Incident Response Policy

CallCenterRate

Version du 13 mai 2026

---

1. Objet

La présente Incident Response Policy a pour objet de définir les principes et procédures appliqués par **Confluent Digital SAS** en matière :

- de détection ;
- d'analyse ;
- de gestion ;
- de traitement ;
- et de notification

des incidents de sécurité susceptibles d'affecter la plateforme SaaS **CallCenterRate** ou les données traitées dans le cadre des Services.

Cette politique vise notamment à :

- limiter les impacts des incidents ;
- protéger les données ;
- assurer la continuité des Services ;
- respecter les obligations réglementaires applicables.

---

2. Définition d'un incident

Un incident désigne tout événement susceptible :

- d'affecter la confidentialité ;
- l'intégrité ;
- la disponibilité ;
- ou la sécurité

des systèmes, Services ou données traités par CallCenterRate.

Les incidents peuvent notamment inclure :

- accès non autorisé ;

- compromission de compte ;
- tentative d’intrusion ;
- fuite de données ;
- malware ;
- indisponibilité de service ;
- altération de données ;
- attaque informatique ;
- erreur humaine ;
- défaillance technique.

---

3. Principes généraux

Confluent Digital SAS applique une approche raisonnable visant à :

- détecter rapidement les incidents ;
- limiter leur propagation ;
- réduire leur impact ;
- restaurer les Services ;
- améliorer continuellement les mesures de sécurité.

---

4. Détection des incidents

Les incidents peuvent être détectés notamment via :

- outils de monitoring ;
- systèmes d’alerting ;
- logs techniques ;
- détection d’anomalies ;
- signalements utilisateurs ;
- contrôles internes ;
- notifications de prestataires tiers.

---

5. Classification des incidents

Les incidents peuvent être classés selon leur niveau de criticité.

Incident critique

Incident susceptible d'entraîner :

- indisponibilité majeure ;
- fuite importante de données ;
- compromission critique ;
- impact significatif sur les Clients.

Incident majeur

Incident affectant significativement :

- certaines fonctionnalités ;
- la sécurité ;
- ou un nombre limité de Clients.

Incident mineur

Incident à impact limité :

- anomalie isolée ;
- dysfonctionnement mineur ;
- tentative bloquée sans impact significatif.

---

6. Gestion des incidents

Lorsqu'un incident est identifié, Confluent Digital SAS peut notamment :

- analyser la situation ;
- isoler les systèmes concernés ;
- limiter les accès ;
- suspendre certains services ;
- appliquer des correctifs ;
- restaurer les données ou services concernés ;
- renforcer les mesures de sécurité.

---

7. Notification des violations de données

En cas de violation de données personnelles susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, Confluent Digital SAS notifiera le Client dans les meilleurs délais après en avoir pris connaissance.

La notification pourra notamment inclure :

- la nature de l'incident ;
- les catégories de données concernées ;
- les impacts potentiels identifiés ;
- les mesures correctives mises en œuvre ;
- les recommandations éventuelles.

Confluent Digital SAS notifiera également les autorités compétentes lorsque cela est requis par la réglementation applicable.

---

8. Responsabilité du Client

Le Client demeure responsable :

- de la sécurité de ses accès ;
- de la confidentialité de ses identifiants ;
- de la sécurité de ses équipements ;
- des actions réalisées via ses comptes ;
- des données importées dans la plateforme.

Le Client s'engage à signaler sans délai :

- tout accès suspect ;
- toute compromission ;
- toute activité anormale ;
- toute suspicion de violation de sécurité.

---

9. Services tiers

Certains incidents peuvent provenir :

- de services tiers ;

- d’APIs externes ;
- de fournisseurs cloud ;
- de prestataires techniques.

Confluent Digital SAS ne peut garantir l’absence totale d’incidents affectant des services tiers.

---

10. Conservation des preuves et logs

Des logs techniques et éléments de traçabilité peuvent être conservés afin :

- d’analyser les incidents ;
- de sécuriser les infrastructures ;
- de prévenir les usages frauduleux ;
- de répondre aux obligations légales.

---

11. Amélioration continue

À la suite d’un incident significatif, Confluent Digital SAS peut :

- réaliser une analyse interne ;
- identifier les causes ;
- mettre en œuvre des mesures correctives ;
- renforcer les procédures de sécurité ;
- adapter ses contrôles techniques et organisationnels.

---

12. Confidentialité

Les informations relatives aux incidents de sécurité sont traitées de manière confidentielle et communiquées uniquement :

- aux personnes habilitées ;
- aux Clients concernés ;
- aux autorités compétentes lorsque cela est nécessaire.

---

13. Limitation de garantie

Confluent Digital SAS met en œuvre des moyens raisonnables afin de prévenir et gérer les incidents de sécurité.

Toutefois :

- aucun système informatique ne peut garantir une sécurité absolue ;
- aucune garantie d'absence totale d'incident ne peut être fournie.

---

14. Contact sécurité

Toute suspicion d'incident ou de vulnérabilité peut être signalée à :

security@confluent-digital.com

Les demandes relatives à la protection des données peuvent être adressées à :

dpo@confluent-digital.com

---

15. Modification de la politique

Confluent Digital SAS peut modifier la présente Incident Response Policy afin :

- de renforcer la sécurité ;
- d'adapter ses procédures ;
- de respecter les évolutions réglementaires ;
- de faire évoluer les Services.

---

16. Droit applicable

La présente politique est soumise au droit français.

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