CHARTE D'UTILISATION

I-AR-01-V1

Date	Version	Elaboré par	Vérifié par	Validé par
30/07/2025	I-AR-01-V1	Dina HAKIM	Éric CHIPENG FAT	Jamal ALAYOUD

Cette Charte a pour objectifs spécifiques de :

- Promouvoir la sécurité des informations au sein de l'entreprise.
- Prévenir les comportements à risque et les abus des systèmes d'information.
- Sensibiliser les utilisateurs à la confidentialité et à la protection des données et ressources numériques.

Les employés et utilisateurs de ALEF Security ont accès aux ressources informatiques mises à leur disposition par l'entreprise, et cette Charte définit les règles d'utilisation de ces ressources de manière transparente.

I- Utilisateurs Concernés

La Charte s'applique à tous les utilisateurs des systèmes d'information de ALEF Security, y compris
:

- Les dirigeants
- Les salariés permanents
- Les stagiaires
- Les alternants
- Les employés prestataires
- Les partenaires externes
- Les clients et visiteurs

Il est de la responsabilité des salariés de veiller à ce que toute personne à qui ils permettent l'accès au système d'information accepte cette Charte.

II- Périmètre du Système d'Information

Le système d'information de ALEF Security comprend :

- Ordinateurs
- Téléphones
- Réseau informatique (routeurs, connectique)
- Photocopieurs
- Logiciels(antivirus)
- Données informatisées
- Messagerie
- Autres actifs numériques

Tout matériel connecté au système d'information, y compris le matériel personnel, est régi par la Charte.

III- Règles Générales d'Utilisation

1. **Utilisation Professionnelle** : Les systèmes d'information de l'entreprise doivent être utilisés principalement à des fins professionnelles. Les usages personnels sont accep- tés uniquement dans les conditions précisées par cette Charte ou en conformité avec la législation en vigueur.
2. **Interdiction de Concurrence** : Il est formellement interdit d'utiliser les systèmes d'information pour mener des activités concurrentielles ou toute autre activité susceptible de nuire aux intérêts de l'entreprise.

IV-Protection des Données Personnelles (RGPD)

1. **Responsabilités** : ALEF Security s'engage à respecter les exigences du RGPD et de la loi Informatique et Libertés dans la gestion des données personnelles.
2. **Principes** :

    - **Finalité** : Les données doivent être collectées et traitées uniquement pour des finalités spécifiques, légales et nécessaires.
    - **Minimisation** : Accéder uniquement aux données nécessaires à l'accomplissement des missions.
    - **Durée de Conservation** : Conserver les données seulement pendant la période nécessaire pour atteindre les finalités de traitement.
    - **Confidentialité** : Assurer la confidentialité et l'intégrité des données en mettant en place des mesures de sécurité appropriées.
    - **Notification** : Signaler toute violation de données à caractère personnel à la direction, selon les procédures internes.
    - **Droits des Personnes** : Respecter les droits des personnes concernées, y compris le droit d'accès, de rectification et de suppression des données.

V- Sécurité Informatique

1. **Responsabilité et Prudence** : Les utilisateurs doivent faire preuve de prudence et de responsabilité dans l'utilisation des ressources informatiques.
2. **Confidentialité** : Préserver la confidentialité des informations, notamment des données personnelles.
3. **Mot de Passe** : Les mots de passe doivent être complexes, gardés secrets et renouvelés régulièrement.
4. **Verrouillage de Session** : Verrouiller la session lorsque l'on quitte son poste de travail.
5. **Installation de Logiciels** : Ne pas installer ou modifier des logiciels sans autorisation.
6. **Copie de Données** : Respecter les procédures pour les copies de données, obtenir les autorisations nécessaires et suivre les règles de sécurité.

VI- Modalités d'Utilisation des Ressources Informatiques

1. **Postes de Travail** : Utiliser les postes de travail principalement pour les tâches professionnelles et manipuler les ressources avec soin pour éviter toute perte ou détérioration.
2. **Applications** : Utiliser les applications conformément aux besoins professionnels. Les demandes d'accès à de nouvelles applications doivent être validées par le service informatique.
3. **Téléphonie Mobile** : Utiliser les téléphones mobiles fournis principalement pour les communications professionnelles. Les appels et messages personnels doivent rester raisonnables.
4. **Support Amovible** : L'utilisation de supports amovibles doit respecter les règles de sécurité en vigueur et nécessiter l'approbation préalable du supérieur hiérarchique.

VII- Accès à Internet

1. **Accès Autorisé** : L'accès à Internet est autorisé pour les besoins professionnels. Cer- tains sites peuvent être restreints pour des raisons de sécurité.
2. **Sites Interdits** : L'accès à des sites non professionnels (jeux, streaming, réseaux so- ciaux personnels) est limité. Respecter les politiques de sécurité en vigueur.

VIII- Utilisation des emails

1. **Email Professionnel** : Les messages envoyés ou reçus via l'adresse email professionnelle sont présumés professionnels.
2. **Emails Personnels** : Les emails personnels doivent être clairement identifiés comme tels (mention "PRIVE" dans l'objet) et classés dans un répertoire "PRIVE". Ils ne doivent pas interférer avec les tâches professionnelles.
3. **Confidentialité** : Les emails contenant des informations sensibles doivent être protégés par des mesures de sécurité appropriées.

IX- Utilisation des Ressources Externes

1. **Supports Amovibles** : L'utilisation de supports amovibles est soumise à des règles strictes pour prévenir la perte ou le vol de données. Les utilisateurs doivent obtenir l'autorisation préalable du service informatique avant d'utiliser ces supports.
2. **Connexion d'Appareils Personnels** : La connexion d'appareils personnels au système d'information doit être approuvée par le service informatique et respecter les po- litiques de sécurité.

X- Formation et Sensibilisation à la Cybersécurité

ALEF Sécurité propose des formations régulières pour ses utilisateurs, telles que les programmes CYB-SAFE, qui permettent de rester informé des dernières menaces et des bonnes pratiques de cybersécurité.

1. Modules de Sensibilisation : Les formations incluent des modules sur la protection contre l'ingénierie sociale, la navigation en toute sécurité, la protection des données et la sécurité des infrastructures physiques et logicielles.
2. Formation Continue : Il est attendu des utilisateurs qu'ils participent activement aux formations et mettent en pratique les recommandations fournies. Des sessions spécifiques peuvent être organisées selon les nouvelles menaces identifiées.

XI- Engagement de l'Utilisateur

1. **Acceptation de la Charte** : Chaque utilisateur doit lire, comprendre et accepter les termes de cette Charte avant d'avoir accès aux systèmes d'information.
2. **Respect des Règles** : Les utilisateurs s'engagent à respecter les règles établies dans cette Charte et à signaler tout comportement ou incident compromettant la sécurité des systèmes d'information.

XII- Conditions de Départ

Lors du départ d'un employé ou d'un prestataire, tous les équipements et accès doivent être restitués. Les fichiers professionnels doivent être remis à l'équipe informatique et les données personnelles supprimées des systèmes de l'entreprise.

XIII- Révisions et Mise à Jour

1. **Révisions** : Cette Charte sera révisée régulièrement pour s'assurer qu'elle reste conforme aux évolutions technologiques et réglementaires. Les utilisateurs seront informés de toute modification.
2. **Mise à Jour** : Toute mise à jour de la Charte sera communiquée aux utilisateurs et prendra effet à la date indiquée dans le document.

XIV- Sanctions

1. **Manquements** : Tout manquement aux règles de la Charte peut entraîner des sanc- tions, allant de la restriction d'accès aux systèmes d'information à des mesures disci- plinaires plus sévères, selon la gravité de l'infraction.
2. **Procédure** : Les sanctions seront appliquées conformément aux procédures disciplinaires de l'entreprise, en respectant les droits des employés et les règles du droit du travail.

XV- Information et Entrée en Vigueur

1. **Communication** : La Charte sera annexée au règlement intérieur et communiquée individuellement à chaque employé.

2. **Entrée en Vigueur** : La Charte entre en vigueur le 10 octobre 2024. Tous les utilisa- teurs doivent en prendre connaissance et l'accepter pour avoir accès aux systèmes d'information de ALEF Sécurité.

XVI- Acceptation

En signant cette Charte, l'utilisateur reconnaît avoir pris connaissance des termes et s'engage à les respecter. L'utilisateur accepte que le non-respect de cette Charte puisse entraîner des sanctions conformément aux politiques de l'entreprise.

Fait à : NANTERRE le [Date] : 29/07/2025

Nom : ALAYOUD

Prénom : Jamal

Signature :

ALEF SECURITY
183 Av Georges Clemenceau - 92000 Nanterre
01 46 95 52 07 - contact@alef-security.com
SIRET : 802 678 292 00029 - AUT-092-2114-10-02-20150485789
ARTICLE L.612-14 « L'AUTORISATION D'EXERCICE NE CONFERE AUCUNE PREROGATIVE DE PUISSANCE PUBLIQUE A L'ENTREPRISE OU AUX PERSONNES QUI EN BENEFICIENT »