Politique de Sécurité Mobile — Audi

Auteur : Responsable Sécurité
Date : Septembre 2025

1. Objectif

Cette politique définit les règles de sécurité applicables au développement, au déploiement et à l'utilisation des applications mobiles au sein de la société **Audi**.
L'entreprise, constructeur automobile de référence, compte **5000 salariés** et dispose d'une flotte interne de **500 smartphones professionnels** utilisés par ses équipes commerciales, techniques et administratives.

L'objectif est de :

Protéger les données critiques (véhicules, clients et partenaires)

Réduire les risques de compromission,

Encadrer la gestion sécurisée de la flotte mobile,

Garantir la conformité réglementaire (RGPD, ISO 27001, normes industrielles).

2. Portée

Cette politique s'applique :

Aux applications mobiles développées par ou pour Audi (apps clients, apps internes pour la gestion de flotte, apps support technique ou bien même script/projet créer par leurs SI).

Aux collaborateurs utilisant les **500 smartphones professionnels fournis par l'entreprise**.

Aux salariés accédant aux systèmes internes depuis un terminal personnel (BYOD), sous réserve de validation et de conformité MDM.

3. Principes Directeurs

Sécurité du développement

Intégrer la sécurité dès la conception des applications mobiles utilisées pour les véhicules connectés et services clients.

Interdire le stockage de **secrets en clair** (API keys, tokens liés aux véhicules ou aux systèmes internes).

Forcer l'usage de **protocoles chiffrés (HTTPS/TLS 1.2+)** pour la communication avec les serveurs Audi.

Interdire le déploiement en production de versions contenant du code de debug ou des logs sensibles.

Protection des données

Chiffrement obligatoire des données liées aux véhicules, aux clients et aux partenaires (AES-256 recommandé).

Utilisation de **Keystore Android / Keychain iOS** pour stocker les secrets.

Authentification forte (MFA) pour l'accès aux données sensibles (ex. : données clients, télédiagnostic véhicules).

Gestion de la flotte mobile (500 smartphones)

Tous les terminaux Audi doivent être inscrits dans une solution **Mobile Device Management (MDM)**.

Blocage automatique des terminaux compromis (root/jailbreak).

Obligation de mise à jour régulière des OS et applications.

Limitation stricte de l'installation d'applications tierces non validées par Audi.

Publication & distribution

Les APK/IPA internes doivent être **signés et distribués via le MDM** ou les stores officiels validés par Audi.

Les builds doivent passer par un **pipeline CI/CD sécurisé**, avec validation sécurité avant mise en production.

4. Contrôles & conformité

Revue de code sécurité obligatoire pour toute app mobile Audi.

Tests de sécurité (SAST, DAST, pentests) réalisés sur les apps liées aux services clients et aux véhicules connectés.

Audit annuel des **500 smartphones professionnels** et des applications déployées.

Conformité avec RGPD et normes industrielles de l'automobile.

5. Prévention

Mise en place de formation informatique sur l'utilisation des smartphone

Sensibilisation sur les risques informatiques et les méthode utilisé pour attaqué informatiquement une entreprise

6. Sanctions

Tout manquement à cette politique pourra entraîner :

La désactivation du smartphone professionnel concerné,

La suspension temporaire des accès aux services Audi,

7. Recommandations complémentaires

Formation des 5000 salariés d'Audi sur les risques mobiles et bonnes pratiques.

Mise en place d'un **bug bounty interne** ciblant les applications mobiles clients et internes.

Élaboration d'un **plan de réponse à incident mobile** incluant procédures de retrait rapide des applications compromises.

8 . Conclusion

Avec une flotte de **500 smartphones** et une base de **5000 salariés**, Audi doit garantir un haut niveau de sécurité mobile.

Le respect de cette politique est essentiel pour protéger les données clients, préserver l'image de marque et soutenir la stratégie digitale du constructeur automobile.