

Politique de sécurité de l'information

Version
01/07/2026

Émetteur
Pierre de Cintré, associé

Périmètre
Ensemble des collaborateurs et des missions

Objet et périmètre

La présente politique décrit les mesures techniques et organisationnelles appliquées par DEAPDATA à ses postes de travail, à son infrastructure et à ses missions. Nos interventions se déroulent au sein de systèmes d'information critiques : ces mesures sont la contrepartie de cet accès.

Gouvernance

La sécurité de l'information relève de Pierre de Cintré, associé, qui est également l'interlocuteur des services achats et sécurité de nos clients, à contact@deapdata.com.

Postes de travail et accès

DEAPDATA fournit un poste de travail à ses fonctions internes, ainsi qu'aux consultants lorsque le client n'en met pas à disposition. En mission, les consultants travaillent le plus souvent sur l'environnement fourni par le client.

- Verrouillage automatique de session et politique de mots de passe.
- Application régulière des mises à jour de sécurité.
- Procédure de départ : révocation immédiate des accès et restitution du matériel.

Sauvegardes

- **Périmètre** — postes de travail et serveur d'infrastructure.
- **Fréquence** — mensuelle.
- **Rétention** — 30 jours.
- **Localisation** — chez OVH, en France. Une copie de secours est conservée chez Dropbox, dont les serveurs sont situés aux États-Unis.
- **Test de restauration** — une fois par an.

Gestion des incidents

- Tout incident — poste compromis, message frauduleux ouvert, perte de matériel — est signalé sans délai à Pierre de Cintré, à contact@deapdata.com.
- Les incidents sont consignés dans un registre interne.
- Le client concerné est informé sans délai, et au plus tard sous 48 heures.
- En cas de violation de données personnelles, la notification au responsable de traitement intervient dans les meilleurs délais, dans le respect du délai prévu au contrat.

Continuité d'activité

En cas d'indisponibilité de notre hébergeur, la copie de sauvegarde de secours permet de reprendre l'activité. Le retour à un fonctionnement normal est visé sous 48 heures.

Interventions chez le client

Nos consultants interviennent le plus souvent dans l'environnement de travail fourni par le client. Les règles de sécurité du client s'appliquent alors intégralement et priment sur les nôtres. Nos consultants n'agissent que sur

instruction du responsable de traitement, et recourent systématiquement aux données pseudonymisées ou anonymisées dans les phases de développement et de recette.

Sensibilisation

Les collaborateurs sont sensibilisés régulièrement à la sécurité et à l'hameçonnage. Un engagement de confidentialité est signé par chaque collaborateur à son entrée, complété des engagements spécifiques exigés par chaque client.

Sous-traitants techniques

 OVH SAS, 2 rue Kellermann, 59100 Roubaix — hébergement de l'infrastructure technique et de la messagerie professionnelle.

 Dropbox — copie de sauvegarde de secours, hébergée aux États-Unis. Ce transfert est encadré par les garanties prévues à l'accord de traitement des données de Dropbox.

Fin de mission

Restitution des accès, suppression des copies locales, attestation de destruction sur demande.

Suivi et révision

Cette politique est portée par la direction et revue chaque année.

DEAPDATA — société à responsabilité limitée au capital de 2 000 € — RCS de Rouen 823 765 615.
Siège social : 25 rue Domrémy, 76000 Rouen — Bureaux : Paris 16^e et La Défense — deapdata.com