Політика використання мобільних пристроїв у «FinSecure Inc»

1. Мета та сфера застосування

1.1. Мета

Метою цієї політики є встановлення чітких правил та вимог щодо безпечного використання мобільних пристроїв (смартфонів, планшетів, ноутбуків) для доступу до корпоративних даних та систем «FinSecure Inc». Політика спрямована на мінімізацію ризиків, пов'язаних з втратою, крадіжкою пристроїв або несанкціонованим доступом до конфіденційної фінансової інформації.

1.2. Сфера застосування

Ця політика поширюється на всіх співробітників, підрядників та інших осіб, які використовують мобільні пристрої для доступу до інформаційних ресурсів «FinSecure Inc», включаючи:
Корпоративні пристрої (COD – Corporate-Owned Device): пристрої, належні компанії.
Особисті пристрої (BYOD – Bring Your Own Device): приватні пристрої, що використовуються для робочих цілей.

2. Визначення категорій пристроїв та загальні правила

2.1. Корпоративні пристрої

Опис: Смартфони, планшети та ноутбуки, належні «FinSecure Inc», видані співробітникам для виконання службових обов'язків.
Правила:
Використання виключно для робочих цілей. Обмежене особисте використання допускається за згодою керівника, але не повинно становити ризик для безпеки.
Пристрій підлягає обов'язковій реєстрації в системі MDM (Mobile Device Management).
Співробітник несе повну матеріальну відповідальність за виданий йому пристрій.

2.2. Особисті пристрої (BYOD)

Опис: Приватні смартфони, планшети та ноутбуки співробітників, які використовуються для доступу до корпоративної пошти, календарів та додатків.
Правила:
Використання особистих пристроїв для роботи дозволяється за наявності письмової згоди співробітника та після реєстрації в MDM/MAM-системі.
Компанія має право встановити обмеження та правила безпеки на робочий профіль/додатки на особистому пристрої.
Ноутбуки: Використання особистих ноутбуків для прямого доступу до корпоративної мережі (наприклад, через VPN) заборонено. Дозволяється лише веб-доступ до схвалених корпоративних систем через захищені з'єднання.

3. Вимоги до безпеки пристроїв (MDM)

3.1. Базові вимоги для всіх пристроїв, що отримують доступ до корпоративних даних:
Обов'язкове використання PIN-коду/пароля: Пароль має містити не менше 6 символів. На корпоративних пристроях – не менше 8 символів, включаючи цифри та літери.
Автоматичне блокування: Автоблокування має активуватися не пізніше ніж через 5 хвилин бездіяльності.
Шифрування даних: Обов'язкове шифрування внутрішньої пам'яті пристрою (наприклад, FileVault для macOS, BitLocker для Windows, вбудоване шифрування для iOS/Android).

Вимоги до програмного забезпечення: Операційна система та програмне забезпечення мають підтримуватися виробником та бути актуальними.

3.2. Процедури дій у разі втрати або крадіжки пристрою:
Співробітник зобов'язаний негайно повідомити службу інформаційної безпеки (ІБ) та свого керівника.
Служба ІБ має можливість дистанційно:

1. Заблокувати пристрій.
2. Активувати пошук пристрою (якщо функція доступна).
3. Виконати повне віддалене очищення (wipe) всіх даних на корпоративному пристрої.
4. Для BYOD-пристроїв – виконати очищення виключно корпоративного профілю та всіх корпоративних даних.

3.3. Додаткові заходи безпеки:
VPN: Обов'язкове використання схваленого корпоративного VPN-з'єднання для доступу до внутрішніх ресурсів компанії з будь-якої зовнішньої мережі.
Двофакторна автентифікація (2FA): Обов'язкова для доступу до всіх корпоративних систем (пошта, CRM, фінансові платформи).

4. Керування застосунками (MAM)

4.1. Дозволені застосунки:
Доступ до корпоративних даних дозволяється лише через схвалені компанією застосунки (наприклад, Microsoft Outlook, Authenticator, схвалені фінансові програми).
Перелік дозволених застосунків підтримується та розповсюджується службою ІБ.

4.2. Обмеження та заборони:
Заборонено встановлення та використання застосунків, які не пройшли перевірку безпеки (наприклад, сторонні клієнти месенджерів, файлообмінні програми з невідомих джерел).
Соціальні мережі та некорпоративні засоби комунікації: Використання на корпоративних пристроях заборонено. На особистих пристроях (BYOD) використання соціальних мереж у робочий час не заохочується, але не блокується, якщо це не порушує корпоративний профіль безпеки.

4.3. Оновлення безпеки застосунків:
Усі корпоративні та дозволені застосунки мають оновлюватися до останньої стабільної версії.
Система MAM забезпечує автоматичне розгортання оновлень безпеки для критично важливих додатків.

5. Політика BYOD (Bring Your Own Device)
5.1. Вимоги до особистих пристроїв:
Підтримувані платформи: iOS версії не старішою за 2 останніх випущених версії; Android версії не старішою за 2 останніх випущених версії. Пристрої з джейлбрейком/рутованим доступом не допускаються.
Критерії дозволу: Рішення про дозвіл на використання особистого пристрою приймає керівник співробітника за погодженням зі службою ІБ на підставі перевірки пристрою на відповідність вимогам безпеки.

5.2. Захист корпоративних даних на особистих пристроях:

Контейнеризація (розділення даних): На всіх BYOD-пристроях обов'язково впроваджується корпоративний профіль (контейнер) за допомогою MAM-рішень. Це забезпечує ізоляцію робочих даних (пошта, контакти, документи) від особистих.
Корпоративні застосунки: Усі робочі додатки встановлюються та керуються всередині корпоративного профілю.
Права компанії: «FinSecure Inc» має право дистанційно видалити корпоративний профіль та всі корпоративні дані в разі:

Втрати пристрою.

Припинення трудових відносин із співробітником.

Виявлення порушення цієї політики безпеки.