PLAN DIRECTEUR DE LA FLOTTE MOBILE

Gouvernance, Préparation, Enrôlement et Sécurisation

Référence : IT-MOB-2026-001 | **Classification :** Confidentiel

Sommaire

1. Cadre de Gouvernance et Stratégie

Ce document définit les standards pour l'ensemble des terminaux mobiles (smartphones et tablettes) accédant aux ressources du Système d'Information (SI).

1.1 Objectifs Stratégiques

- **Mobilité sécurisée :** Permettre le travail nomade sans compromettre l'intégrité des données.
- **Standardisation :** Réduire les coûts de maintenance en limitant le nombre de modèles supportés.
- **Automatisation :** Minimiser l'intervention humaine lors du déploiement (Zero-Touch).

1.2 Modèles de Détention (Ownership)

Nous distinguons trois modes de gestion pour répondre aux besoins métiers :

Modèle	Propriété	Niveau de Contrôle	Usage
COBO	Entreprise	Total (Bridage complet)	Logistique, Entrepôts, Bornes.
COPE	Entreprise	Conteneurisé (Espace Pro/Perso)	Cadres, Commerciaux, Administratifs.
BYOD	Employé	Applicatif uniquement (MAM)	Collaborateurs ponctuels, Prestataires.

2. Spécifications Matérielles et Logicielles

2.1 Catalogue de Matériel Homologué

Seuls les appareils suivants sont autorisés à l'enrôlement automatique pour garantir la compatibilité avec les agents MDM :

- **Apple :** iPhone 13 et supérieurs, iPad Air/Pro (Génération 5+).
- **Android :** Gamme Samsung Enterprise Edition (S22+, A54), Google Pixel 7+.

2.2 Pré-requis Logiciels

Le système d'exploitation (OS) doit toujours être maintenu à la version *n-1* par rapport à la dernière sortie majeure.

3. Architecture d'Enrôlement (Zero-Touch)

L'enrôlement est le processus par lequel un appareil est déclaré dans la solution de gestion **Unified Endpoint Management (UEM)**.

3.1 Apple Business Manager (ABM)

Tous les appareils iOS sont achetés via un revendeur agréé qui injecte les numéros de série directement dans notre portail ABM. Lors du premier allumage (ou après un reset), l'appareil contacte les serveurs Apple et se voit imposer le profil MDM de l'entreprise.

3.2 Android Enterprise Zero-Touch

Similaire à ABM, ce programme permet un déploiement massif sans configuration manuelle. Le mode "Device Owner" est activé par défaut, offrant à l'IT les droits administrateurs complets sur le terminal.

4. Configuration Master et Profils MDM

Une fois enrôlé, l'appareil reçoit une série de "Payloads" (charges utiles) de configuration.

4.1 Profils Réseau et Connectivité

- **Wi-Fi Corporate :** Déploiement automatique du SSID via certificat WPA3-Enterprise.
- **VPN Always-On :** Tunnel sécurisé activé automatiquement pour les applications internes (Intranet, ERP).

4.2 Restrictions de Sécurité (Sandboxing)

```
- Désactivation de l'appareil photo (si requis par le site).
- Interdiction du copier-coller entre le conteneur Pro et Perso.
- Blocage de l'installation d'applications via des fichiers .APK ou .IPA tiers.
```

5. Déploiement des Applications et VPP

5.1 Gestion des Licences (VPP)

Le **Volume Purchase Program** permet d'acheter des licences d'applications en masse et de les distribuer sans que l'utilisateur ait besoin de créer un compte Apple ID ou Google personnel.

5.2 Catalogue d'Applications Métiers

Les applications sont classées en trois catégories :

1. **Obligatoires :** Installées automatiquement (Outlook, Teams, Onedrive, MTD).
2. **À la demande :** Disponibles dans le "Self-Service Portal" de l'entreprise.
3. **Critiques :** Applications de production (ex: Gestion de stock) avec accès conditionnel.

6. Sécurité Mobile (MTD) et Conformité

La mobilité est le premier vecteur d'attaque. Nous intégrons une solution **Mobile Threat Defense (MTD)**.

6.1 Analyse des Menaces

L'agent de sécurité analyse en temps réel :

- **Niveau Réseau :** Détection des attaques de type "Man-in-the-Middle" sur les Wi-Fi publics.
- **Niveau App :** Scan des applications pour détecter des comportements de type "Spyware".
- **Niveau Système :** Vérification de l'intégrité du Kernel (détection de Root/Jailbreak).

6.2 Actions Correctives Automatisées

> **ALERTE CONFORMITÉ :** Si un terminal est détecté comme compromis, l'accès au serveur de messagerie est révoqué en moins de 30 secondes (Accès Conditionnel Azure AD/Intune).

7. Gestion du Cycle de Vie et Support

7.1 Processus de Remplacement (Swap)

En cas de casse, un processus de "Swap standard" est mis en place :

1. Déclaration du sinistre via le portail Self-Service.
2. Envoi d'un appareil de remplacement pré-enrôlé sous 24h.
3. L'utilisateur se connecte, ses applications et données cloud se synchronisent automatiquement.

7.2 Mise au rebut sécurisée

L'effacement des données (Remote Wipe) doit être certifié. Pour les appareils en fin de vie, un certificat d'effacement conforme au RGPD est généré par la console MDM avant recyclage physique.

8. Glossaire et Annexes

- **MDM (Mobile Device Management) :** Gestion des terminaux.
- **MAM (Mobile Application Management) :** Gestion des applications.
- **IMEI :** Numéro d'identité unique du matériel mobile.
- **UEM :** Unified Endpoint Management (plateforme centrale).
