Politique de Gestion des Accès et Authentification

CallCenterRate

Version du 13 mai 2026

---

1. Objet

La présente Politique de Gestion des Accès et Authentification a pour objet de définir les principes de sécurité appliqués par **Confluent Digital SAS** concernant :

- l'accès à la plateforme CallCenterRate ;
- la gestion des comptes utilisateurs ;
- les mécanismes d'authentification ;
- la protection des accès ;
- la limitation des privilèges.

Cette politique vise notamment à :

- protéger les données traitées ;
- prévenir les accès non autorisés ;
- limiter les risques de compromission ;
- renforcer la sécurité globale des Services.

---

2. Comptes utilisateurs

L'accès à la plateforme nécessite la création d'un compte utilisateur.

Chaque compte :

- est personnel ;
- ne doit pas être partagé ;
- est associé à un utilisateur identifié ;
- doit être utilisé conformément aux Conditions Générales applicables.

Le Client demeure responsable :

- des accès accordés à ses utilisateurs ;
- de la gestion des habilitations ;
- des actions réalisées via ses comptes.

---

3. Authentification

L’accès aux Services peut être sécurisé notamment via :

- identifiant et mot de passe ;
- authentification multi-facteurs (MFA) lorsque disponible ;
- authentification unique (SSO) lorsque proposée ;
- mécanismes de sécurité complémentaires.

Confluent Digital SAS se réserve le droit :

- d’imposer certaines règles de sécurité ;
- de renforcer les exigences d’authentification ;
- de suspendre des accès à risque.

---

4. Gestion des mots de passe

Les utilisateurs doivent :

- choisir des mots de passe robustes ;
- préserver leur confidentialité ;
- éviter toute réutilisation non sécurisée ;
- modifier leurs identifiants en cas de suspicion de compromission.

Les mots de passe ne doivent :

- pas être partagés ;
- pas être transmis à des tiers ;
- pas être stockés de manière non sécurisée.

---

5. Gestion des habilitations

Les accès aux Services doivent être limités :

- aux seules personnes autorisées ;
- selon les besoins professionnels ;
- conformément au principe du moindre privilège.

Le Client est responsable :

- de l’attribution des droits ;
- de la suppression des accès obsolètes ;
- du contrôle des utilisateurs actifs.

---

6. Suspension et désactivation des accès

Confluent Digital SAS peut suspendre ou désactiver un accès :

- en cas d’activité suspecte ;
- de tentative d’intrusion ;
- de compromission présumée ;
- de violation des Conditions Générales ;
- de risque pour la sécurité ;
- de défaut de paiement ;
- d’usage abusif des Services.

Le Client doit immédiatement désactiver les accès des utilisateurs :

- quittant l’organisation ;
- n’ayant plus besoin des Services ;
- ou disposant de privilèges devenus inutiles.

---

7. Journalisation et surveillance

Les accès et connexions peuvent faire l’objet :

- de logs techniques ;
- de journalisation ;
- de surveillance sécurité ;
- de détection d’anomalies.

Ces informations peuvent être utilisées afin :

- de sécuriser les Services ;
- de détecter les comportements suspects ;
- d’assurer la traçabilité ;
- de respecter les obligations réglementaires.

---

8. Sécurité des sessions

Des mécanismes raisonnables peuvent être mis en œuvre afin de :

- limiter les risques de détournement de session ;
- prévenir les accès frauduleux ;
- sécuriser les connexions.

Confluent Digital SAS peut notamment :

- expirer automatiquement certaines sessions ;
- invalider des accès suspects ;
- imposer une réauthentification.

---

9. Services tiers et authentification externe

Lorsque la plateforme permet l'utilisation de services tiers d'authentification :

- SSO ;
- OAuth ;
- fournisseurs d'identité externes ;

le Client demeure responsable :

- de la sécurité de ces services ;
- de la gestion des accès associés ;
- des autorisations accordées.

Confluent Digital SAS ne saurait être tenue responsable des incidents provenant directement des fournisseurs tiers d'authentification.

---

10. Responsabilité du Client

Le Client demeure responsable :

- de la confidentialité de ses identifiants ;
- de la sécurité de ses équipements ;
- des accès accordés ;
- des actions réalisées via les comptes utilisateurs.

Toute utilisation des identifiants du Client est réputée réalisée sous sa responsabilité.

Le Client s'engage à signaler immédiatement :

- toute compromission ;
- tout accès suspect ;
- toute perte d'identifiants ;
- toute activité anormale.

---

11. Protection des données personnelles

Les traitements liés à la gestion des accès peuvent inclure :

- identifiants ;
- logs de connexion ;
- adresses IP ;
- informations de session ;
- métadonnées techniques.

Ces traitements sont réalisés conformément :

- au RGPD ;
- à la Politique de Confidentialité ;
- au DPA applicable.

---

12. Limitation de garantie

Confluent Digital SAS met en œuvre des moyens raisonnables afin de sécuriser les accès aux Services.

Toutefois :

- aucun système d'authentification ne peut garantir une sécurité absolue ;
- aucune protection ne peut empêcher tout risque de compromission.

---

13. Modification de la politique

Confluent Digital SAS peut modifier la présente politique à tout moment afin :

- de renforcer la sécurité ;

- d’adapter les Services ;
- de respecter les évolutions réglementaires ;
- d’intégrer de nouveaux mécanismes d’authentification.

---

14. Contact

Sécurité

security@confluent-digital.com

Protection des données

dpo@confluent-digital.com

Support

support@confluent-digital.com

---

15. Droit applicable

La présente politique est soumise au droit français.

Tout litige relatif à son interprétation ou son exécution relève des juridictions françaises compétentes.