TLP: WHITE

Rialtas na hÉireann
Government of Ireland

Mobile Device Management for Public Sector Bodies

March 2023

V1.0

Prepared by the Department of
the Environment, Climate and Communications
gov.ie

Version	Status (Draft or Approved)	Date	Author/Editor	Details of changes
0.1	Draft	30/03/23	NCSC Engagement	Initial document compiled.
0.2	Draft	03/04/23	NCSC Engagement	Feedback from stakeholders.
1.0	Approved	06/04/23	NCSC Director	Approved by NCSC Mgmt Team.

1. Contents

2. Executive Summary

The widespread use of mobile devices has brought about a new and evolving level of cyber security related risk to organisations. The flexibility and convenience that these devices provide to employees in performing daily activities and accessing information, has resulted in their extensive use within the Information and Communications Technology (ICT) environment of all Public Service Bodies (PSBs). Risks associated with these devices are more pronounced where devices are used for both personal and business purposes. It is essential that these devices are secured against cyber-attacks, data breaches and other malicious activities.

The aim of this document is to supplement the existing Cyber Security Baseline Standards (CSBS) framework. This framework addresses ICT challenges for improved resilience and security of public sector ICT systems and outlines controls that organisations should have in place to mitigate risks. The measures outlined in this document will provide an additional level of granularity to ensure an acceptable security standard is achieved across the PSBs for all mobile devices.

The implementation of a Mobile Device Management (MDM) framework will introduce several benefits to organisations:

- Better Management of Devices
- Secure Data and Applications
- Enhanced Productivity and Efficiency

Within this document the process of mobile device security will focus on the following specific areas:

- An overview of the threats arising from the use of mobile devices.
- Guidance on conducting a risk assessment to ensure the appropriate level of security is put in place by each PSB relative to their risk profile.
- Advice on the procurement of devices & the various deployment models.
- Guidance on the use of MDM processes and tools.
- An overview of the appropriate security measures that PSBs should implement based on their risk assessment.
- A process to vet the security of third-party applications

Mobile device cyber security is critical to protecting sensitive data and ensuring business continuity. By following the process outlined in this document PSBs can ensure that their mobile devices are secured against potential security threats. It will be necessary to establish the use case for devices within an organisation and consider the relevant recommendations that are applicable.

A summary of the **top 10** items of importance from this guide is as follows:

1. Use MDM to manage corporate fleets.
2. Maintain a register of mobile device assets and to whom they are assigned.
3. Before deploying mobile devices, perform a risk assessment by identifying the threats and vulnerabilities associated with the range of mobile devices within the organisation.
4. Review assignment of devices at least annually
5. Have a strict process around the management of mobile devices for joiners, movers, and leavers in your organisation.
6. Consider whitelisting and blacklisting applications in line with your corporate social media policies.
7. Force Operating System updates as well as automatic app upgrading.
8. Have the facility to remote wipe a mobile device.
9. Deploy strict security policies.
10. Review security sources around mobile devices

3. Introduction

This guidance document provides guidance in relation to the deployment and management of mobile devices. Mobile devices often need additional protections due to their portability, small size, and common use outside of an organisation's network, which generally places them at higher exposure to threats than other endpoint devices.

3.1. Purpose

This Mobile Device Guidance document is intended to supplement the Public Sector Cyber Security Baseline Standards, which follow a holistic and outcome-based approach to Cyber Security by providing additional detail and considerations for mobile devices which are issued for business use across the organisation. The document explains security concerns inherent in mobile devices and the guidance presented here are a set of measures which are intended to create an acceptable security standard which can be revised over time to address new threats and vulnerabilities and to keep pace with new technologies and suppliers.

3.2. Scope

Mobile devices in scope include smartphones (including tablet devices) which can connect to Wi-Fi and telecommunication networks such as GSM/5G. Other mobile devices such as laptops and proprietary devices are out of scope of this document, as notwithstanding a degree of convergence of the management technologies used for mobile and desktop/laptop devices, the security capabilities currently available for laptops are different than those available for smartphones. Furthermore smartphones/tablets generally contain other features not generally available in laptops such as multiple wireless interfaces, numerous sensors including cameras and GPS In addition to the physical aspects of the devices, there are data and application factors that should be considered.

3.3. Audience

This guidance document provides guidance to ICT Managers in relation to the deployment and management of mobile devices. These guidelines are applicable to all PSBs.

4. Threat Landscape

Allowing staff to view, use or make changes to corporate data on a mobile device is essential for a modern PSB, however certain threats arise as a result of that decision.

Allowing data to be accessed on a mobile device needs to be considered in the context of that data being taken off site and out of the safety of a secure office building as well as a secure office PC and a secure work network. Mobile devices allow an end user to take that data anywhere and possibly make changes to it on a potentially unsafe device and unsafe network.

The Covid-19 pandemic and the advent of widespread remote and blended working, as well as the general need for some staff to work and travel means the use of mobile devices is essential. This requirement has led to an increased requirement for the installation of work applications and remote access software or email clients on mobile devices. It is important for PSBs to understand what the risks are, what are the types of attacks that can affect a mobile device and what the consequences of a breach are. This document also addresses how PSBs can assess those risks and what you can to in order to mitigate them.

4.1. Mobile device security risks

There are many risks associated with allowing an employee access to company data and email on a mobile device. Being aware of these risks is the first step towards protecting the data that can be accessed on that mobile device with the end goal being to mitigate as many of these risks as possible. Some of these risks include:

- **Data leakage**: If an employee's mobile device is lost or stolen, sensitive information stored on the device could be compromised.
- **Unauthorised access**: If an employee's mobile device is not properly secured, unauthorised users may be able to access the device and company data.
- **Malware and phishing attacks**: Mobile devices can be targeted by malware and phishing attacks, which can compromise data and lead to other security breaches.
- **Compliance with regulations**: PSBs are subject to regulatory compliance requirements, such as GDPR, which may prohibit or restrict the use of mobile devices for accessing sensitive data.
- **Level of control**: PSBs may have limited control over employees' personal mobile devices, which may not have the same security measures in place as company-owned devices.
- **Employee turnover**: If an employee leaves the PSB, they may still have access to company data on their personal mobile device, creating a potential security risk.

- **Public Open Wi-Fi**: Connecting to open public Wi-Fi networks that do not require a password or use encryption is convenient, but end users need to be advised to avoid public open Wi-Fi and made aware that by connecting to them this could allow anyone nearby to easily spy on their online activity. Even worse, a cybercriminal can create a fake Wi-Fi hotspot in order to trick users to connect to it and steal their data.
- **Malicious or Unsafe apps**: Often, if an app or game that provides a useful function or is very entertaining but cost nothing and you believe that it is too good to be true then that is probably because it is. Most free apps make their money through data collection of other information on your phone and can even listen through your mic or check your search history or these apps could even be malware pretending to be something else.
- **USB Connections:** There is the potential for malware to be uploaded onto mobile devices at compromised public USB charging points or through maliciously modified charge cables, which can lead to access to the device data. Mobile devices also have the potential of passing on malware to PC/Servers through USB port connections and this can be prevented through the AV scanning of USB devices, disabling of USB ports and appropriate DLP measures.

To mitigate these risks, PSBs should implement policies and procedures for mobile device usage, including security requirements such as password protection, encryption, and remote wiping capabilities. Additionally, PSBs may consider providing employees with corporate devices for accessing the organisation's data and email to maintain better control and security.

4.2.Types of attacks that can target mobile devices.

There are many ways in which an attacker might target a mobile device. Similar to the security risks, being aware of these can help in the mitigation of these risks. Some risks include:

- **Malware**: Malware is a type of software that is designed to damage, disrupt, or gain unauthorised access to a computer system. Malware can infect mobile phones through various means, including downloading malicious apps or clicking on phishing links.
- **Spyware:** This is a classification of software that monitors and records user activity, can be used to eavesdrop on conversations and access data that is stored or transmitted by device. It can be installed on devices through the side

loading of compromised third party apps, visiting compromised websites, or installed manually on unattended devices.

- **Phishing**: Phishing is a technique that cybercriminals use to trick users into providing sensitive information such as login credentials, credit card details, and personal information by posing as a trustworthy entity or individual. Phishing attacks can be carried out via email, text messages, social media, or phone calls.
- **Smishing**: Smishing is a type of phishing attack that is carried out through SMS or text messages. In this type of attack, cybercriminals send text messages with a link that, when clicked, downloads malware onto the mobile device.
- **Wi-Fi Eavesdropping**: Wi-Fi eavesdropping is a technique used by cybercriminals to intercept Wi-Fi traffic and steal sensitive information such as passwords, credit card details, and personal information. This attack is carried out by setting up a fake Wi-Fi network that appears to be legitimate but is actually controlled by the attacker.
- **Bluejacking**: Bluejacking is a type of attack that targets Bluetooth-enabled devices. In this type of attack, the attacker sends unsolicited messages or files to the victim's device using Bluetooth technology.
- **Rogue Applications**: Rogue applications are mobile apps that are designed to look legitimate but are actually malware in disguise. Once installed, these apps can steal sensitive information, display unwanted ads, or hijack the device.
- **Physical Access:** Physical access to a mobile device can allow an attacker to bypass security measures such as passwords or biometric authentication and gain access to sensitive information stored on the device.
- **SIM card attacks**: SIM card attacks involve exploiting vulnerabilities in the SIM card, which is used to authenticate the device with the cellular network. This type of attack can allow an attacker to intercept calls, messages, and data transmitted over the cellular network.

4.3.The consequences of a breach

The consequences of a data breach on a corporate mobile device can be severe and wide-ranging, both for an individual's personal data as well as sensitive company data. If the work mobile device contains personal information, such as contact details, photos, banking information, or even health data, a data breach could lead to identity theft or financial fraud.

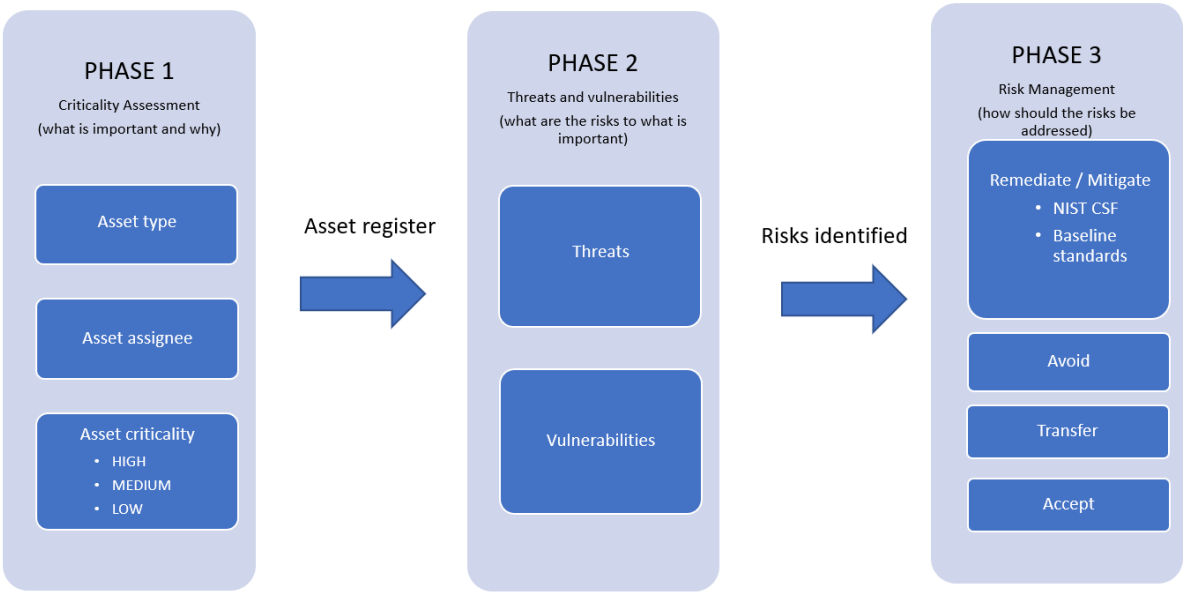
From an PSB point of view, a data breach could result in the loss of sensitive Government data and could damage the PSBs reputation and result in financial losses and also be a violation of General Data Protection Regulation (GDPR). Most data breaches also result in significant downtime to check and make sure future business and security practices will not lead to another incident. This is especially true as once a breach has occurred there is often an increased risk of future attacks as attackers may see the company as an easy target.

Overall, a data breach on a work mobile device can have serious consequences for both the individual and the company. It is important to take proactive measures to prevent data breaches, which we will list out in further detail later in this document.

5. Risk Assessment

Before deploying mobile devices, organisations should perform a risk assessment by identifying the threats and vulnerabilities associated with the range of mobile devices within the organisation.

This guidance document describes a 3-phase systematic and repeatable process to help organisation quantify the risks and apply appropriate security controls to mitigate those risks.



5.1. **Phase 1** – Identify devices and their criticality (what is important and why)

(CSBS 2.8 Digital Resources – End point Devices)

In this phase the organisation needs to ensure that there is an asset list/record of all mobile devices and their criticality. The following list is an example of the types of criteria that an organisation could use to compile the mobile devices asset list and determine their criticality. Devices with higher criticality levels will require a higher level of controls.

- **Identify Type of Device** (iPhone 13 128GB, Samsung Galaxy S23 Ultra 256GB etc.
- **Record device owner** (For a company device, the owner is the company)
- **Who are these devices assigned to** (Staff ID, name.)

- **Assign Device Criticality** (e.g., High, Medium, Low) calculated from:
    - Staff member grade (this will typically determine the nature of information the user has access to such as organisation strategy etc)
    - Staff member role (what does the staff member do and who depends on the staff member – e.g., ICT support, admin, engineering operations, etc)
    - Applications/data the user has access to (financial, HR, etc)
    - Is staff member a 'privileged user' (a privileged user has access to admin level functions and can typically override system controls)
    - Staff member travel patterns (does staff member travel to locations which could be considered hostile or adversarial)

Example:

IMEI	Make	Owner	Assigned to	Risk	Model
490154203237518	**iPhone 13 128GB**	Dept. Of ...	Joe Bloggs	Medium	COPE
490154327929272	**Samsung S22**	Jane Bloggs	Jane Bloggs	Low	BYOD

5.2. **Phase 2** - Identify the Threats and Vulnerabilities (what are the risks facing the devices)

(CSBS 1.3 Identify and Manage ICT Security Risks, 2.10 Secure Web and Infrastructure Configuration)

As both the organisations themselves and the threat landscape in which they operate are in constant flux, organisations need to remain vigilant to ensure their controls remain up to date.

Threats

(CSBS 1.3 Identify and Manage ICT Security Risks)

The following is a non-exhaustive list of threats for mobile devices which organisations should consider, along with the risks described in the threat landscape section.

- Device loss
- Unauthorised local access
- Device compromise via malware
- Network Compromise (call/message interception)
- ***Technical Threats***
    - *Data leakage*
        - user geo-location (GPS, nearby Wi-Fi, mobile network code etc)
        - device specific (IMEI - identifies phone, installed apps, OS, and hardware info etc)
        - user profile (IMSI – identifies SIM, app usage etc)
        - social relationship (SMS history, call history etc)
    - *Poor quality security*
        - Poor quality software development practices leading to vulnerabilities in the code.
        - Misconfiguration of services leading to data leakage or system vulnerabilities
        - Poor quality access controls leading to data leakage, inappropriate data access.
        - Poor control over its own supply chain
- ***Non-Technical threats***
        - *Spying/Espionage:* Concerns of spying/espionage arise when the ownership of the vendor has strong links to a given third country.
        - *Influence Operations:* Concerns of undue influence over users arise when a third country, through strong links with a vendor, could control recommendation algorithms. Note this would not need to be Foreign Information Manipulation Interference (FIMI), but rather could include recommending content which favours a particular ideology or against an individual.
        - *Ethical concerns:* Ethical concerns may arise which could impact an organisations reputation when the technology it deploys has links

to third countries which use the technology to suppress or abuse human rights.

Vulnerabilities

(CSBS 2.3.5 Digital Resources – ICT Digital Resources)

Organisations can identify vulnerabilities in a variety of ways. Not all vulnerabilities are equal, and an organisation should have a systematic vulnerability management process to prioritise the remediation of vulnerabilities based on the severity of the vulnerability and the criticality of the asset. The following non exhaustive list describes some ways an organisation can gather vulnerability information.

- Self-Discovery, e.g., through automated or manual scanning
- CVE (Common vulnerabilities and exposures) lists
- Vendor /Manufacturer reporting
- 3rd Party security reporting,
- Threat Intelligence feeds
- CISA Known Exploited Vulnerabilities list
- NCSC Advisories/Alerts

5.3. **Phase 3** – Risk Management (How should risks be addressed)

(CSBS 1.3.1 Identify and Manage ICT Security Risks)

Implement strong and clear governance that cascades from the top downwards and bottom upwards to ensure that risks are identified and managed according to the organisations risk appetite.

Risk management is used to shape and control risk but cannot eliminate all risk.

Risk Decisions

- *Risk Remediate/Mitigate (controls)* - actions taken to reduce the risks potential for harm to an acceptable level.
    - Implement and monitor appropriate and proportional controls as per organisations cyber security framework, policy, and standards, such as

Mobile Device Management (MDM), Joiners Movers and Leavers (JML) process, Privileged User Management (PUM) processes etc.

- *Risk Avoidance* – remove the exposure to the risk, for example by disallowing an application or device.
- *Risk transfer* – shift some of the risk to another entity, for example financial loss may be covered by cyber insurance.
- *Risk acceptance* – a decision not to take action regarding a particular risk. Decisions regarding risk acceptance need to be clearly documented and approved by the service owners.

6. Sourcing & Configuring Devices

The NCSC Guidelines on Cyber Security Specifications (ICT Procurement Criteria for Public Service Bodies) report[1] provides detailed advice on the cyber security requirements through all phases of procurement and is relevant for the procurement of mobile devices.

NCSC advises that organisations should only purchase mobile devices from reputable vendors, with a good track record in terms of cybersecurity and vulnerability remediation.

The following should be considered during the procurement of devices:

- **Decide which devices are going to be used:** Consider the business use for the devices, your security requirements and relevant security features available.
- **Look for manufacturers who have good supply chain security:** Ensuring that device manufacturers have extensive supply chain security policies in place will mitigate against the risk of device compromise at source and through firmware updates.
- **Decide which supplier(s) will be used to buy the devices:** The above factors relating to device functionality and manufacturer supply chain security, should form part of the PSB procurement process.

6.1.Considerations when choosing devices.

(CSBS 2.3.4 Digital Resources – ICT Digital Resources, 2.14 Security by Design)

When choosing mobile phones for use by your organisation, there will be many factors to consider. Organisations will often base their decision on price, functionality, and portability. These are important considerations, but once you have a shortlist of devices ready, some further thought should be given to the security of the devices, and the systems they run.

Operating System Considerations

The two main operating systems to consider are Google's Android and Apple's iOS.

Android

[1] Not yet published.

Android devices include a wide range of smartphones from various Manufacturers.

The Android Enterprise Recommended (AER) programme contains devices that have been subjected to more rigorous testing and security requirements than non-recommended devices. These additional requirements include minimum software versions, hardware performance, MDM capabilities and delivery of Android security updates within 90 days of release from Google for a minimum of three years. Some manufacturers release one or more future versions of Android on their devices. You should consider these manufacturers if you want to ensure access to future major releases of the platform. Hardware-backed keystores significantly strengthen the encryption features of an Android device and should be selected when available.

Before choosing a manufacturer to supply your devices, you should inquire about their security reputation, such as their response to vulnerabilities in the past and what apps including app permissions, they pre-install on their devices. You should consider how long the device will be supported by the manufacturer. This way you will receive security updates and bug fixes.

Google Play Protect checks apps and devices for harmful behaviour. It checks devices for potentially harmful apps/malware from other sources. It may deactivate or remove harmful apps from the device. It issues privacy alerts about apps that can get user permissions to access a user's personal information, violating their Developer Policy. It may reset app permissions to protect a user's privacy on certain Android versions. NCSC recommends you choose devices carrying the Google Play Protect certification.

Several OEMs also include additional features. For example, Samsung's Knox Platform for Enterprise features security enhancements over the standard build of Android. PSBs should evaluate the relative security of each OEMs offering before contracting.

iOS Devices

iOS is the operating system which powers the iPhone. IOS devices typically receive software updates for around 5 years after first release. Recent iOS devices have secure hardware features such as Boot ROM, which forms a hardware root of trust for secure boot, dedicated AES engines for efficient and secure encryption and decryption, and a Secure Enclave which is a system on chip (SoC) which provides the foundation for the secure generation and storage of the keys necessary for encrypting data at rest, and it protects and evaluates the biometric data for Face ID and Touch ID. Secure boot begins in hardware and builds a chain of trust through software, where each step is designed

to ensure that the next is functioning properly before handing over control. The secure boot chain, system security and app security capabilities all help to verify that only trusted code and apps run on a device. Apple provides layers of protection to help ensure that apps are free of known malware and haven't been tampered with. Additional protections enforce that access from apps to user data is mediated. These security controls typically provide a stable, secure platform for apps.

Resources from manufacturers:

Android: Android Security | Android Open-Source Project

iOS: Apple Platform Security – Apple Support (UK)

6.2. Devices images and standardisation

If possible, all devices issued to end users with the same role should have a near identical initial setup. With large organisations it is highly recommended to use MDM software to manage this. Listed below are some ways MDM software can assist you and your IT team in not only the setup of new devices but also the upkeep of existing hardware assets and even decommission of retired, lost or stolen mobile devices.

- **Imaging:** A standard process of wiping and then imaging a mobile device as it enters use as well as when it returns from service and is being prepared for a new end user is best practice. Most MDM software will allow you to do this. As standard a device purchased from a supplier already comes pre-configured with some apps as well as bloatware and adware. Wiping the device and loading in a pre-approved image of only designated work applications is the best way of ensuring the devices safety from the beginning.
- **Device and software testing:** It is advised where applicable, to deploy and test procedures for enrolling new devices into your MDM infrastructure. The same advice is also applicable to any configuration change or addition of new software to your standardised image.
- **Zero-touch enrolment for devices:** This relates primarily to organisations with large numbers of devices as it reduces the administration time of enrolling devices manually and ensures security of devices in transit to users. Zero-touch can do things such as push out a security or OS update and even install a new piece of software to all devices remotely regardless of location. Finally, Zero-touch can even remotely wipe a device or section of it. This may be necessary

if that device is retired or potentially compromised. This helps ensure data and device security.

It is important to provide user guidance which informs users how to complete enrolment on their new devices. This should include what to expect from the enrolment process, including screenshots and when and where to enter their corporate credentials as well as a warning about the dangers of trying to circumvent any of the restrictions put in place on the device.

6.3. Deployment Model

The following are the most commonly used terms when describing Mobile Device deployment models:

- **BYOD** (Bring Your Own Device).
- **CYOD** (Choose Your Own Device).
- **COPE** (Company Owned/Personally Enabled); and
- **COBO** (Company Owned/Business Only.)

PSBs need to be aware that with mobile devices accessing company systems and data, an increase in IT systems integration and access has to be balanced with a reduction in the risk created by having unmanaged mobile devices connect to your network. **For this reason, it is generally unadvisable to have BYOD as part of a PSBs company device management setup and policies as BYOD generally gives more user freedom.** However, where the nature of a PSB entails the need for some user groups to have BYOD access to company systems and data, ensure that appropriate controls are put in place to protect this data and ensure appropriate levels of security are maintained on the device through enrolment in some level of MDM (more on MDM is covered in section 7 of this document). For example, company apps won't work on BYOD devices without some minimal MDM type policies in place such as device lock being enabled, sufficiently complex password/biometrics etc. It is advisable to have a policy and process agreed by the user, in relation to the removal of corporate data from a personal device which may entail wiping of the device. This should also apply to a personal device that is lost or stolen.

COPE programs recognise that a lot of users will not want to carry two smartphones with them. Organisations provide smartphones primarily for work use, but basic functions such as voice calls, messaging and personal applications are allowed, with some controls on usage and flexibility.

COPE is weighted towards the PSB's needs for applications, integration and security, and the end user is allowed to use the device for non-business functions as well. Where a PSB opts for a COPE setup it is strongly recommended that they use containerisation tools, such as the Work Profile and partitioning (covered in the section 8.5 of this document) to maintain a security separation between personal and work data and applications.

COBO prohibiting the personal use of a mobile device. With a COBO approach PSBs can take a strict approach to which software an application can run on the device. COBO provides the most control to ICT and Security staff to ensure that the PSBs IT network is protected from threats, however, may inconvenience staff who are required to carry two devices and may not use their work device for personal purposes. It should be noted that COBO can also assist in terms of staff wellness and implementing 'right to disconnect' policies.

It is up to each PSB to assess the level of security they feel is needed versus the accessibility and availability for the end user. The risk assessment that PSBs carry out as part of Section 5 of this document will inform what approach is needed for which type of users. In general, it is best to adopt a COBO approach for the most sensitive users.

7. Mobile Device Management (MDM)

7.1.Know what you have.

(CSBS 2.3 Digital Resources – ICT Digital Resources, 2.8 Digital Resources – End Point Devices)

Asset management helps keep track of hardware assets and warranties, so you do not waste money replacing products at full cost. From a mobile device point of view ICT managers should be ensuring that all of an organisation's mobile device assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes.

Asset management is essential for security management, but it also saves money by helping avoid unnecessary purchases not only with mobile device hardware but the licensing and support costs that goes with the software being used on those devices. Keeping track of software and subscriptions ensures you do not keep paying for something that you stopped using years ago or that you do keep paying maintenance on support contracts for essential systems.

Note: An MDM solution is recommended for corporate devices and aids in asset management. This process is made easier with software which can help you keep track of sensitive systems an individual user has on their mobile device as well as the device itself.

Knowing what you have means if anything were to happen, you are not left with a situation where you have critical systems down and no one with the expertise to help you resolve the situation. If your staff need to work on a mobile device even if it is just to run the authentication for your VPN or checking email when travelling, having those systems go down because no one was keeping track of their renewal could cause major disruption.

7.2. Joiners Movers Leavers (JML) & MDM

(CSBS 1.9 Joiners, Movers, Leavers Policy, 2.11.5 User Account Protection)

Asset Management is not only important for keeping track of lost, stolen, or retired devices, it is also ensuring that a device is returned once a staff member leaves or even changes role to another role where that device is no longer needed. Increasingly today's workforce do not see their current position as their position for life and often end up as part of the company for two years or less.

MDM can also help with this. You do not want staff to leave and keep company property forcing you to buy more hardware for that staff members replacement or keep allowing that staff leaver to access to critical systems or information when they are no longer a part of the company.

An MDM system in conjunction with a leavers policy can not only assist with keeping track of all your mobile devices but also prevent you from keeping on paying for software licencing unnecessarily that are still running on those or even retired devices if a staff member is issued with a replacement or upgrade. In some cases, with asset management disabling the software will also allow you to remotely wipe any company data associated with that software.

MDM may assist with compliance with security and legal policies. It is important however to have one centralised system where all your assets are tracked together, rather than each manager looking after their own teams' assets all on different systems as this led to inconsistencies and gaps. For more information on how a JML process see section later in this document or *CSBS 1.9.1 Joiners, Movers, Leavers Policy*.

7.3.Cost Savings

While an MDM system may cost money and require staff time to initially set up, doing so can bring efficiencies over time depending on the workforce and amount of assets you have. Once set up a good MDM system should be easy to use, and its update and maintenance should seamlessly fit into existing ICT policies and procedures.

If you have a small amount of assets to keep track of, a simple Excel spreadsheet may be enough just to list who has what and for what purpose, not only for hardware but software as well. If you have a large amount of assets to keep track of then a mobile device management software could help you track and automate a lot of your set up and upkeep.

Some MDM software allows you to auto enrol any mobile device that signs into your company email and the user is not allowed to use the company software or email until they go through this enrolment process thus registering it on the software and automatically updating that the user who signed into that email is the one that owns the device they signed in on. This reduces the time needed by ICT or management to maintain your list of assets.

7.4.Device provisioning, logging, and monitoring

(CSBS 2.7 Digital Resources – Logging/Auditing)

It is important that PSBs have an ability to monitor the activity of mobile devices when they are interacting with the IT network. Collecting appropriate logs will also assist during any forensic investigations after an incident has occurred. It can also assist in the case a device has been lost or stolen to understand what data the device has been in contact with.

With more advanced MDM software it can also allow you to remotely wipe or remove access to those devices, this helps contain any potential loss of company data or breach. As mentioned in cost saving section above, MDM software can be used to automatically update who owns what device, but they can also do much more and as much or little as you want or feel comfortable controlling.

Some MDM software allows you to auto enrol the device sending back key information such as make, model and OS version. In addition, MDM can also block the installation of certain apps including gambling or social media related apps if these are not deemed appropriate to have on a corporate device. Similarly, you can restrict internet usage to only websites that are deemed useful to the user's role. It is even possible to block the sending or receiving of information deemed confidential on mobile devices.

You can also set the MDM software to alert you to suspicious activity such as incorrect password attempts or beaches of policy. It is up to each organisation to make their own decisions on what measures they feel are necessary to protect the company data available on a mobile device and it may be the case that the same rules do not apply to each user as some may be handling more sensitive data than others.

Many of the features mentioned will vary across MDM products and consideration should be given to your specific requirements when choosing a solution.

7.5.Where to start

While it is highly recommended that MDM software is used to track and monitor all mobile devices, as well as enforce standardised protection measures, this approach is not always practical for PSBs.

As a basic measure all PSBs should have a written policy agreement that staff must agree to in order to gain access to a company mobile device or access company data on their own device. Manual tracking of assets within a central location and policies for managers or IT staff is necessary to ensure this method is always up to date.

MDM software is the preferred option as it gives IT and the company more control. MDM software works in conjunction with any work-related apps. It can allow you to

set certain compliance rules for staff to be to be able to access any company data. Failure to agree to those rules and compliance practices will force the software to cut off access to all work-related apps and documentation. This document lists some of the policies in the previous section you can implement with MDM software, but this is covered in more detail in the Security Measures Section.

8. Security Measures

8.1. Basic Protection Measures

(CSBS 2.2 Identification and Authentication)

All mobile devices should be secured with a strong password or PIN (any PINs used should be a minimum of six digits.). This ensures that, were the device to fall into the wrong hands, the data contained could not be immediately accessed. This method however is not 100% safe as some attackers can access the data even if it is behind a pin code.

An attacker may have gained access to the staff members passcode through social engineering or shoulder surfing or even by removing the hard dive on the device and accessing the raw data. It is always best practice to either have a policy or your MDM software set to enforce the use of biometrics, meaning a fingerprint, facial scan or similar authentication is needed to unlock the phone.

Most modern phones have the ability to scan for biometrics already built into them. The device should also auto lock and the password or biometrics be required again after several minutes of inactivity. If such a device is lost or stolen steps should be taken immediately to ensure the appropriate staff are notified as soon as possible, as the loss or theft of a Departmental phone should be considered a data breach as it holds company information.

8.2. Multi Factor Authentication (MFA) on the device.

(CSBS 2.12 Multi-Factor Authentication)

MFA or two-factor authentication (2FA) or two step verification, is an extra layer of security for online services asking users for another piece of evidence in addition to their password. It is recommended that MFA is enforced for users accessing PSB resources from their mobile device and the implementation of MFA needs to balance security with usability by the end user in carrying out their work.

The key benefit of MFA is the need for a matching pair, rather than the inherent strength of the second or multiple “factors”. It involves using your username and password and one other piece of information. This other piece of information can come in various forms. Often broken down into ***“something you have, something you know, and something you are.”*** :

- ***"Something you have"***- A **one-time dynamically issued token** either through an app on the user's phone or another device other than the one they are trying to sign into or a physical object in the possession of the user such as a key fob with a rotating token linked to the user's account, or a digital certificate issued to the user's device.

- ***"Something you know"*** -An **additional piece of information that is only known to the user**, such as their username and password.

- ***"Something you are***"-A **physical characteristic of the user (biometrics)** such as a fingerprint scan or facial recognition.

For this to work properly it is recommended that the user be forced to check in once every 24 hours. MFA stops an unauthorised user from gaining access to company data on a mobile device. If the device were to become lost or stolen, then this gives an unauthorised user only a short window to bypass any other protection measure such as the password.

8.3. Digital Certificates

An additional policy PSBs should consider implementing is to install appropriate certificates on the end user's mobile device.

A device certificate is a unique identifier used to authenticate phones and other devices. Digital Certificates on mobile devices can allow employees to encrypt and digitally sign email communications sent from devices, ensuring privacy of sensitive information, proof of message origin and mitigation against phishing attacks.

Digital Certificates can also be used to make access to Wi-Fi and VPN connections more secure as they require the device to have the cert installed and correctly configured in order to be able to access your enterprise connections.

8.4. Storing Passwords

Where possible, the end user must not store corporate passwords in cloud-based services or locally on mobile devices. These services can be compromised, and corporate credentials can be stolen. A password management tool is the recommended approach to storing passwords securely and making them readily available as required.

8.5. Single Sign On (SSO)

SSO simplifies identity management internally within an enterprise and with trusted external partners by reducing the need for users to maintain multiple identities in both internal and external directories, applications, and other platforms, eliminating the need for local identities at each asset. It allows for seamless working without compromising on security. Additionally, it reduces the labour costs associated with managing multiple identities for each user on the various on-premises and/or cloud-based applications.

Passwords are a vulnerability due to the complexity of requiring a user to remember multicharacter passwords that almost every application requires today. SSO reduces the user burden by only asking them to remember one solid, complex, and hard-to-guess passphrase, and facilitates the migration to strong MFA, potentially eliminating passwords altogether.

8.6. Partitioning: Personal and Business

Another means to secure corporate data on mobile devices is through the use of an MDM solution to create “Work Profiles” or “Containerisation”, that provision an encrypted container on the device for the use of specific applications and data. This results in a separation on the device between the work side and a personal side, allowing for a dual-use device. This solution will allow full control over the Work Profile and can be used in both BYOD and COPE configurations. In the case of BYOD, the organisation can only see data and control settings within the Work Profile and cannot interact with the non-Work Profile side. For the COPE configuration an organisation has additional controls over the non-Work Profile side to control settings, features and restrictions.

Through the use of an MDM solution, configurations can be applied to ensure separation is maintained between the two profiles. Functions such as copy/paste should be limited to within the work or personal profile but never transcend from one to another. Similarly, a screen grab may be taken within a profile but should be restricted to use only within the respective profile. The Side loading of apps from third party or unauthorised app stores can and should be restricted (more on MDM is covered in section 7 of this document).

Features such as the ability to remote wipe the Work Profile the next time a device is powered on and has access to the internet to receive the remote command adds additional security around the JML process as well as securing the device if it is lost or stolen.

Another solution to securing corporate data on a mobile device, is through the use of secure folders. This creates an encrypted container that can be used to store corporate data including files and apps. Apps configured within this folder are only accessible on authentication and are completely separated from apps and storage in the personal area. A risk analysis of this approach should be taken as it may not always be possible to limit Apps installed into this folder, files could be moved out of the secure folder and the clipboard (copy/paste) could be enabled.

It should be noted that the advice above is generic in nature and there are notable differences between iOS and Android implementations that need to be considered when choosing a solution.

In both these scenarios, consideration should be given to App activity in the non-Work Profile partition as there are still potential risks relating to App permissions that may include the ability to monitor voice calls, and a social media App could still be used to monitor the location and profile the preferences and interests of the user.

Please see "Section 9 – Vetting of third-party application or software" for more detailed information.

8.7. Social Media Usage on mobile devices

(CSBS 2.8 Digital Resources – End point Devices , 2.12 Multi-Factor Authentication (MFA))

A Social Media Usage Policy to guide staff when using social media on mobile devices in a private capacity when at work is strongly advisable for PSBs. The aim of the policy is to protect staff, the reputation of the organisation, and the security and integrity of their computer networks. This includes the appropriate use of any approved social media for official business. Any social media usage policies should be easily accessible by all permanent and contract staff. An effective policy should warn that devices only be used to access appropriate content and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity.

If a PSB chooses to issue staff with an organisation-owned mobile device to access their organisation's systems or data, they should be satisfied that it does not present an unacceptable security risk.

Strong login passwords/PINs should be used for the device while undertaking any social media use for business purposes. Any PINs used should be a minimum of six

digits. However, it is strongly advised to use biometric authentication (face or fingerprint).

It is also strongly recommended to use MFA where available and where appropriate and technically possible. PSBs should ensure that MFA is necessary for access to corporate social media accounts. Corporate social media accounts are the public face of PSBs, and MFA will block brute force password attacks and prevent against misuse if the password is inadvertently disclosed in public.

8.8. Privileged Access Management

(CSBS 1.8 Access Control Procedures, 1.9 Joiner, Movers, Leavers Policy, 2.1 Access Control and Responsibility)

If a PSB chooses to issue staff with an organisation-owned mobile device to access their organisation's systems or data, they should be satisfied that it does not present an unacceptable security risk.

PSB's are **strongly advised** that systems should not be administered with privileged access through mobile devices. Access permissions and authorisations should be managed, incorporating the principles of least privilege and separation of duties, and periodically revalidated.

Under the principle of Least Privilege, PSB's should ensure that individuals should be given the bare minimum access needed on a mobile device to perform their job functions and no more. Under the principle of separation of duties, PSB's also need to ensure that no user should have all the privileges necessary on the mobile device to complete a critical business function.

The principles of Least Privilege and Separation of Duties should be applied to privileged access through a mobile device. To achieve this, privileged users should only be granted specific privileged accounts and associated permissions which PSBs consider are essential to their business role or function.

Administrators for PSB's should not be able to grant themselves privileged access to the network through the mobile device. Privileged user access rights should be regularly reviewed by PSBs and updated (including updating privileged user rights as part of the joiners, movers, and leaver's (JML) process).

It is strongly advisable that any privileged access should be via accounts secured with MFA. The second factor should be locally generated, and not be transmitted (i.e not SMS). Soft tokens (e.g., authenticator apps) can be used for this purpose.

8.9. Use of External Networks

(CSBS 1.8 Access Control Procedures, 1.9 Joiners, Movers, Leavers Policy, 2.1 Access Control and Responsibility)

Because mobile devices primarily use non-enterprise networks for internet access, PSB's typically will have no control over the security of the external communications networks the devices access.

Communications media may include wireless systems such as Bluetooth, Wi-Fi, and cellular networks. Bluetooth devices often are used to transmit audio information (e.g., voice traffic, music) as well as notifications and health information from wearable devices . Wi-Fi and cellular can be used to transmit multiple types of traffic, including voice and data. All these network protocols and media are susceptible to eavesdropping and man-in-the-middle (MitM) attacks that can intercept and modify communications between a device and an enterprise system. PSBs should base its mobile device security on the assumption that external networks between its mobile devices and its enterprise system, such as internet service provider(s) and cellular networks, cannot be trusted. PSB's should ensure that VPNs are utilised in order to reduce the risk from untrusted networks and protect the confidentiality and integrity of communications. Additionally, the use of mutual authentication mechanisms should be considered in order to verify the identities of both endpoints before transmitting data. Another possible mitigation to consider is to prohibit use of unsecured Wi-Fi networks, such as those running known vulnerable protocols.

8.10. Joiner, Movers, Leavers Process

(CSBS 1.9.1 Joiners, Movers, Leavers Policy)

It is advisable that PSB's ensure that any organisational processes are linked with the Human Resources (HR) part of the organisation. For example, staff may have a higher level of access than required or maintain their access to critical systems or sensitive data after they have moved positions or left the organisation entirely. It may also result in staff not receiving key induction or follow-up training, or not understanding their obligations while they were with the organisation or after they have left.

An appropriate Joiner, Movers, Leavers Policy (JML) should be in place. The PSB should ensure that the policy is defined, approved by management, published, and communicated to employees and relevant external parties. It should include details for revoking access when it is no longer required or changed for movers. Implementation of the policy demonstrates control of ICT assets and consequently aides with cyber security and financial due diligence.

PSBs should ensure that the Joiners process sets out that staff have the appropriate equipment and technology available to conduct their work in a secure manner. Similarly, mobile devices and credentials should be issued as part of the joiners' process.

When staff change roles, or take on new responsibilities, a specific Movers' process should be in operation, which provides them with any new security authorisations and access, and revokes previous credentials, security clearance and access.

Finally, as part of the Leaver's process, staff should have all security authorisations, clearances and associated accesses revoked. All PSB owned equipment, including mobile devices should be reclaimed, and credentials such as ID cards and badges returned.

The JML process, particularly when it comes to security authorisations and access to information systems, should be linked with HR processes and automated wherever possible. The JML process should also be subject to monitoring and audit to ensure that they are fit for purpose, reflect best practice and that the policies are being adhered to.

8.11. Keeping Devices Up to Date

(CSBS 2.3 Digital Resources – ICT Digital Resources, 2.8 Digital Resources – End point Devices)

Modern mobile devices run a huge amount of software including operating systems such as Android and iOS and the applications installed. To prevent known vulnerabilities from being exploited, all the following software must be kept up to date:

- **Operating System (OS):** Please ensure that automatic updates are enabled, but users will need to be vigilant that the updates are actually taking place, e.g., some automatic updates may not commence until the device has been manually

restarted, so if this has not been done over time, it will leave the device vulnerable.

- **Web browser** and extensions
- **Third-party apps - especially office apps**: While some apps will update themselves through the mobile device's app store, mobile device users will need be made aware that they need to update others themselves.
- **Antivirus:** If an antivirus solution is deployed on mobile devices it will need to be updated for bug fixes, new features, and new virus signatures which can be used to detect new malware that's recently been detected by the Anti-Virus companies.

Monitoring tools should be used to ensure updates are being applied to Apps and devices. It may be necessary to have processes in place where major OS updates are tested in advance of pushing out to users.

Mobile devices, apps and operating systems will reach a point in their lifecycle where they are no longer supported, and PSB's will need to replace unsupported software and devices as soon as possible in this scenario. Responsibility for this should be assigned.

9. Vetting of third-party applications or software

(CSBS 2.3 Digital Resources – ICT Resources)

Bearing in mind the risk assessment process outlined in Section 5, from time to time, PSBs will have to make decisions on onboarding or the use of third-party applications or software on mobile devices.

Whilst allowing users to access and install a broad range of third-party applications brings certain advantages, there are also risks associated with certain applications.

Third-party applications will typically be able to read and/or modify some or all the user's data on that device, including your organisation's data where appropriate segregation is not in place.

Apps which have been poorly coded, or which do not receive security updates could contain vulnerabilities and be exploited by threat actors in order to gain access to or steal data from a device.

PSBs should have clear internal policy on the use of third-party applications, and where necessary use MDM or other methods to enforce policies.

9.1. Allow lists & Deny Lists

PSBs may take certain approaches such as allow-lists or deny-lists of certain applications in order to ensure that devices are secured from potentially malicious applications.

The more restrictive approach is to maintain and enforce an allow list of applications which have been assessed and explicitly allowed through an appropriate approval process. Whilst this strategy is highly effective in ensuring security, it involves an overhead in staffing requests for approval, and may cause inconvenience and friction with certain users. Depending on the risk assessment carried out in Section 4, this approach could be used for the most sensitive users with access to the most critical areas of the business, who may be required to use "Enterprise only" devices. Equally, where a Corporately Owned Personally Enabled (COPE) approach is used, and the enterprise part of the phone is adequately separated, allow-lists could be enforced on the enterprise segment of the phone.

A less restrictive, but easier to manage approach, is to maintain and enforce a deny-list of known malicious or high-risk applications. This approach provides more latitude for users to access and use a broad range of applications but runs the risk of failing to add unknown malicious applications to the deny-list. This approach could be used on the personally enabled segment of a phone, or on less sensitive users, depending on the outcome of the risk assessment outlined in section 4.

9.2. Assessing the Risk of Third-Party Applications and Software

In order to determine whether an application should be added to either an allow list or a deny list, PSBs should consider various factors, in assessing the security of the application.

9.2.1. Business Need

PSBs should determine whether the application is required for business use, which can form part of the determination as to whether the application is placed on an approve/deny list. Applications could be placed into the following categories:

Essential – Applications which are essential to the functioning of the organisation and are required by users to conduct their day-to-day business activities. Examples of applications that may fall into this category include email, video conferencing apps, certain messaging apps, authenticator apps, word processing apps, pdf viewers, pre-installed manufacturer apps like phone, calculator etc.

Some Business Use – Applications which have a business use but may not be essential for most users to conduct their day-to-day business activities. Examples of applications that may fall into his category include transport apps, weather apps, banking and payment apps, certain social networking apps relating to work, food delivery apps etc.

Limited Business Use – Applications which have limited or no business use and are most likely relating solely to personal activity. Examples of applications which fall into this category include gambling apps, gaming apps, social media apps unrelated to work, image modification and beauty apps etc.

9.2.2. Permissions

PSBs should consider the levels of permissions an app requires in order to run on the device, and whether it is appropriate to the purpose of the app. In general, applications should run with the lowest number of permissions possible. For example, there is no reason a gaming application should have access to phone books, messages, or call logs etc. There are a number of tools and providers that have extensive reports outlining the permissions and access that mobile device apps have.

9.2.3. Data & Privacy

PSBs should consider the amount of data the application will have access to, and what level of data the device sends to the application servers. PSBs should be aware of the stated privacy policies of the developer as well as independent testing by researchers or findings by Data Protection authorities.

Many applications, such as certain social media applications, send large amounts of data, including personal data, to application servers. In some cases, this data may be sent outside of the EU, where the same levels of data protection, in place under GDPR are not present. This should be a factor PSBs consider when deciding whether to add an application to an allow-list or deny-list.

9.2.4. Cybersecurity

Where possible PSBs should evaluate the reputation and cyber security practices of the applications developer in order to reduce the chances the app introduces vulnerabilities into a device. This may include examining the developer's history of known common vulnerabilities and exposures (CVE), their responsiveness to updating and patching the app, whether they operate a vulnerability disclosure policy, whether they have a history of cyber security incidents or serious concerns have been raised about the developer or the security of the app.

9.2.5. Non-Technical Factors

The PSB should, where possible, also examine whether the developer is likely to be subject to interference from a foreign country (“third country”), such as a through legal or extra-judicial requirements to provide data to or cooperate with the intelligence services or military of a third country.

Such interference may be facilitated by the presence of the following factors:

- whether or not a strong link exists between the developer and the government of any third country.
- the status of the rule of law and the political situation within the third country in question, whether there is democratic or legislative oversight, including an independent judiciary, in place, and whether data protection or security agreements exist between the European Union and the third country in question.
- the characteristics of the developer’s business ownership and practices, whether the ownership structure is transparent and whether the developer sources of finance are transparent.

- the ability of the third country in question to exert any form of pressure upon the developer, such as influencing the source code of the app, security updates or the content on the app.
- whether or not the third country, from which the developer originates, conducts, or is associated with an offensive cyber policy.

9.2.6. NCSC Advice

From time to time, on request of Government, the NCSC may assess the security of certain third-party applications and issue advice on same. PSBs should strongly consider this advice when making decisions on adding an application to an allow-list or deny-list.

The PSB may consider some or all of the previously outlined criteria e.g., it may be sufficient to just consider the app has limited/no business use or that the NCSC has issued a recommendation and take decision on that basis, without having to carry out a full assessment of each new application.

9.3. Exceptions

PSBs may need to allow exceptions to the decisions taken in relation to third party applications. For example, a PSB may decide to add a social media app to a deny-list for users, however, they may need to make exceptions for certain users such as their communications team, who may need to use the app to communicate with the public. PSBs should assess these exceptions on a case-by-case basis and take a risk-based approach. PSBs may implement solutions such as providing a separate device that does not have access to the enterprise network thus reducing the risk.

10. Further Reading

NCSC-IE Advisories/Alerts

https://www.ncsc.gov.ie/news

NCSC-UK Mobile Device Management

https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management

NIST SP 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

NIST SP 800-163R1: Vetting the Security of Mobile Applications

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf

NCSC-NL IT Security Guidelines for Mobile Apps

https://english.ncsc.nl/publications/publications/2019/juni/01/whitepaper-it-security-guidelines-for-mobile-apps

CVE (Common vulnerabilities and exposures) lists

https://cve.mitre.org/

CISA Known Exploited Vulnerabilities list

https://www.cisa.gov/known-exploited-vulnerabilities-catalog