Positive

Mesures Techniques et Organisationnelles

Avril 2026

Introduction

Ce document décrit les dispositions que Positive Group Sales Solutions met en œuvre pour répondre aux exigences de sécurité ainsi qu'aux enjeux de cyber sécurité. Il définit en particulier les mesures techniques, organisationnelles et procédurales qui sont mises en œuvre pour maintenir la sécurité et la protection des données, y compris des données personnelles conformément à l'article 32 du RGPD.

Le Client doit s'assurer que les mesures de sécurité mises en place sont pertinentes par rapport aux risques associés à son utilisation des Services.

Evolution des mesures

Les mesures techniques et organisationnelles peuvent évoluer à tout moment. Toutefois, ces modifications n'auront pas pour objet de dégrader le niveau de protection des Données personnelles.

1. Contrôle d'accès physique aux locaux et aux installations

Mesures appropriées pour contrôler et empêcher l'accès physique des personnes non autorisées aux locaux et installations.

- Système d'alarme
- Personnel de sécurité, concierges
- Installations de vidéo surveillance
- Système automatique de contrôle d'accès / Distinction de zones selon les risques
- Lecteur d'identification par biométrie ou par badges, cartes à puce, cartes magnétiques, avec journalisation et système de verrouillage à transpondeur
- Serrures de sécurité
- Vérification d'identité
- Enregistrement / Accompagnement des visiteurs

En fonction de l'emplacement et de l'installation, une combinaison de la liste ci-dessus est présente. Il est nécessaire de prendre en compte que toutes les fonctionnalités ne sont pas présentes et nécessaires sur tous les locaux ou installations.

2. Contrôle d'accès aux données, aux systèmes

Mesures appropriées pour limiter les accès aux systèmes et aux données

- Attribution des droits des utilisateurs répondant au principe de moindre privilège, avec révision ou suppression en cas de changements d'affectation ou de départ.
- Création de profils utilisateur :
  - Droits d'accès différenciés (profils, rôles, transactions et objets)
  - Administration des droits par les administrateurs système
- Procédures de mot de passe (y compris les caractères spéciaux, la longueur minimale, le changement de mot de passe etc.)
- Authentification avec nom d'utilisateur / mot de passe
- Authentification à plusieurs facteurs obligatoire
- Verrouillage automatique des sessions en cas de non utilisation
- Verrouillage automatique de compte utilisateur après plusieurs tentatives d'accès erronées
- Administration des postes de travail localement
- Accès d'administration des serveurs via SSM
- Utilisation de gestionnaires de mots de passe sécurisés
- Chiffrement des disques d'ordinateurs nomades

- Chiffrement des échanges
- Utilisation de clé de sécurité physique pour l'accès aux interfaces d'administration
- Utilisation d'un logiciel anti-virus / firewalls / limitation des services et flux non nécessaires
- Mises à jour en continu des systèmes d'exploitation et applications
- Cloisonnement des réseaux / réseau d'administration
- Actes d'administration tracés et centralisés avec temps uniformisé
- Centralisation des traces applicatives sur les données (accès, entrées, modifications, suppressions)

Selon le rôle, le type de logiciel, le niveau de risque, des exigences clients spécifiques et la nécessité, une combinaison des mesures est en place.

3. Contrôle de disponibilité

Mesures prévoyant la disponibilité et la protection des données contre la destruction ou la perte accidentelle.

- Procédures de sauvegarde ; Stockage de sauvegarde
- Stockage des sauvegardes à 2 localisations différentes
- Disaster recovery plan (DRP), données dupliquées sur site secondaire
- Systèmes anti-virus / pare-feu
- Systèmes d'alarme incendie et fumée
- Détection automatique des incendies
- Extinction automatique à gaz
- Détection des intrusions
- Présence d'extincteurs portatifs et mobiles
- Alimentation électrique de secours en cas de défaillance
- Lien Internet de secours en cas de défaillance
- Climatisation de secours en cas de défaillance
- Plan de maintenance préventive et tests basés sur les préconisations des constructeurs

En fonction de l'emplacement et de l'installation, une combinaison de la liste ci-dessus est présente. Il est nécessaire de prendre en compte que toutes les fonctionnalités ne sont pas présentes et nécessaires sur tous les locaux ou installations.

4. Contrôle de ségrégation

Mesures pour prévoir un traitement distinct (stockage, modification, suppression, transmission) de données à des fins différentes. Utilisation de jeux de données factices hors systèmes de production.

- Séparation du système de test et de production
- Séparation du système de développement et de production
- Séparation logique des données clients

5. Mesures internes générales

- Désignation d'un Data Protection Officer (DPO)
- Évaluation périodique des mesures en place
- Plateforme d'échange de fichiers sécurisée
- Procédure de notification de violation de données à caractère personnel impactant les données de nos clients
- Procédure de respect des droits des personnes concernées en matière de protection des données personnelles
- Accords de confidentialité et de protection des données personnelles conclus avec le personnel
- Actions de sensibilisation auprès du personnel dès l'intégration et en continu sur les aspects de protection et sécurité des données : Communication (réseau social interne, ateliers...), séances de formation
- Sensibilisations des développeurs aux bonnes pratiques, revues de code, pair programming

- Contrats de sous-traitance ultérieure intégrant des clauses de protection des données personnelles

6. Sécurité des infrastructures et autres mesures

Mesures au regard de la sécurité continue des systèmes.

- Évaluation périodique de la sécurité des application (2 audits par an)
- Limitation d'attaques par bourrage d'identifiants (bruteforce) et rate limiting
- Durcissement des systèmes
- Plan de mise à jour des systèmes de production
- Surveillance continue des vulnérabilités (CERT) et déploiement de correctifs selon criticité
- Processus sécurisé de mise au rebut des matériels
- Procédure de remontée et de traitement d'incidents