USE IT MATE

The Mobile Agent Security Blueprint

How to secure your team when they are working from cars, cafes, and open homes.

Author: Jasson Borgueta, Technical Lead — Use IT Mate (Bundaberg & Wide Bay)
support@useitmate.com

Your office is secure. Your agents out in the field are not.

Property Managers and Sales Agents spend 50% of their week outside the office. They are opening confidential tenant ledgers at local cafes, reviewing lease agreements in their cars, and leaving iPads on kitchen counters during open homes.

Here is how corporate agencies lock down their mobile workforce.

Store the completed checklist with employee records.

1. The "Public Wi-Fi" Ban
Logging into PropertyMe or VaultRE on a free cafe or airport Wi-Fi network is a massive vulnerability. These networks are easily spoofed by hackers sitting in the same room.

- The Rule: Agents must be banned from using public Wi-Fi. They must be instructed to only use the built-in 4G/5G Hotspot on their company iPhone to connect their laptops to the internet while on the road. It is encrypted, private, and costs the agency almost nothing in extra data.

2. Visual Hacking & Privacy Filters
If a PM is answering emails at an open home or a coffee shop, anyone standing behind them can photograph confidential rental applications or financial ledgers.

- The Fix: Every agency laptop must be fitted with a Magnetic Privacy Filter (approx. $60). These black out the screen for anyone not looking directly at it head-on, completely eliminating "shoulder surfing."

3. The "Lost Device" Protocol (MDM)
If a Sales Agent leaves an unlocked agency iPad in an Uber, whoever finds it has immediate access to your entire CRM.

- The Fix: All portable devices must be enrolled in a Mobile Device Management (MDM) platform like Microsoft Intune. If a device is lost, the Operations Manager can click one button to remotely "brick" the device and wipe it back to factory settings, destroying the data before it falls into the wrong hands.