BYOD 365 balances security and privacy for BYOD users on Office 365

"We get 320,000 attacks every day, mostly by email and many of those come through BYO devices."

J.Britton Tabor, Executive Vice President-Erlanger Health Systems

Without an appropriate policy and technical controls in place, your data is exposed when employees use unmanaged office 365 apps on their personal device.

BYOD 365 balances security for your organization with privacy for your employees.

Step 1: BYOD Policy Document

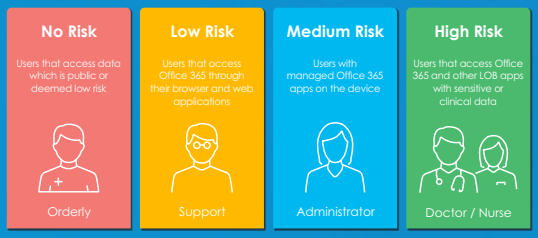
Mobile Mentor develops a BYOD Policy Document by working with IT, Security, HR, Finance and employees to achieve a broad consensus on security and privacy.

FINANCE	HR	EMPLOYEES	IT
Cost management	Eligibility criteria	Privacy protection	Office 365 Data
Risk and liability	Usage guidelines	Stipend model	Device security
Personal vs. business	Safe driving practises	Device management	Groups and profiles
International roaming	User profiling	Changing devices	Support workload
Carrier contracts	Device allocations	Email & Office 365	

Step 2: Tiered Trust Model

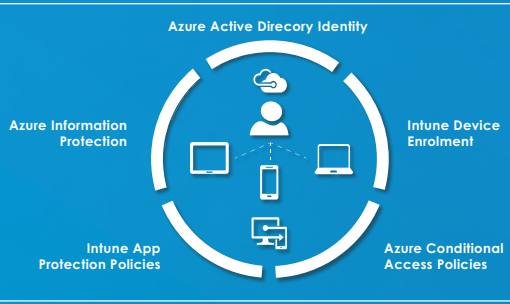
A Tiered Trust Model defines the security requirements for each persona based on their risk profile. We then design the appropriate security model for each persona.

An example of a Tiered Trust Model



Step 3: Implement in Intune test environment

Our engineers design and implement the appropriate settings and controls in your Microsoft environment for test and validation.



Outcome

BYOD employees will be more productive and feel assured their privacy is protected. Your data will be secure with appropriate controls applied to each employee.

USA 1 877 707 3848 - NZ +64 9 888 0512 - AUS +61 2 9575 4827
www.mobile-mentor.com

mobile mentor