# Security Standard – Mobile Device (SS-017)

Chief Security Office

**Date:** 22/05/2025

This Mobile Device Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

Government Publications Security Policies and Standards

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

(Important note for screen reader users.) Paragraphs that contain a **'must'** statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains 'must' activities.

Table 1 – Terms

| Term | Intention |
|---|---|
| must | denotes a requirement: a mandatory element. |
| should | should denotes a recommendation: an advisory element. |
| may | denotes approval. |
| might | denotes a possibility. |
| can | denotes both capability and possibility. |
| is/are | is/are denotes a description. |

# 1. Contents

## 2. Revision history

| Version | Author | Description | Date |
|---|---|---|---|
| 1.0 | | First published version | 04/07/2017 |
| 2.0 | | Full update in line with current best practices and standards;<br>• Updated Intro, purpose, audience, scope; added reference to CIS security controls<br>• Added NIST CSF references<br>11.1.4 – Update regarding walled garden approach<br>11.1.5 Requirement added regarding device lifecycle<br>11.1.6 Requirement added for blocking unauthorised data transfers<br>11.2.1 Added reference to NCSC Mobile Device Guidance<br>11.2.2 Amended passcode requirements<br>11.2.3 Updated timeout requirements<br>11.3.1 Requirement added for application vetting<br>11.3.5 Requirement added to prohibit jailbreaking and block jailbroken devices.<br>11.3.6 Requirement added for compromise detection<br>11.4.8 Requirement added for public Wi-Fi access points | 27/02/2023 |

| | | | |
|---|---|---|---|
| 2.1 | | All NIST references reviewed and updated to reflect NIST 2.0<br>All security measures reviewed in line with risk and threat assessments<br>Approval history - Review period changed to up to 2 years<br>Introduction – Added ref to BYOD<br>11.2.2 Password requirements<br>11.2.5 Login attempts, automatic locking<br>11.2.6 Device locking; Wi-Fi<br>11.2.9 Configured and managed; Ref added to Malware standard<br>11.2.10 Detected and reported<br>11.2.14 Approved device OS<br>11.2.15 Notification preview<br>11.3.3 Controlled by<br>11.4.1 Ref added to Remote Access Standard<br>11.4.2 VPN established before accessing corporate data or services<br>11.4.3 Enabled<br>11.4.5 Ref added to Remote Access Standard<br>11.5.5 Device and MDM patching<br>11.6.1 MDM system<br>Internal References – added BYOD standard | 22/05/2025 |

| | | | |
|---|---|---|---|
| | | Internal references – Added Access & Authentication; Remote Access; Malware Protection; BYOD; Security Patching | |

## 3. Approval history

| Version | Name | Role | Date |
|---|---|---|---|
| 1.0 | | Chief Security Officer | 04/07/2017 |
| 2.0 | | Chief Security Officer | 27/02/2023 |
| 2.1 | | Chief Security Officer | 22/05/2025 |

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

## 4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by 1st line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. D].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

## 5. Exceptions Process

(Important) this paragraph contains ‘must’ activities.

In this document the term **“must”** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

## 6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications.

## 7. Accessibility statement

(Important) this paragraph contains ‘must’ activities.

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

## 8. Introduction

(Important) this paragraph contains ‘must’ activities.

This Mobile Device Security Standard defines the minimum technical security measures that **must** be implemented for use within the Authority.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to mobile devices are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with mobile devices, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.

With the use of Mobile Device Management or other mobile security solutions, the collection and monitoring of user or employee data can impact an individual's personal privacy. Please refer to the DWP Acceptable Use Policy [Ref. D] for statements regarding personal use of Authority equipment.

With the introduction of Bring Your Own Device (BYOD), security requirements differ between corporately provided devices and users' personal devices. Please refer to SS-037 Bring Your Own Device (BYOD) Security Standard [Ref. G] for specific requirements.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the existing security posture in a number of important areas.

The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF), and are enabled by the implementation of controls from the CIS Critical Security Controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

## 9. Purpose

The purpose of this standard is to ensure that Authority systems and services are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

## 10. Scope.

This standard applies to all mobile device deployments within the Department and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data. For Bring Your Own Device (BYOD) deployments, please refer to SS-037 Bring Your Own Device (BYOD) Security Standard [Ref. G] for specific requirements.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

## 11. Minimum Technical Security Measures

(Important) this paragraph contains ‘must’ activities.

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

### 11.1. General Security Requirements

(Important) this table contains ‘must’ activities.

| Reference | Minimum Technical Security Measures | NIST ID |
|---|---|---|
| 11.1.1 | The mobile device **must** be owned, inventoried, configured and managed by the Authority or its approved supplier. | ID.AM-01 |
| 11.1.2 | The mobile device **must** be allocated to a named individual for their use only. | ID.AM-01 |
| 11.1.3 | Users **must** be provided with guidance on the secure use of mobile devices and remote working. | PR.AT-01 |
| 11.1.4 | Design principles for any Authority mobile device solution, **must** follow the NCSC walled garden pattern approach for supporting infrastructure, but not for individual mobile devices, unless a different approach is approved by the Authority. | PR.DS-01<br>PR.DS-02 |
| 11.1.5 | Device lifecycle **must** be managed considering overall device health e.g. battery life. | ID.AM-08 |
| 11.1.6 | The Mobile Device Management (MDM) system **must** block any data transfer from unauthorised devices, including chargers. | PR.DS-02 |

### 11.2. Mobile Device Security Configurations

(Important) this table contains ‘must’ activities.

| Reference | Minimum Technical Security Measures | NIST ID |
|---|---|---|
| 11.2.1 | All mobile devices **must** be configured in accordance with the relevant NCSC Mobile Device Guidance [see External References]. | PR.DS-01<br>PR.DS-02<br>PR.DS-10 |
| 11.2.2 | A user **must** authenticate to the device using a passcode containing the minimum of eight characters, with at least two special characters. Alternatively, biometric login can also be used. It’s important to note that this security measure deviates from SS-001 Access & Authentication [Ref. H] and NCSC guidance, to reflect the higher likelihood of loss or theft of mobile devices. | PR.AA-03 |
| 11.2.3 | The device **must** automatically lock after no more than 5 minutes of inactivity (15 minutes for tablet devices). Remote locking via the Mobile Device Management (MDM) system **must** also be enabled. | PR.DS-01 |
| 11.2.4 | All usable storage on the device **must** be encrypted in line with SS-007 Use of Cryptography Security Standard [Ref. B]. | PR.DS-01 |
| 11.2.5 | The device **must** lock automatically after a maximum of ten failed login attempts. | PR.DS-01 |
| 11.2.6 | The data contained on the device **must** be able to be remotely wiped and the device locked via the MDM system, whilst connected to a mobile network or Wi-Fi, if the device is lost or stolen. | PR.DS-01 |

| | | |
|---|---|---|
| 11.2.7 | Devices **must** not be able to synchronise to non-Authority devices. | PR.DS-01 |
| 11.2.8 | Devices **must** only back-up data to Authority approved storage locations. | PR.DS-01 |
| 11.2.9 | Anti-malware **must** be installed on all mobile devices, configured and managed in line with SS-015 Malware Protection Security Standard [Ref. E]. | PR.DS-01<br>DE.CM-09 |
| 11.2.10 | A user **must** not be able to modify the boot process of a device and, any attempt **must** be detected and reported via the MDM service. | PR.AA-05 |
| 11.2.11 | A user **must** not be able to modify or disable security safeguards. | PR.AA-05 |
| 11.2.12 | Devices **must** be erased and all data removed before the device is re-issued to a new user. | PR.DS-01 |
| 11.2.13 | At the end of life, the devices **must** be sanitised securely in accordance with the manufacturer's guidelines and SS-036 Secure Sanitisation & Destruction Security Standard [Ref. A]. | PR.DS-01<br>ID.AM-08 |
| 11.2.14 | All mobile devices **must** be running an Authority approved version of the operating system, enforced by the MDM system. | ID.AM-08<br>PR.PS-02<br>PR.PS-03 |
| 11.2.15 | Mobile devices **must** be configured so that notification previews cannot be viewed without user authentication. | PR.DS-01<br>PR.DS-02 |

### 11.3. Mobile Application Security Requirements

(Important) this table contains ‘must’ activities.

| Reference | Minimum Technical Security Measures | NIST ID |
|---|---|---|
| 11.3.1 | All applications installed on Authority devices **must** be risked assessed and approved. Application vetting tools or services to identify insecure storage of sensitive data **must** be implemented. | ID.RA-09 |
| 11.3.2 | All Applications **must** be digitally signed to ensure that only applications from trusted entities are installed on the device and that code has not been modified | ID.RA-09 |
| 11.3.3 | Access to App Stores **must** be controlled by the Authority MDM settings. | PR.AA-05 |
| 11.3.4 | There **must** be a mechanism to install, update and remove all applications and to safeguard the mechanisms used to perform these actions. | ID.AM-08<br>PR.PS-02 |
| 11.3.5 | MDM policies **must** prohibit ‘jailbreaking’ or ‘rooting’ of the device, and the ‘side-loading’ of apps. If a jailbroken device is detected, the Authority MDM service **must** block it. | PR.PS-01<br>PR.PS-05<br>DE.CM-09 |
| 11.3.6 | Compromise detection **must** be implemented for mobile devices and prevent the installation of apps from unauthorised sources. | PR.PS-05<br>DE.CM-09 |

### 11.4. Mobile Device Connectivity Security Requirements

(Important) this table contains 'must' activities.

| Reference | Minimum Technical Security Measures | NIST ID |
|---|---|---|
| 11.4.1 | All traffic to and from the mobile device **must** be routed over an Authority approved VPN tunnel, in line with SS-016 Remote Access Security Standard [Ref. I]. | PR.DS-02 |
| 11.4.2 | The VPN between the source endpoint device and the enterprise gateway **must** be established using full end to end tunnelling using an Authority approved encryption algorithm. This **must** be established before allowing access to any corporate services or data. | PR.DS-02 |
| 11.4.3 | Devices **must** be configured so that the USB interface is only enabled for charging. | PR.DS-02 |
| 11.4.4 | Devices **must** not be able to transfer Authority data to any other device, unless it is via an Authority approved method. All data transfer protocols **must** be disabled by default. | PR.DS-02 |
| 11.4.5 | Devices **must** not be able to connect to wireless networks requiring login via a landing page, in line with SS-016 Remote Access Security Standard [Ref. I]. | PR.DS-02 |
| 11.4.6 | Only authenticated Devices **must** be allowed access to the Authority's enterprise services. | PR.AA-03<br>PR.AA-05 |
| 11.4.7 | Wi-Fi connections security **must** be in line with SS-019 Wireless Network Security Standard [Ref. C]. | PR.DS-02 |

| | | |
|---|---|---|
| 11.4.8 | Mobile Device connections **must** be configured to not auto-connect to public Wi-Fi access points, and to refuse connection from known compromised Wi-Fi access points. | PR.DS-02 |

### 11.5. Mobile Device Management Security Requirements

(Important) this table contains 'must' activities.

| Reference | Minimum Technical Security Measures | NIST ID |
|---|---|---|
| 11.5.1 | All Authority mobile devices **must** be centrally managed using MDM (Mobile Device Management). | ID.AM-01<br>ID.AM-08 |
| 11.5.2 | Access to enterprise resources **must** be restricted, based on the mobile devices and user access rights. | PR.AA-01<br>PR.AA-05 |
| 11.5.3 | The central MDM system **must** automatically monitor, detect, and report when policy violations occur, such as changes from the approved security configuration baseline, and automatically take action where required. | DE.CM-03<br>DE.CM-09 |
| 11.5.4 | Devices **must** be enrolled on the central MDM system prior to being issued, unless, after a risk assessment, it is not deemed to be a requirement. | ID.AM-01<br>ID.AM-08 |
| 11.5.5 | The device OS and the MDM system software **must** be patched up to date in line with SS-033 Security Patching Standard [Ref. F]. | ID.AM-08<br>PR.PS-02 |

### 11.6. Monitoring and Logging

(Important) this table contains ‘must’ activities.

| Reference | Minimum Technical Security Measures | NIST ID |
|---|---|---|
| 11.6.1 | The MDM system **must** enable logging to its maximum required capability, without impacting performance. | PR.PS-04<br>DE.CM-09 |
| 11.6.2 | Logging of appropriate security related events for each mobile device **must** be enabled by default, where available. | PR.PS-04<br>DE.CM-09 |

## 12. Appendices

### Appendix A - Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 2 – List of Security Outcomes Mapping

| Ref | Security Outcome (sub-category) | Related security measures |
|---|---|---|
| ID.AM-01 | Inventories of hardware managed by the organisation are maintained | 11.5.1, 11.5.4 |
| ID.AM-08 | Systems, hardware, software, services, and data are managed throughout their life cycles | 11.2.13, 11.2.14, 11.3.4, 11.5.1, 11.5.4, 11.5.5 |
| ID.RA-09 | The authenticity and integrity of hardware and software are assessed prior to acquisition and use | 11.3.1, 11.3.2 |
| PR.AA-01 | Identities and credentials for authorised users, services, and hardware are managed by the organisation | 11.5.2 |
| PR.AA-03 | Users, services, and hardware are authenticated | 11.2.2, 11.4.6 |
| PR.AA-05 | Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties | 11.2.10, 11.2.11, 11.3.3, 11.4.6, 11.5.2 |

| | | |
|---|---|---|
| PR.AT-01 | Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind | 11.1.3 |
| PR.DS-01 | The confidentiality, integrity, and availability of data-at-rest are protected | 11.1.4, 11.2.1, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.2.12, 11.2.13, 11.2.15 |
| PR.DS-02 | The confidentiality, integrity, and availability of data-in-transit are protected | 11.1.4, 11.1.6, 11.2.1, 11.2.15, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.7, 11.4.8 |
| PR.DS-10 | The confidentiality, integrity, and availability of data-in-use are protected | 11.2.1 |
| PR.PS-01 | Configuration management practices are established and applied | 11.3.5 |
| PR.PS-02 | Software is maintained, replaced, and removed commensurate with risk | 11.2.14, 11.3.4, 11.5.5 |
| PR.PS-03 | Hardware is maintained, replaced, and removed commensurate with risk | 11.2.14 |
| PR.PS-04 | Log records are generated and made available for continuous monitoring | 11.6.1, 11.6.2 |
| PR.PS-05 | Installation and execution of unauthorised software are prevented | 11.3.5, 11.3.6 |
| DE.CM-03 | Personnel activity and technology usage are monitored to find potentially adverse events | 11.5.3 |

| | | |
|---|---|---|
| DE.CM-09 | Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events | 11.3.5, 11.3.6, 11.5.3, 11.6.1, 11.6.2 |

**Appendix B - Internal references**

Below, is a list of internal documents that **should** be read in conjunction with this standard.

Table 3 – Internal References

| Ref | Document | Publicly Available* |
|---|---|---|
| A | SS-036 Secure Sanitisation & Destruction Security Standard | Yes |
| B | SS-007 Use of Cryptography Security Standard | Yes |
| C | SS-019 Wireless Network Security Standard | Yes |
| D | DWP Acceptable Use Policy | Yes |
| E | SS-015 Malware Protection Security Standard | Yes |
| F | SS-033 Security Patching Standard | Yes |
| G | SS-037 Bring Your Own Device (BYOD) Security Standard | No |
| H | SS-001 Access & Authentication Security Standard | Yes |
| I | SS-016 Remote Access Security Standard | Yes |
| J | Security Assurance Strategy | No |

*Request to access to non-publicly available documents **should** be made to the Authority.

## Appendix C External references

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

| Ref | Document |
|---|---|
| | CIS Critical Security Controls Set |
| | Device Security Guidance - NCSC.GOV.UK |
| | NIST Special Publication 800-124 2 Revision 2 |
| | NIST Mobile Threat Catalogue |

## Appendix D Abbreviations

Table 5 – Abbreviations

| Abbreviation | Definition |
|---|---|
| MDM | Mobile Device Management |
| VPN | Virtual Private Network |
| DPA | Data Privacy ACT |
| MTC | Mobile Threats Catalogue |

## Appendix E Definition of Terms

Table 6 – Glossary

| Term | Definition |
|---|---|
| Mobile Device | Smart phones and tablets. |
| Jailbreaking | The process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device. |
| Rooting | The process of allowing users to attain privileged control (known as root access) over various subsystems. |
| Side-loading | Installing apps that aren't from an official source. |

## Appendix F - Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

Guidance and tools for digital accessibility

Understanding accessibility requirements for public sector bodies