociaux et les forums - et pas seulement des plateformes telles que Facebook ou X.

Cette ligne de conduite s'articule autour de 2 éléments différents : d'une part, l'utilisation des médias sociaux personnels concernant l'entreprise et, d'autre part, la représentation de notre entreprise par le biais des médias sociaux.

Éléments de la ligne directrice

Utilisation des médias sociaux personnels

Les employés sont autorisés à accéder à leurs comptes personnels au travail. Mais il est attendu que tous agissent de manière responsable et de veiller à ce que la productivité ne soit pas affectée.

L'utilisation des comptes à des fins personnelles doit rester dans les limites du raisonnable.

Il est également demandé de faire preuve de prudence lorsque vous publiez des messages sur les médias sociaux. Nous ne pouvons pas restreindre ce que vous y publiez, mais il est attendu que vous respectiez à tout moment nos politiques de confidentialité. Il est également rappelé de ne pas enfreindre nos politiques de lutte contre le harcèlement, nous conseillons à nos employés de :

- De veiller à ce que les autres sachent que leur compte personnel ou leurs déclarations ne représentent pas notre entreprise. Vous ne devez pas affirmer ou laisser entendre que vos opinions et contenus personnels sont autorisés ou approuvés par notre entreprise. Nous conseillons d'utiliser une clause de non-responsabilité telle que « mes opinions sont les miennes » afin d'éviter tout malentendu.
- Évitez de partager la propriété intellectuelle, sur un compte personnel sans autorisation. Les politiques de confidentialité et l'image de la société et les lois s'appliquent toujours.
- Évitez tout contenu diffamatoire, offensant ou désobligeant. Il peut être considéré comme une violation de la politique anti-harcèlement de notre entreprise, s'il est dirigé vers des collègues, des clients ou des partenaires.

Représentation de notre entreprise

Certains employés représentent notre entreprise en gérant des comptes de médias sociaux d'entreprise ou en s'exprimant au nom de notre entreprise. Lorsque vous êtes responsable d'un compte de médias sociaux d'entreprise, il est attendu d'agir avec prudence et responsabilité afin de protéger l'image et la réputation de notre entreprise. Vous devez

- Être respectueux, poli et patient lorsque vous participez à des conversations au nom de Socfin. Vous devez être particulièrement prudent(e) lorsque vous faites des déclarations ou des promesses à l'égard des clients et des parties prenantes.
- Éviter, dans la mesure du possible, de s'exprimer sur des sujets qui ne relèvent pas de votre domaine d'expertise. Chacun doit veiller à ne pas répondre à des questions ou faire des déclarations qui relèvent de la responsabilité de quelqu'un d'autre.
- Suivez notre politique de confidentialité et de protection des données et respectez les lois sur les droits d'auteur, les marques déposées, le plagiat et l'utilisation équitable.
- Informez le Département Communication du Groupe lorsque vous vous apprêtez à partager un contenu à fort impact.
- Éviter de supprimer ou d'ignorer des commentaires sans raison. Il faut écouter les critiques et y répondre.
- Ne jamais publier de contenu ou de commentaires discriminatoires, offensants ou diffamatoires.
- Corriger ou supprimer tout contenu trompeur ou faux le plus rapidement possible.

Conséquences disciplinaires

Nous nous efforçons de surveiller toutes les publications sur les médias sociaux.

Nous pourrions être amenés à prendre des mesures disciplinaires pouvant aller jusqu'au licenciement si les employés ne respectent pas cette ligne de conduite. Les exemples de non-conformité à la politique de l'employé en matière de médias sociaux sont notamment les suivants :

- Ne pas tenir compte des responsabilités professionnelles et des délais pour utiliser les médias sociaux au travail.
- Divulguer des informations confidentielles par le biais de comptes personnels ou d'entreprise.
- Faire des commentaires offensants à l'égard du groupe ou d'autres membres de la communauté en ligne.

Annexe 2 - Lignes directrices de Socfin concernant l'utilisation d'Internet

Résumé et objectif de la directive

Les lignes directrices relatives à l'utilisation d'Internet par les employés décrivent les conditions d'utilisation de la connexion Internet, du réseau et de l'équipement de l'entreprise. Nous voulons éviter toute utilisation inappropriée ou illégale d'Internet qui créerait des risques pour la légalité et la réputation de notre entreprise.

Champ d'application

Les présentes lignes directrices relatives à l'utilisation d'Internet par les employés s'appliquent à l'ensemble de nos employés, contractants, bénévoles et partenaires qui ont accès à notre réseau et à nos ordinateurs.

Éléments de la ligne directrice relative à l'utilisation d'Internet par les employés

Qu'est-ce qu'une utilisation appropriée d'Internet par les employés ?

Il est conseillé à nos employés d'utiliser la connexion Internet de notre entreprise pour les raisons suivantes :

- Pour accomplir leurs tâches professionnelles.
- Pour rechercher des informations qu'ils peuvent utiliser pour améliorer leur travail.

Nous ne voulons pas restreindre l'accès de nos employés aux sites Internet de leur choix, mais nous attendons d'eux qu'ils fassent preuve de discernement et qu'ils restent productifs au travail lorsqu'ils utilisent Internet.

Toute utilisation de notre réseau et de notre connexion doit être conforme à notre politique de confidentialité et de protection des données.

Les employés doivent :

- Garder leurs mots de passe secrets à tout moment.
- Se connecter à leurs comptes d'entreprise uniquement à partir d'appareils sûrs.
- Utiliser des mots de passe forts pour se connecter aux sites Internet et aux services liés au travail.

Qu'est-ce qu'une utilisation inappropriée d'Internet par un employé ?

- Télécharger du matériel obscène, offensant ou illégal.
- Envoyer des informations confidentielles à des destinataires non autorisés.
- Porter atteinte à la vie privée et aux informations sensibles d'une autre personne.
- Télécharger des films, de la musique et d'autres documents et logiciels protégés par des droits d'auteur.
- Visiter des sites Internet potentiellement dangereux qui peuvent compromettre la sécurité de notre réseau et de nos ordinateurs.
- Effectuer des actions non autorisées ou illégales, comme le piratage, la fraude, l'achat/la vente de biens illégaux, etc.

Nous conseillons également à nos employés d'être prudents lorsqu'ils téléchargent et ouvrent/exécutent des fichiers et des logiciels. S'ils ne sont pas sûrs qu'un fichier soit sûr, ils doivent s'adresser au Département Informatique.

Socfin peut installer des logiciels antivirus et de cryptage de disque sur les ordinateurs de l'entreprise. Les employés ne peuvent pas désactiver ou configurer les paramètres et les pare-feux sans l'approbation de leur supérieur.

Nous n'assumerons aucune responsabilité si les appareils des employés sont infectés par des logiciels malveillants ou si leurs données personnelles sont compromises à la suite d'une utilisation inappropriée par les employés.

Courrier électronique

Voir procédure d'accès aux boîtes e-mails.