**Політика використання мобільних пристроїв у «FinSecure Inc» - з урахуванням MDM, MAM, BYOD та корпоративних Linux платформ, на базі Microsoft Intune.**

1. **Визначення пристроїв**

|  |  |  |
| --- | --- | --- |
| **Тип пристрою** | **Приклад** | **Статус у політиці** |
| Корпоративні ноутбуки | Windows 10-11 Pro, macOS, Linux | Повністю контрольовані через MDM |
| Корпоративні мобільні телефони | Android Enterprise, iPhone з MDM | Повністю контрольовані через MDM |
| Корпоративні планшети | iPad, Surface | Контрольовані через MDM |
| Особисті пристрої (BYOD) | Android/iOS смартфони, ноутбуки | Частково контрольовані через MAM |

*Правила для кожної категорії:*

Корпоративні пристрої:

* Повна реєстрація в Intune або альтернативній системі (для Linux)
* Примусове застосування політик безпеки
* Дозволено встановлення лише корпоративно затверджених застосунків
* Обов’язкове шифрування, MFA, VPN

**Особисті пристрої (BYOD):**

* Реєстрація через **App Protection Policies (MAM)**
* Дані контейнеризовані
* Встановлення ***Microsoft Company Portal* - *обов’язково***
* Доступ лише до обмеженого набору корпоративних ресурсів

1. **Вимоги до безпеки пристроїв (MDM)**

*Основні вимоги:*

Шифрування:

* Усі пристрої повинні мати активоване шифрування (*BitLocker / FileVault / Android encryption*)

VPN:

* Доступ до внутрішніх ресурсів лише через корпоративний VPN

Двофакторна автентифікація (MFA):

* Обов’язкова для всіх користувачів через Microsoft Authenticator

Паролі та блокування:

* Мінімальна довжина пароля - десять символів, включаючи що найменше одну велику літеру, одну цифру та один спеціальний символ
* Автоматичне блокування після 5 хвилин бездіяльності (або за часом визначеним відділом CS, в залежності від ролей)

Процедури втрати/крадіжки:

* Віддалене стирання (Remote Wipe) через Intune або скрипт Linux
* Автоматичне блокування при порушенні політики відповідності
* Сповіщення адміністратору через Intune Alerts
* Видалення корпоративного профілю (контейнеру) без впливу на особисті дані (для BYOD)

1. **Керування застосунками (МАМ)**

*Дозволені корпоративні застосунки*

|  |  |
| --- | --- |
| **Категорія** | **Застосунки** |
| Комунікація | Outlook, Teams, OneDrive |
| Документи | Word, Excel, PowerPoint, SharePoint |
| Безпека | Microsoft Defender, Authenticator |
| Linux | Thunderbird, LibreOffice, VS Code, Docker |

*Заборонені корпоративні застосунки*

* Соціальні мережі: TikTok, Telegram, Facebook (та інші застосунки на корпоративних пристроях визначених політикою організації, корпоративними правилами, та правилами визначеними відділом CS)
* Неконтрольовані месенджери: Viber, WhatsApp (на BYOD - дозволено лише з обмеженням копіювання, може включати інші месенджери та обмеження визначені відділом CS)
* Невідомі VPN або проксі-сервіси

**\*\*Всі дозволи, заборони та обмеження щодо застосунків повинні бути узгодження з відділом корпоративної безпеки (CS) відповідно до внутрішніх регламентів**

*Протоколи оновлення*

* Усі застосунки повинні оновлюватись автоматично через Microsoft Store, apt/yum (Linux)або корпоративний портал
* Заборонено відкладати оновлення більше ніж на 5 днів
* Застосунки без цифрового підпису не допускаються до встановлення, за винятком випадків, коли їх використання погодження з відділом СS та супроводжується окремим аудитом безпеки

1. **Політика BYOD**

*Вимоги до особистих пристроїв*

* Операційна система: Android 10+, iOS 14+, Windows 10 Pro+ (Інші операційні системи можуть бути дозволені до встановлення за умови попереднього погодження з відділом CS та проходження повної процедури перевірки відповідності політикам компанії)
* Встановлення ***Microsoft Company Portal*** - ***обов’язкове***
* Реєстрація через ***App Protection Policies***, без повного MDM-контролю

*Вимоги до особистих пристроїв відповідно до платформи:*

* *Android/iOS* - Android 10+, iOS 14+, Company Portal, контейнеризація, MFA
* *Windows/macOS* - Windows 10 Pro+, FileVault/BitLocker, VPN, Company Portal
* *Linux* - Ubuntu / Fedora / Debian, обов’язкове шифрування (LUKS), VPN - з’єднання, активований SELinux або AppArmor, контрольований доступ через локальні ACL або централізовану систему обліку

*Критерії дозволу*

|  |  |  |
| --- | --- | --- |
| **Тип пристрою** | **Дозволено / Заборонено / Дозволено з обмеженнями** | **Умови використання** |
| Особистий смартфон | Дозволено | Контейнерізація, MFA, Company Portal |
| Особистий ноутбук | Дозволено з обмеженнями | Windows 10 Pro, VPN, шифрування (обмеження та дозволи додатково погоджує відділ CS) |
| Rooted/Jailbroken | Заборонено | Заборонено |

*Захист корпоративних даних*

* Контейнеризація (Мobile Аpplication Мanagement - MAM)
* Заборона копіювання/вставки між корпоративними та особистими застосунками
* Віддалене стирання корпоративного контейнера при порушенні політики
* Вимога MFA для доступу до корпоративних ресурсів

1. **Додатковий пункт для Linux пристроїв:**

*Правила для Linux-пристроїв:*

* **Реєстрація в системі обліку пристроїв** (через Intune або альтернативно - JAMF, Canonical Landscape, Puppet)
* **Примусове застосування політик безпеки** через скрипти, конфігураційні менеджери або вручну
* Встановлення лише корпоративно затверджених застосунків
* **Моніторинг відповідності** через SIEM або локальні журнали

*Вимоги до безпеки Linux пристроїв*

Шифрування:

* Обов’язкове використання LUKS (Linux Unified Key Setup) для шифрування диску

VPN:

* Використання OpenVPN або WireGuard з корпоративними сертифікатами

Аутентифікація:

* MFA через Microsoft Authenticator або PAM-модулі (наприклад, pam\_oath, pam\_google\_authenticator)

Паролі та блокування:

* Мінімальна довжина пароля десять символів, включаючи що найменше одну велику літеру, одну цифру та один спеціальний символ
* Автоматичне блокування екрану через gnome-screensaver або xlock

Контроль доступу:

* SELinux або AppArmor - активовані
* iptables або nftables - налаштовані для обмеження зовнішнього трафіку

Антивірус:

* На Linux-пристроях має бути встановлено антивірусне рішення, узгоджене з політикою компанії - ClamAV (для базового захисту) або ESET Endpoint Security (для розширеного контролю)

**Словник**

*ClamAV* - відкритий антивірусний двигун для Linux, призначений для виявлення шкідливого ПЗ, зокрема троянів, вірусів і фішингових файлів.

*ESET Endpoint Security* - комерційне антивірусне рішення з розширеними функціями захисту кінцевих точок, включаючи фаервол, веб-захист і контроль пристроїв.

*Iptables* - утиліта для налаштування фільтрації мережевого трафіку в Linux, що дозволяє створювати правила доступу на основі IP, портів і протоколів.

*nftables* - сучасна заміна iptables, яка забезпечує більш гнучке керування мережевими фільтрами та має спрощений синтаксис.

*SELinux* - система контролю доступу в Linux, що реалізує політики безпеки на основі контекстів, обмежуючи дії процесів і користувачів.

*AppArmor* - альтернатива SELinux, яка дозволяє обмежити доступ застосунків до системних ресурсів через профілі безпеки.

*gnome-screensaver* - компонент середовища GNOME, що автоматично блокує екран після періоду бездіяльності, забезпечуючи фізичний захист пристрою.

*xlock* - утиліта для блокування X-сесії в Unix-подібних системах, яка запобігає несанкціонованому доступу до робочого середовища.

*PAM-модулі* - компоненти Pluggable Authentication Modules, які дозволяють гнучко налаштовувати автентифікацію в Linux-системах.

*pam\_oath* - PAM-модуль, що реалізує одноразові паролі (OTP) на основі алгоритмів HOTP/TOTP для двофакторної автентифікації.

*pam\_google\_authenticator* - модуль PAM, який інтегрує Google Authenticator для генерації одноразових кодів MFA на локальному пристрої.

*OpenVPN* - протокол VPN з відкритим кодом, який забезпечує захищене з’єднання між пристроєм і корпоративною мережею через TLS/SSL.

*WireGuard* - сучасний VPN-протокол, що відзначається високою продуктивністю, простотою конфігурації та використанням сучасної криптографії.

*LUKS (Linux Unified Key Setup)* - стандарт для шифрування дисків у Linux, який забезпечує захист даних на рівні блоку з підтримкою кількох ключів.

*JAMF* - платформа для MDM-керування пристроями Apple, що дозволяє централізовано налаштовувати, оновлювати та захищати macOS/iOS.

*Canonical Landscape* - рішення для централізованого керування Ubuntu-системами, включаючи оновлення, моніторинг і аудит безпеки.

*Puppet* - система автоматизації конфігурацій, яка дозволяє керувати налаштуваннями серверів і робочих станцій через декларативні маніфести.

*Мobile Аpplication Мanagement (MAM)* - підхід до захисту корпоративних даних на мобільних пристроях через контроль застосунків без повного управління пристроєм.

***ACL (Access Control List)*** - механізм управління доступом, який дозволяє задавати права для окремих користувачів або груп на файли та каталоги.

*Microsoft Intune* - хмарна платформа MDM/MAM від Microsoft, яка дозволяє керувати пристроями, застосунками та політиками безпеки в корпоративному середовищі.

***Відділ CS (Cyber Security)*** - внутрішній підрозділ компанії, відповідальний за забезпечення кібербезпеки, включаючи розробку політик захисту, моніторинг інцидентів, аудит систем і реагування на кіберзагрози.