Enabling Opportunity, Realising Potential

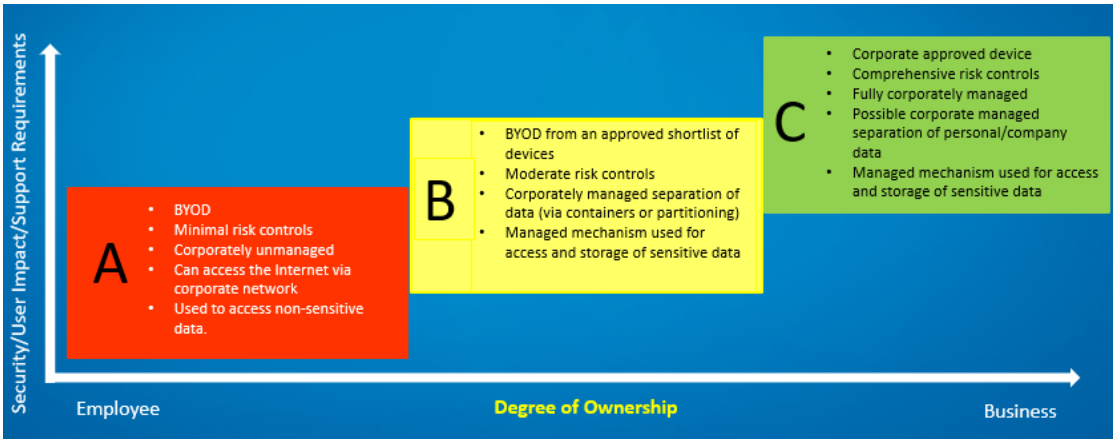
Mobile Device Management – Getting IT Right!

There are some important considerations and decisions you need to make before implementing Mobile Device Management.

Step 1: Assess your current mobility needs and practices in your business.

- Talk with managers and employees about their mobility needs
- Audit inventory of current/corporate devices
- Assess current work practices, and make decisions around how to:
  - Protect users and devices
  - Protect the corporate network
  - Protect your corporate data

Step 2: Decide on your approach to mobility



Step 3: Define your MDM process and policy considerations

Use the template overleaf and *Maxsum Sample Mobile Device Management Policy Documentation* to start defining your:

- Employee onboarding and exit policies
- MDM procedures and response processes
- Acceptable use policies
- BYOD/Corporate device use policies
- Channels for gaining consent and acknowledgement from users.

An employee leaves your business	Employee devices are lost or stolen	Disgruntled current or ex-employees

Mobile Device Management Policy Decisions

Listed below are key features and considerations for businesses seeking to define their approach to mobility and implement Mobile Device Management Policies for both BYOD devices and company-issued devices.

Features	Scenario B Managed BYOD Mobile Phones/Devices		Scenario C Managed Corporate Mobile Phones/Devices	
Mobile Phones				
Enforce devices to be locked with password/PIN/fingerprint scan/face unlock protection	YES		YES	
Install, use and manage MDM container apps	YES		YES	
Enforce use of company email through container apps only (Block company email use via non-container apps)	YES		YES	
Enforce document/file access and use through container app	YES		YES	
Enforce containers to be protected with password/PIN/fingerprint scan/face unlock protection	YES		YES	
Deploy security app (Android)	YES		YES	
Allow container app only wipe	YES		YES	
Allow full device wipe	NO		YES	
Push company-approved apps to mobile phones/devices	NO		YES	
Install only corporate approved apps via a Company App Store (Block all other app via App Store/ Playstore)	NO		YES	
Allow corporate Wi-Fi/VPN access	NO		YES	
Push corporate certificates	NO		YES	
Block camera use	NO		YES	
Allow device password reset	NO		YES	
Show location tracking for lost/stolen devices	NO		YES	
MacOS Devices				
Enforce password policies				
Allow Airprint				
Allow Wi-Fi/VPN access				
Allow device wipe				
Windows Devices				
Enforce password policies				
Allow Wi-Fi/VPN access				
Allow device wipes				
Allow set-up email profile/exchange/ Office 365				
Deploy SSL Certificates				

**This is a generic list of items involved in common MDM implementation scenarios. There may be other IT environment or device-specific considerations that will require further investigation.*

***Available features and recommendations are subject to change and updates.*