Utelize®

Utelize Mobile Best Practice Guide

Approach to Mobile Device Lifecycle Management (MDLM)

Prepared by
Utelize Communications Limited
www.utelize.co.uk

Enabling Mobile IT

Mobile devices are getting more complex and costly to support

The rapid growth of smartphone and tablet adoption within business has brought a range of new challenges for IT teams to manage. This whitepaper looks at the various elements of managing the 'lifecycle' associated with mobile devices and reviews how organisations can reduce the total cost of ownership (TCO) when it comes to supporting devices.

Most organisations are already familiar with the ongoing challenges of managing device security policies using mobile device management (MDM) and enterprise mobility management (EMM) software. The requirement to protect both devices and confidential data from a growing range of security threats has never been greater, and the introduction of new EU General Data Protection Regulations (GDPR) in May '18 will only serve to drive further controls in this area. However, security is just one of the challenges facing many IT teams, who are being asked to support a growing number of business, and, in some cases, BYOD tablets and smartphones.

The fact is, mobile devices are no longer disposable items, smartphones can be more expensive than laptops, and often contain similar - or greater - levels of confidential personal and business data. And, of course, they are re-saleable, portable, prone to damage therefore loss, damage, and thefts are high.

As a result, organisations of all sizes are starting to consider the management of these devices as a 'lifecycle' process, in the same way that they do with other mobile computing.

Key elements of mobile device lifecycle management (MDLM)

The lifecycle covers many different stages and whilst each organisation will adopt a different approach to managing its mobile devices, the lifecycle is common, and usually covers the following stages:

1. **Sourcing** – which devices to deploy, and where to source them from
2. **Finance** – how to pay for devices, and whether to own or lease them
3. **Security** – applying the right balance of mobile device management and threat prevention
4. **Staging** – preparation of devices for end users
5. **Repairs & Insurance** – in-life support and management of repair processes
6. **Disposal & Recycling** – ensuring end-of-life device wiping, and securing the residual value of the device

This whitepaper reviews each of these core lifecycle elements and explores a range of measures that organisations can take to streamline support and reduce long term device ownership costs.

Sourcing

Traditionally, most businesses have purchased mobile devices as part of their mobile network contract, typically using some form of 'tech fund', or device subsidy. A growing number of businesses are, however, looking to bypass this model and purchase devices independently as a way of improving security and reducing costs.

Mobile tech funds are a clever way for mobile networks to encourage their customers to buy mobile devices directly from them, rather than explore the marketplace. This model had some merit when the cost of the device represented a small fraction of the cost of the airtime over the contract term. Today, however, when smartphones are often significantly more expensive than the airtime over a 24-month period, trying to partially subsidise or fund the device with airtime makes little sense.

However, for a mobile network to provide a tech fund in the first instance, they must first inflate airtime costs. If, for example, your mobile contract contains £100,000 of inclusive tech fund, then it is highly likely that the network artificially increased your airtime costs by a value that exceeds this £100,000, or they expect to recover this amount in hidden overspending and overage margins (like roaming). To protect themselves, the network will often place minimum spend or connection commitments in the contract to guarantee their return - but in most cases, they won't provide additional subsidy if the minimum commitments are exceeded.

Once you have been provided with a tech fund, the mobile network has you as a captive audience, and they are almost certainly guaranteed the orders for your mobile devices. However, as few organisations know in advance what devices they will need, or which new devices may come to the market, then few negotiate detailed terms around device purchases from their network. As a result, the cost of devices purchased using a tech fund can be up to 10% more expensive than purchasing these devices from the market, and it is rare that the networks will negotiate on the cost of devices when a tech fund is used for payment. So, it's not uncommon to find that the mobile network is making significant additional margin at your expense on both the airtime and devices. Considering devices are now commonly more expensive than airtime, this could be materially impacting upon your telecoms budget.

Mobile networks are trying to address the growing challenge of funding more expensive devices by offering longer contract terms of 30 or 36 months, or more. Whilst on paper this generates more tech fund, it creates greater problems. Corporate devices are unlikely to last three or more years, warranties only last 24 months, and it simply locks in airtime pricing on terms that will drift further out from the market. Most organisations taking a three-year contract end up re-signing mid-term when their tech fund runs out, leaving them with little room to negotiate market competitive terms.

Cost, however, is not the only consideration when purchasing devices. Mobile software security patches are frequently updated by manufacturers/OS providers to address the latest risks and security threats. Part of your mobile device security best practice will be to ensure that these patches are updated upon release to minimise risks. However, when you purchase a device through a network, the network - not your IT team - determines whether and when the update will be released. So, if you want full control of your mobile device security, sourcing 'factory open' and unlocked devices will mean that you will have access to updates as soon as they are available. Unlocking a network-provided mobile device does not change the OS updates process, which is why ideally you should consider factory open devices.

Finally, the sourcing of open and unlocked devices has two main secondary advantages. First, it allows users to change network in the future without having to unlock the device from your existing network. Secondly, unlocked devices retain a greater residual value. We explore residual value (RV) in greater detail in the next section.

For organisations looking to gain the maximum value for money, there is also the opportunity to significantly reduce device purchase costs by investing in Premium Used Devices. Professionally wiped of all user data, fully refurbished and restored and boxed as new with a new IMEI, most users would be hard-pressed to ever know their device was not brand new.

Many Premium Used devices have never even been used - they have simply been opened and returned, requiring re-packaging professionally, and they normally come with a full warranty. Premium Used devices could help your business to reduce device costs by up to 20% as against purchasing brand new devices, and are a very good way of maintaining stock for repairs and losses.

Key Points

- Buying mobile device from a network using a tech fund is easy – but you will probably be overpaying for both the airtime and devices
- Mobile devices, when appropriately sourced from the market, will be factory open and unlocked – this makes it easier to change network in the future
- Unlocked devices typically retain a greater residual value than network locked devices
- Factory open devices allow you to update security patches quicker than network locked devices
- Premium Used devices can help to significantly reduce the cost of purchasing mobile devices

Finance

Most mobile device purchases are normally either purchased outright as a CAPEX (capital expenditure) or as a one-off OPEX (operating expense), recently, there has been an emergence of different finance options which has transformed this model. Organisations can now choose to spread purchase costs over 24–36 months, or even lease (rent) the device as an alternative to an outright purchase. This not only breaks the traditional tie to purchasing devices through the mobile networks, and the hidden costs of buying devices through tech funds, but it also creates opportunities to more cost-effectively upgrade technology for your users. In short, you can choose to either reduce device purchasing costs, or use the same budget to secure access to improved technology for your employees.

The cost of leasing devices is driven by three main factors:

- The finance cost – this is based on the credit-worthiness of your organisation
- The anticipated residual value (RV) left in the device at the end of the term
- The term that you wish to use the device for

Investing in devices which have the highest levels of RV means that the cost of finance can be reduced, because the finance company will get some of the cost back on the original device, so in effect they only need to finance a percentage of the actual device value.

As a guideline, Apple devices typically retain the greatest RV after 24 months, often above 20%, whereas some other devices can be almost worthless (even when in good condition). This leads to a scenario where it can be less expensive to fund a more expensive Apple device than it is to fund a lower cost one. If your organisation is aiming to use a device for more than 24 months, then you may find that purchasing the device is a more cost-effective solution than leasing.

Therefore, including your Finance department in mobile device purchasing and funding discussions is now a critical component to consider when investing in mobile devices, regardless of whether you are planning to purchase from the market or via a tech fund. If the Finance team does not understand RV, GDPR and WEEE (Waste Electrical and Electronic Equipment Directive) regulations - meaning you will have an obligation to collect, wipe and recycle the device at the end of its life - then you'll probably end up overspending and having budget issues down the line.

Rather than simply looking at the one-off cost of the device, look at the cost of ownership, and be sure to review residual values, and end-of-life recycling costs, and you may find that leasing can be one option to reduce the overall cost of devices by 10-15% - or even more.

Whether you purchase or lease devices, by decoupling mobile devices from airtime contracts your organisation will be able to have much better transparency of costs and potentially negotiate more flexible and lower cost airtime contracts on a SIM-only basis. It may also be possible to use multiple networks to secure the best coverage options for your users.

Mobile networks like to bundle devices and network over 24–36 months because these terms lock you in as a captive customer, and allow them to maximise profits. Separating network from device costs makes the whole process more transparent and will not only allow you to negotiate much shorter lock-in terms, it will also reduce the total cost of ownership for mobile devices and airtime.

Key Points

- Renting/leasing allows organisations to treat mobile devices as an OPEX cost
- Renting/leasing costs are impacted by creditworthiness, contract term, and residual value
- Not all mobile devices have the same residual value (in percentage terms) – currently, Apple devices achieve the greatest RV after 24 months, so they can be more cost-effective to lease than other devices of the same value
- Leasing works best on an 18-24 month term – if your organisation is looking to utilise assets for 3-4 years, then capitalising the purchase may offer better value
- Leasing arrangements can be combined with wider device lifecycle services – for example: end-of-term device wipe; break/fix support; extended warranty; and insurance. If you are looking for a full support service, leasing can be an effective way to secure this as a single monthly payment per device
- With leasing, you will not own the device at the end of the term, and any unreturned or damaged devices will need to be paid for – normally this is capped at the residual value of the device and not the cost of a replacement

Security

This section is a summary of the key elements of mobile security, looking at the role of mobile device management (MDM) software, enterprise mobility management (EMM), and mobile threat prevention (MTP). We also review the role of Apple DEP and OS patches and upgrades, and the importance of sourcing mobile devices from the right vendors.

Enterprise Mobility Management (EMM) – is the set of people, processes and technology focused on managing mobile devices, wireless networks, and other mobile computing services in a business context. It incorporates MDM, MAM and MCM.

Mobile Device Management (MDM) – this software controls the policies around your organisation's mobile device management, allowing personal and business data to be separated, limitations of specific phone functions, etc. When devices are in breach of the policies alerting and reporting can highlight exceptions, force updates, or remove applications. When devices are lost or stolen it allows tracking of the phone, and can support locking and wiping of corporate information.

Mobile Content Management (MCM) – this provides secure access to corporate data on smartphones, tablets and other endpoint devices.

Mobile Application Management (MAM) – these tools allow the business to manage application updates, and control or bar access to specific applications.

Mobile Threat Defence (MTD) – this provides organisations with more sophisticated protection from advanced malware and device security threats, providing even greater levels of protection from risk and data loss.

Organisations deploy these and other tools in varying degrees depending on the type of user and device, and the level of sensitive data that is involved. For some, simply being able to lock and wipe a device is sufficient to meet the IT security policies, whilst for others there will be more restrictive policies, and a separation of business and personal data combined with full MTD services. In all cases, there is a balance to be found – restricting devices and imposing high levels of control are great for security, but they often involve removing the very functions that deliver a great user experience and productivity gains.

Security & Sourcing

Whilst cost is always an important consideration when purchasing devices, it is important to understand that there are significant differences between purchasing 'factory open & unlocked' devices, and devices provided by your mobile network. Mobile software security patches are frequently updated by manufacturers/OS providers to address the latest risks and security threats. Part of your mobile device management & security 'best practice' should be to ensure that patches are implemented upon release to minimise risks.

When you purchase a device through a network, they determine when these updates will be released, not the IT team. If you want full control of your mobile device security, sourcing 'factory open & unlocked' devices will mean that you will have access to updates as soon as they are available. Unlocking a network-provided mobile device does not change the OS updates process, which is why ideally you should consider factory open devices.

Staging

Staging is the process of pre-configuring mobile devices for users prior to deployment.

Examples of basic device staging can include:

- Charging the device
- Inserting and testing the SIM card and network connection
- Adding ‘asset tagging’
- Testing the device’s basic operation
- Applying screen protectors/cases
- Including accessories in the package
- Including user guides and information in the package

More complex staging can include:

- Updating operating system software (O/S)
- Configuring device settings
- MDM enrolment
- Apple DEP enrolment (see below)
- Device encryption
- Configuring email and corporate applications
- Installing business application containers
- Configuring MTD

Configuring mobile devices can be a time-consuming process and often detracts from other, higher priority activities. When the configuration of devices is managed centrally, each device reaches the end user fully tested and operational. This significantly cuts down user support and issues, and removes the need for users to set up their own devices.

Depending on how mobile devices are sourced, it is possible to add staging services to the fulfilment process. With staging services, a third party will set up the device to an agreed specification. The specification will be tailored to your own organisation, and typically charged based on a fixed cost per device.

To establish the fixed cost, the staging provider will work with the customer to create a fully-documented process, and once the process is agreed, the service provider will typically complete two individually timed device builds, measuring the actual time spent to complete each build. The average of these two times will then be taken to create the cost per build.

Apple's Device Enrolment Program (DEP)

Apple's DEP is gaining greater adoption within larger organisations who are looking to simplify the configuration of iOS and macOS devices. DEP allows organisations to apply true corporate ownership and supervision of the device, and to automate enrolment to the organisation's MDM platform, without having to take the device out of the box. To simplify the process further, it's possible to skip certain Setup Assistant screens so users can start using their devices right out of the box. From iOS 11 it will also be possible to register devices purchased outside of Apple's authorised reseller program.

DEP key features:

- **MDM enrolment** - iOS devices can be preconfigured to require automatic enrolment into MDM – and devices can be locked into the MDM – so it reinstalls even if a factory reset is performed.

- **Wireless supervision** - enables enhanced corporate control and ownership of the device – for instance turning off iMessage, AirDrop, or Game Centre - and it provides additional device configurations and features, such as web content filtering.

- **Zero-touch configuration for IT** - with DEP, once users activate their devices, account settings, apps, and access to IT services can be auto-configured over the air. You don't need staging services or to physically to access each device to complete the setup.

- **Streamlined Setup Assistant** - DEP also makes it easier for users to set up their own iOS devices and Mac computers. Using an MDM solution to configure devices, users are guided through the activation process with the built-in Setup Assistant, and IT can specify that certain set-up screens are skipped.

- **Availability** - DEP is available in the following countries or regions: Australia, Austria, Belgium, Brazil, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hong Kong, Hungary, India, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, United Kingdom, and United States.

Key Points

- Staging is often a hidden IT cost that can consume significant IT resources, especially on larger device refreshes
- Staging services can reduce the impact on IT, and should be based on documented 'build specifications' and a timed set-up
- Staging devices minimises user time spend on setting them up, and ensures a consistent configuration
- Apple's DEP program enables organisations to simplify and reduce the cost of configuration and MDM enrolment without touching the device

Repairs & Insurance

One of the downsides to smartphone ownership is the significant increase in damage and vs. basic models. That, coupled with the higher cost for smartphone screens and repairs, it is likely that mobile device repairs and supports costs are set to increase in the future.

Market estimates vary significantly, and typically indicate that over a two-year period between 20% and 40% of smartphone devices will develop some form of user-impacting fault or problem, and most likely this will be caused by user damage. Accidental damage is responsible for over 90% of smartphone failures, with damage from drops and liquid damage being the main causes. For larger corporate estates, this number is likely to be lower than the average, and our customer feedback indicates that repairs and losses run at about 10-15%. This figure may, however, hide repairs completed by users, or losses masked as 'upgrades', that are also more common with corporate mobile estates.

Whilst cases and screen protectors are a low-cost consideration, significant numbers of business users still don't protect their phones. Increasingly, manufacturers are making their devices water resistant, and so that should help reduce the estimated 100,000 smartphones that get damaged by water or other liquids.

According to insurance company 'Protect Your Bubble', 446,000 people in the UK had their phones stolen last year (2016), for those organisations that don't use MDM tolls and policies, only 53% of users have a pin code protecting their devices, 21% use a tracking app and 32% take no security measures at all.

Planning for these inevitable losses is an important element of mobile device lifecycle management, and spans a wide range of areas:

- **Device inventory** – This needs to track who owns/uses the device, where the device was purchased from and when, and details including the IMEI. Most MDM software will provide some form of device inventory, although extending this to capture purchase and support details is recommended.

- **'In warranty' repairs** - manufacturer faults are becoming less common, and typically 'in warranty' repairs will represent only a very small percentage of an organisation's device faults and repairs. Most manufacturers offer a 24-month standard manufacturer warranty, Apple's is 12 months. Establishing processes for 'in warranty' repairs is key to reducing downtime for users and IT teams. Some vendors will offer a next day swap-out, where the faulty device is replaced with another device, which may only be for a limited time, after which you will need to send the device back to the manufacturer directly.

  For Apple devices, it is possible to extend the warranty using Apple Care; however, for larger estates this is an expensive route. Instead, most authorised Apple repair partners also offer some form of in-house extended warranty.

- **'Out of warranty' repairs** – the cost of repairs can be very expensive, and often significant damage means that the phone can be beyond economic repair ('BER'). Despite this, it is still important to establish a repair or swap-out processes for damaged devices, to reduce user downtime and the impact on IT resources.

  Most authorised repairers will offer an initial estimate based on a description of the damage, followed by a formal quotation when they receive the device. As part of your repair processes, it is important to establish the logistics/delivery process, and associated costs.

- **Insurance** – At an individual user level, for a personally-owned device, applying insurance to a smartphone device makes sense, as the cost of a single claim for damage, loss or repairs will typically outweigh the cost of insurance.

  For organisations that wish to insure devices, we would recommend that you also consider talking to your existing commercial insurance company. Often, commercial insurance policies will assess mobile device estates on a different risk basis from individuals, which can substantially reduce the costs.

  For larger mobile estates, or where the repair statistics are not yet understood, it may be more cost-effective to create a pool of devices to cover replacements.

  Alternatively, purchasing Premium Used Device as replacements will provide an immediate stock of devices to exchange with users' devices whilst theirs is being repaired, and will typically cost about 20% less than new devices. Whilst Premium Used Devices often look and feel like new, the replacement of existing devices with the same (but refurbished) devices can help to reduce claims by employees who are simply looking for upgrades.

- **Out-of-hours support** – whilst it is possible to put in place 24/7 support that can manage the device swap-out process and repairs at any time, it is an expensive support model, and so most organisations don't support it. This leaves businesses exposed to security risks when devices are lost or stolen outside normal business hours. The sooner lost, and stolen devices are reported, the sooner the network can lock down the SIM, (and prevent unauthorised usage and business costs) - and the sooner MDM lock, locate, and wipe policies can be invoked.

  If users can't report these losses to IT support until Monday morning, this poses a significant risk - especially with new EU GDPR regulations that require data losses to be reported within 72 hours. Having a basic support service, or self-service functionality to enable devices and SIMs to be locked down in the event of out-of-hours losses, is highly recommended for all organisations.

Key Points

- Over 24 months, expect between 10% and 20% of your smartphone estate to suffer some significant damage or loss
- Alternatives to traditional mobile insurance policies may substantially reduce costs – talk to your existing commercial insurance company first to get a clear cost and terms
- Well-defined repairs and replacement processes can remove significant hidden IT support costs, and get users back up and running more efficiently
- Consider using Premium Used Devices as replacements to reduce costs
- Evaluate out-of-hours processes – do users know who to contact? Are current processes suitable to lock down devices and SIMs in the event of a lost or stolen device?

Disposal & Recycling

Whilst consumers have long understood that smartphones have a residual value, organisations and businesses have been slower to adopt formal recycling and resale processes. The fear of data and information getting into the wrong hands probably outweighed the financial benefits of resale. However, in practice, for many organisations these devices either remain in top drawers, or are passed on to friends and family with no accountability or tracking. With existing WEEE directives, and the upcoming EU GDPR regulations from May 2018, this is no longer going to be an acceptable practice.

When it comes to the end of the lifecycle for your mobile device, the options depend on the residual value of the device and your internal processes and inventory. In the section 'Mobile Device Finance' above, we reviewed the impact of differing residual values across different device models and manufacturers. For devices that retain a solid residual value, the disposal of the device to a suitable IT asset recycling and disposal business should be considered.

The process with a security accredited or ISO27001 provider should include a certified professional device wipe (normally triple wipe), and as part of the process the value should be pre-agreed (subject to the device meeting the agreed quality). When recycling a sizeable mobile device estate, it is also possible to work on a 'share of resale' model. In this model, the asset disposal firm will refurbish the equipment on your behalf, and then share the achieved resale value or margin with the business.

For organisations looking to refresh devices, it may be worth considering using the residual value to achieve an improved price for the new devices, and to ensure certified disposal or resale in the process.

For devices with a very low or non-existent residual value, the priority is to ensure a secure WEEE certified recycling or destruction process, where nothing goes to landfill. Whilst the devices may have limited resale appeal, most devices do contain some base material value, and it may still be possible to negotiate a 'nil net cost' recycling process that ensures that the devices are professionally recycled.

Conclusion

Mobile device lifecycle management is a rapidly-evolving and complex business challenge. However, approached strategically, it is possible to reduce the impact on your IT team, and optimise long-term expenditure in the process

Connect with Utelize to discuss your communications solutions

We specialise in helping enterprises and large public-sector organisations to manage and procure mobile airtime and devices. We provide consulting, technology and resources, helping our customers to:

- manage mobile services, devices, security and usage proactively
- reduce mobile costs significantly
- optimise mobile airtime and device administration
- negotiate flexible and competitive terms from mobile networks
- understand the impact of wholesale and regulatory changes in the telecoms market
- evaluate which mobile telecoms technologies and services can best support their business needs

To arrange a no obligation meeting, reach out to us

hello@utelize.co.uk

03300 240 444

www.utelize.co.uk

Utelize®