

Groupe Socfin - Politique de cybersécurité

Département	Date effective	Version	Date révision
Compliance	Mai 2025	1.0	/

1. Introduction

La politique de Socfin en matière de cybersécurité décrit nos lignes directrices et nos dispositions pour préserver la sécurité de nos données et de notre infrastructure technologique.

Plus nous nous appuyons sur la technologie pour collecter, stocker et gérer des informations, plus nous sommes vulnérables à de graves atteintes à la sécurité. Les erreurs humaines, les attaques de pirates informatiques et les dysfonctionnements des systèmes peuvent causer d'importants dommages financiers et compromettre la réputation de notre entreprise.

La présente politique de cybersécurité établit un cadre cohérent pour garantir la sécurité des informations et des ressources technologiques au sein du siège de Socfin et de ses filiales en Afrique, en Asie et en Europe. Cette politique vise à préserver la confidentialité, l'intégrité et la disponibilité tout en tenant compte des réglementations régionales et des nuances culturelles.

Les technologies de l'information évoluent constamment et rapidement avec de nouveaux matériels, logiciels, réseaux et menaces. Cette politique fera donc l'objet de mises à jour régulières basées sur le savoir-faire des experts en technologie ainsi que sur le retour d'information des utilisateurs de la technologie.

Les technologies de l'information sont là pour aider les employés et les partenaires de Socfin à accomplir leur travail de la manière la meilleure et la plus efficace possible. La présente politique de cybersécurité vise à définir un équilibre optimal entre la convivialité et la sécurité.

2. Objectif

L'objectif de cette politique est de :

- Promouvoir une approche holistique de la gestion de la sécurité des technologies de l'information au sein des entités de Socfin,
- Protéger les informations et la technologie de Socfin contre la compromission de la confidentialité, de l'intégrité et de la disponibilité :
 - La confidentialité a pour objectif de s'assurer que l'information n'est accessible qu'à ceux et celles dont l'accès est autorisé,
 - L'intégrité a pour objectif de s'assurer de l'exactitude et l'intégralité de l'information et des méthodes de traitement de celle-ci,
 - La disponibilité a pour objectif de s'assurer que l'information ou le système qui l'utilise soit accessible selon les critères définis.
- Sensibiliser les parties prenantes à la sécurité de l'information et aux risques inhérents à l'utilisation des technologies de l'information,

- Soutenir la vision stratégique de Socfin par une approche équilibrée entre la sécurité et la facilité d'utilisation,
- Favoriser une culture de la sécurité au sein de Socfin et promouvoir une approche de la sécurité des technologies de l'information qui relève de la responsabilité de chacun.

3. Champ d'application

Cette politique s'applique à l'ensemble de nos employés, contractants, stagiaires, bénévoles et à toute personne ayant un accès permanent ou temporaire à nos systèmes et à notre matériel.

4. Définitions

Technologies de l'Information : Le terme « TI » est un terme général qui inclut le matériel (computer), les logiciels, les réseaux et l'infrastructure de soutien pour gérer et fournir des informations en utilisant des données, de l'audio ou de la vidéo.

Matériel informatique : Comprend les dispositifs et équipements externes et internes qui vous permettent d'exécuter les principales fonctions telles que l'entrée et la sortie de données, le stockage, la communication, le traitement, etc.

Logiciel : Ensemble d'instructions, de données ou de programmes utilisés pour faire fonctionner les « ordinateurs » et exécuter des tâches spécifiques.

Appareils numériques : Il s'agit d'appareils qui exécutent des processus, des calculs et des opérations sur la base d'instructions reçues de programmes logiciels ou matériels, et qui stockent aussi souvent des informations. Tous les appareils numériques ou ordinateurs comprennent généralement un processeur et une mémoire qui peuvent prendre la forme d'un ordinateur de bureau, d'un ordinateur portable, d'une tablette et d'un smartphone, mais par extension, on les trouve également dans des machines telles que les photocopieuses, les imprimantes, les scanners, les voitures, les radios, les télévisions, etc.

Données informatiques : Comprend toutes les formes d'informations numériques telles que les données, les documents, les images, les enregistrements audio et vidéo, les listes, etc. stockées sur des ordinateurs, des serveurs, des disques durs, un stockage virtuel (dans le cloud), etc.

Authentification : Il s'agit d'une méthode d'identification utilisée pour obtenir l'accès à une zone restreinte, qu'elle soit physique (bureau, laboratoire, salle des serveurs, imprimante, scanner, etc.), informatique (connexion de démarrage, suppression de l'économiseur d'écran, etc.) ou virtuelle (serveur ou compte de messagerie, réseau, stockage dans le cloud, etc.) L'authentification peut prendre la forme d'une clé physique, d'un mot de passe, d'un jeton, d'un lecteur de carte, de données biométriques, etc. tant qu'elle est individuelle et unique.

Internet : Système mondial de réseaux informatiques interconnectés, dans lequel, sous réserve d'autorisation, des informations sont partagées entre les ordinateurs et qui permet aux utilisateurs de se connecter, d'échanger des informations.

Virus : Type de logiciel malveillant qui se propage entre les ordinateurs et endommage les données et les logiciels.

Intelligence Artificielle : « L'IA » est la simulation des processus de l'intelligence humaine par des machines, en particulier des systèmes informatiques. Certains logiciels d'IA sont accessibles au public et peuvent être utilisés pour générer, trier ou analyser des documents, ou pour créer, modifier ou altérer des dessins ou des images.

Employés à distance ou télétravail : Il s'agit d'employés travaillant à domicile ou en dehors du bureau lors d'un voyage d'affaires et ayant un accès à distance au réseau informatique de Socfin.

5. Éléments de la politique

5.1 Données confidentielles

Les données confidentielles sont secrètes et précieuses. Les exemples les plus courants sont les suivants :

- Informations financières non publiées,
- Données de clients/partenaires/fournisseurs,
- Informations personnelles sur les employés,
- Informations sur la recherche et les technologies exclusives,
- Les listes de clients (existants et potentiels).

Tous les employés sont tenus de protéger ces données. Dans cette politique, nous donnerons à nos employés des instructions sur la manière d'éviter les failles de sécurité.

5.2 Protéger les appareils personnels et ceux de l'entreprise

Le premier niveau de sécurité dans les technologies de l'information consiste à s'assurer que seules les personnes autorisées ont accès aux appareils numériques ou aux terminaux.

Des méthodes d'authentification individuelles doivent être utilisées sur tous les appareils numériques utilisés par les employés de Socfin, qu'ils soient d'entreprise ou privés, qui donnent accès aux données de Socfin ou qui peuvent être reliés au réseau de Socfin sous quelque forme que ce soit. En particulier, l'accès aux ordinateurs portables, aux tablettes et aux smartphones doit être protégé par des méthodes d'authentification individuelles et uniques.

Les droits d'accès des employés à des fichiers spécifiques et à des zones de stockage de données collectives sont adaptés aux rôles et responsabilités de chaque individu au sein de chaque filiale.

Les employés ne doivent pas partager leurs mots de passe avec d'autres personnes et ne doivent pas utiliser l'authentification d'autres employés pour accéder aux fichiers de Socfin.

Lorsque les employés utilisent leurs appareils numériques pour accéder aux e-mails ou aux comptes de l'entreprise, ils introduisent un risque de sécurité pour nos données. Nous conseillons à nos employés de sécuriser leurs ordinateurs, tablettes et téléphones portables, qu'ils soient personnels ou fournis par l'entreprise. Pour ce faire, ils doivent :

- Protéger tous les appareils par un mot de passe adéquat (avec double authentification si possible),
- Signaler tout message concernant l'antivirus,
- Veiller à ne pas laisser leurs appareils exposés ou sans surveillance,
- Se connecter aux comptes et systèmes de l'entreprise uniquement via des réseaux sécurisés et privés,
- Passer sous contrôle anti-virus tout périphérique (USB, disque externe, CD) au moment d'être inséré dans un matériel informatique, surtout si celui-ci est connecté au réseau local.

Nous conseillons également à nos employés d'éviter d'accéder aux systèmes et comptes internes à partir des appareils d'autres personnes ou de prêter leurs propres appareils à d'autres personnes.

Lorsque les employés reçoivent un équipement fourni par l'entreprise, ils reçoivent des instructions pour :

- Activer le réseau virtuel (VPN),
- Mots de passe e-mail, Citrix et réseau local.

Ils doivent suivre les instructions pour protéger leurs appareils et s'adresser à notre Département Informatique s'ils ont des questions.

5.3 Protéger les e-mails

Les e-mails contiennent souvent des escroqueries et des logiciels malveillants (par exemple : virus). Pour éviter l'infection par un virus ou le vol de données, nous demandons aux employés de :

- Eviter 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 »),
- Se méfier des titres qui incitent à cliquer (par exemple : offrir des prix, des conseils),
- Vérifiez l'adresse électronique et le nom des personnes qui vous ont envoyé un message afin de vous assurer de leur légitimité,
- Recherchez les incohérences ou les indices (fautes de grammaire, majuscules, nombre excessif de points d'exclamation, etc.).

Si un employé n'est pas sûr d'un e-mail qu'il a reçu est sûr, il peut s'adresser à notre Département Informatique.

5.4 Gérer correctement les mots de passe

Les fuites de mots de passe sont dangereuses car elles peuvent compromettre l'ensemble de notre infrastructure. Non seulement les mots de passe doivent être sécurisés afin de ne pas être facilement piratés, mais ils doivent également rester secrets. C'est pourquoi nous conseillons à nos employés de :

- Choisir des mots de passe comportant au moins 8 caractères (lettres majuscules et minuscules, chiffres et symboles) et d'éviter les informations qui peuvent être facilement devinées (par exemple : les anniversaires),

- Mémoriser les mots de passe et ne pas les écrire. Si les employés doivent écrire leurs mots de passe, ils sont tenus de garder le document papier ou numérique confidentiel et de le détruire une fois leur travail terminé,
- Se souvenir d'un grand nombre de mots de passe peut être décourageant. Le Département Informatique pourra recommander les services d'un outil de gestion des mots de passe qui génère et stocke les mots de passe. Les employés sont tenus de créer un mot de passe sûr pour l'outil lui-même, en suivant les conseils susmentionnés.

5.5 Transférer les données en toute sécurité

Le transfert de données présente un risque pour la sécurité. Les employés doivent :

- Éviter de transférer des données sensibles (par exemple : des informations sur les clients, des dossiers d'employés) vers d'autres appareils ou comptes, sauf en cas d'absolue nécessité. Lorsqu'un transfert massif de ces données est nécessaire, nous demandons aux employés de demander l'aide de notre Département Informatique,
- Partager des données confidentielles sur le réseau/système de l'entreprise et non par le biais d'un réseau Wi-Fi public ou d'une connexion privée,
- S'assurer que les destinataires des données sont des personnes ou des organisations dûment autorisées et qu'ils disposent de politiques de sécurité adéquates.

Notre Département Informatique doit être informé des tentatives d'escroqueries, des atteintes à la vie privée et des logiciels malveillants afin de pouvoir mieux protéger notre infrastructure. C'est pourquoi nous conseillons à nos employés de signaler dès que possible à nos spécialistes les attaques perçues, les e-mails suspects ou les tentatives d'hameçonnage. Notre Département Informatique doit enquêter rapidement, résoudre le problème et envoyer une alerte à l'ensemble de l'entreprise si nécessaire.

Nos spécialistes de la sécurité sont chargés de conseiller les employés sur la manière de détecter les e-mails frauduleux. Nous encourageons nos employés à contacter le Département Informatique pour toute question ou préoccupation.

5.6 Mesures supplémentaires

Pour réduire les risques de failles de sécurité, nous demandons également à nos employés de :

- Eteindre leurs écrans et de verrouiller leurs appareils lorsqu'ils quittent leur bureau,
- Signaler le plus rapidement possible les équipements volés ou endommagés au Départements Admin & RH et Informatique,
- Changer tous les mots de passe des comptes dès qu'un appareil est volé,
- Signaler une menace perçue ou une éventuelle faiblesse de sécurité dans les systèmes de l'entreprise,
- S'abstenir de télécharger des logiciels suspects, non autorisés ou illégaux sur l'équipement de l'entreprise,
- Éviter d'accéder à des sites Internet suspects.

Nous attendons également de nos employés qu'ils respectent nos directives relatives aux médias sociaux et à l'utilisation d'Internet (voir « Charte informatique »).

6. Mise au rebut des équipements

Les procédures de mise au rebut des équipements doivent être conformes aux réglementations régionales en matière d'environnement ainsi que les règles comptables groupe. Avant la mise au rebut, le Département Informatique s'assurera que toutes les données, logiciels et protocoles d'identification de Socfin ont été supprimés de manière sûre et permanente de l'appareil numérique.

Les méthodes de destruction des données doivent être conformes aux lois locales sur la confidentialité et la protection des données.

7. Accès à distance

Les employés travaillant à distance doivent également suivre les instructions de cette politique. Étant donné qu'ils accèdent à distance aux comptes et aux systèmes de notre entreprise, ils sont tenus de respecter toutes les normes et tous les paramètres de cryptage et de protection des données, et de veiller à ce que leur réseau privé soit sécurisé.

Nous les encourageons à demander conseil à notre Département Informatique.

8. Mesures disciplinaires

Nous attendons de tous nos employés qu'ils respectent toujours cette politique et ceux qui causent des violations de la sécurité peuvent faire l'objet de mesures disciplinaires. Nous examinerons chaque incident au cas par cas.

En outre, les employés qui ne respectent pas les consignes de sécurité feront l'objet de mesures disciplinaires.