PLAN DE SECURITE ET DE CONFORMITE

1. Objectif

L'objectif de ce plan est d'assurer la protection, la traçabilité et la conformité des données circulant dans l'ensemble du pipeline (OLTP, OLAP et NoSQL).
Il vise à :

- Sécuriser les échanges et le stockage des données sensibles.
- Prévenir les fuites, fraudes et accès non autorisés.
- Garantir la conformité avec les réglementations RGPD, PCI-DSS et CCPA.
- Mettre en place un cadre d'audit, de reporting et de gouvernance automatisé.

2. Cadre général de sécurité

2.1 Chiffrement des données

- **En transit :**
  Toutes les communications entre les composants du système (API, pipelines, bases de données) sont sécurisées à l'aide du protocole TLS (version 1.2 ou supérieure).
- **Au repos :**

  Les données stockées dans les bases OLTP, OLAP et NoSQL sont chiffrées à l'aide d'un algorithme de chiffrement standard (AES-256).
  La gestion des clés de chiffrement est centralisée via un service de gestion des clés (KMS).
  Les sauvegardes automatiques sont également chiffrées.

2.2 Contrôle d'accès et authentification

- Mise en place d'un **contrôle d'accès basé sur les rôles (RBAC)** pour limiter les permissions des utilisateurs:
  - *Admin* : gestion des accès et politiques.
  - *Data Engineer* : maintenance et supervision des pipelines.
  - *Data Analyst* : lecture seule sur OLAP.
  - *Data Scientist* : accès restreint aux collections NoSQL.

L'authentification multi-facteurs (MFA) est activée pour les comptes sensibles.
Les accès et connexions sont journalisés afin de garantir la traçabilité.

2.3 Sécurité des API

Les APIs constituent la porte d'entrée principale des données transactionnelles et analytiques.
Elles sont sécurisées sur plusieurs couches :

Authentification et autorisation

- Utilisation du protocole OAuth 2.0 avec JWT (JSON Web Tokens).
- Clés API uniques par client et associées à un rôle.
- Tokens à durée de vie limitée et chiffrés.

Protection réseau

- **API Gateway** pour authentification, filtrage et monitoring.
- **WAF (Web Application Firewall)** pour bloquer :
    - injections SQL / NoSQL,
    - XSS,
    - requêtes suspectes ou malformées.
- **Rate limiting** pour limiter le nombre de requêtes et prévenir les attaques DoS.

Sécurité des communications

- Tous les échanges API ↔ services internes **utilisent HTTPS + TLS 1.2 minimum**.
- Les données sensibles sont chiffrées dès la requête (PAN, ID client, token).

Journalisation et audit

- Journalisation complète des appels API : identifiant client, endpoint, timestamp, statut HTTP.
- Conservation 90 jours minimum (CloudWatch / ELK).
- Alertes automatiques sur anomalies (erreurs >5 %, token invalide, volume inhabituel).

2.4 Formation et sensibilisation des équipes

La sécurité dépend autant des **compétences humaines** que des technologies.
Un plan de **formation continue** est mis en place pour développer la culture sécurité et conformité.

Programme de formation

- **Onboarding sécurité** obligatoire pour les nouveaux collaborateurs.
- **Ateliers trimestriels** : gestion des accès, chiffrement, manipulation des données sensibles.
- **Formation annuelle certifiante** : sécurité cloud, DevSecOps, conformité RGPD.
- **Simulations d'incidents** ("table-top exercises") pour tester la réactivité en cas de faille.

Suivi et indicateurs

- Suivi des formations dans un LMS interne.
- KPI mesurés : taux de participation, incidents évités, conformité post-formation.

3. Conformité réglementaire

3.1 RGPD

- **Minimisation des données collectées.**
- **Anonymisation / pseudonymisation** dans OLAP et NoSQL.
- **Droit à l'oubli** : suppression automatisée sur demande.
- **Audit de traitement** : chaque transformation est historisée.
- **Hébergement UE-only** pour les données européennes.

3.2 PCI-DSS

- **Chiffrement fort (AES-256)** et **tokenisation** des données de carte.
- Aucune donnée complète de carte stockée dans OLAP.
- **Audit trimestriel** de conformité sur les flux de paiement.
- **Segmentation réseau** stricte entre environnements (prod / dev / test).

3.3 CCPA

- **Consentement explicite** à la collecte des données.
- **Droit de portabilité et de suppression** via export JSON/CSV.

4 Reporting et audit automatisé

Des rapports de conformité sont générés automatiquement à partir des journaux :

- rapports d'accès,
- rapports d'erreurs,
- rapports de sécurité.

Des audits réguliers sont réalisés afin de vérifier :

- les accès utilisateurs,
- les politiques de sécurité,
- le respect des réglementations.

5 Plan de résilience et reprise après incident

- **Sauvegardes automatiques quotidiennes** (OLTP, OLAP, NoSQL).
- **Réplication** sur AWS pour tolérance aux pannes.
- **Procédures documentées** de restauration testées mensuellement.
- **Kafka et Spark redondants** pour garantir la continuité du streaming.

6 lncident Response Plan (IRP)

Un plan de réponse aux incidents (IRP) est mis en place pour assurer une réaction rapide et coordonnée en cas d'incident de sécurité (intrusion, fuite de données, panne critique, dérive modèle ML…).
Il définit les rôles, les procédures et les outils nécessaires pour :

- **Détecter** et **analyser** rapidement les anomalies (via les logs, alertes ou monitoring).
- **Contenir et corriger** les incidents afin de limiter leur impact sur les systèmes OLTP, OLAP et NoSQL.
- **Restaurer** les services grâce aux sauvegardes automatisées et à la réplication multi-AZ.
- **Documenter et notifier** les incidents conformément aux exigences réglementaires (RGPD, PCI-DSS).

Ce plan est testé régulièrement (simulations internes) et mis à jour après chaque incident afin d'améliorer en continu la posture de sécurité et la résilience du pipeline.