Security Standard - Mobile Device (SS-017)

Chief Security Office

Date: 27/02/23

Department for Work & Pensions

This Mobile Device Security Standard is part of a suite of standards, designed to promote consistency across the Authority, 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:

https://www.gov.uk/government/publications/dwp-procurement-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).

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; • Updated Intro, purpose, audience, scope; added reference to CIS v8 security controls • Added NIST CSF references 11.1.4 – Update regarding walled garden approach 11.1.5 Requirement added regarding device lifecycle 11.1.6 Requirement added for blocking unauthorised data transfers 11.2.1 Added reference to NCSC Mobile Device Guidance 11.2.2 Amended passcode requirements 11.2.3 Updated timeout requirements 11.3.1 Requirement added for application vetting 11.3.5 Requirement added to prohibit jailbreaking and block jailbroken devices. 11.3.6 Requirement added for compromise detection 11.4.8 Requirement added for public Wi-Fi access points	27/02/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	04/07/2017
2.0		Chief Security Officer	27/02/2023

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

4. Compliance

Security assurance teams will verify compliance with this standard through various methods, including but not limited to, internal and external audits, and feed back to the appropriate Authority Risk and System Owner.

5. Exceptions Process

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

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

8. Introduction

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 v8 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 Authority's Acceptable Use Policy [Ref. D] for statements regarding personal use of Authority equipment.

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 Authority's 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 v8 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 Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

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

11. Minimum Technical Security Measures

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

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-1
11.1.2	The mobile device **must** be allocated to a named individual for their use only.	ID.AM-1
11.1.3	Users **must** be provided with guidance on the secure use of mobile devices and remote working.	PR.AT-1
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-5
11.1.5	Device lifecycle **must** be managed considering overall device health e.g. battery life.	PR.DS-3
11.1.6	The Mobile Device Management (MDM) system **must** block any data transfer from unauthorised devices, including chargers.	PR.DS-2 PR.DS-5

11.2 Mobile Device Security Configurations

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-5
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. Biometric login can be also used as an alternative.	PR.AC-1 PR.AC-2 PR.AC-6 PR.AC-7
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-5
11.2.5	All usable storage on the device **must** be encrypted in line with SS-007 Use of Cryptography Security Standard [Ref. B].	PR.DS-1
11.2.6	Data on the device **must** be wiped after a maximum of ten failed passcode entry attempts.	PR.DS-1
11.2.7	The data contained on the device **must** be able to be remotely wiped via the MDM system, whilst connected to the mobile network, if the device is lost or stolen.	PR.DS-1
11.2.8	Devices **must** not be able to synchronize to non-Authority devices.	PR.DS-1
11.2.9	Devices **must** only back-up data to Authority storage locations.	PR.DS-1
11.2.10	Anti-malware **must** be installed on all mobile devices.	PR.DS-1 PR.DS-5 DE.CM-4 DE.CM-5
11.2.11	A user **must** not be able to modify the boot process of a device and, any attempt should be detected.	PR.AC-4 DE.DP-4
11.2.12	A user **must** not be able to modify or disable security safeguards.	PR.AC-4
11.2.13	Devices **must** be erased and all data removed before the device is re-issued to a new user.	PR.DS-1

11.2.14	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-3 PR.IP-6

11.3 Mobile Application Security Requirements

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-1
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.	PR.IP-3
11.3.3	Access to App Stores **must** be restricted by Authority MDM settings.	PR.AC-4
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.	PR.IP-3
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.IP-3
11.3.6	Compromise detection **must** be implemented for mobile devices and prevent the installation of apps from unauthorised sources.	DE.CM-5 DE.CM-7

11.4 Mobile Device Connectivity Security Requirements

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.	PR.DS-2
11.4.2	The VPN between the source endpoint device and the enterprise gateway **must** be established using full end to end tunnelling using a Authority approved encryption algorithm.	PR.DS-2
11.4.3	Devices **must** be configured so that the USB interface is only allowed for charging.	PR.DS-5
11.4.4	Devices **must** not be able to transfer Authority data to any other device, unless it is via an approved Authority method. All data transfer protocols **must** be disabled by default.	PR.DS-5
11.4.5	Devices **must** not be able to connect to wireless networks requiring login via a landing page.	PR.DS-5
11.4.6	Only authenticated Devices **must** be allowed access to Authority enterprise services.	PR.AC-3 PR.AC-5 PR.AC-7
11.4.7	Wi-Fi connections security **must** be in line with SS-019 Wireless Network Security Standard [Ref. C].	PR.DS-2
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-2

11.5 Mobile Device Management Security Requirements

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-1
11.5.2	Access to enterprise resources **must** be restricted, based on the mobile devices and user access rights.	PR.AC-4
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.	PR.IP-3 DE.CM-7

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-1

11.6 Monitoring and Logging

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	The solution **must** enable logging to its maximum required capability, without impacting performance.	PR.PT-1
11.6.2	Logging of appropriate security related events for each mobile device **must** be enabled by default, where available.	PR.PT-1

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 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-1	Physical devices and systems within the organization are inventoried	11.1.1, 11.1.2, 11.5.1, 11.5.4
ID.RA-1	Asset vulnerabilities are identified and documented	11.3.1
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.2.2
PR.AC-2	Physical access to assets is managed and protected	11.2.2
PR.AC-3	Remote access is managed	11.4.6
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.2.11, 11.2.12, 11.3.3, 11.5.2
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.4.6
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.2.2
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.2.2, 11.4.6

PR.AT-1	All users are informed and trained	11.1.3
PR.DS-1	Data-at-rest is protected	11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.2.10, 11.2.13
PR.DS-2	Data-in-transit is protected	11.1.6, 11.4.1, 11.4.2, 11.4.7, 11.4.8
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	11.1.5, 11.2.14
PR.DS-5	Protections against data leaks are implemented	11.1.4, 11.1.6, 11.2.1, 11.2.3, 11.2.10, 11.4.3, 11.4.4, 11.4.5
PR.IP-3	Configuration change control processes are in place	11.3.2, 11.3.4, 11.3.5, 11.5.2
PR.IP-6	Data is destroyed according to policy	11.2.14
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.6.1, 11.6.2
DE.CM-4	Malicious code is detected	11.2.10
DE.CM-5	Unauthorized mobile code is detected	11.2.10, 11.3.6
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	11.3.6, 11.5.3
DE.DP-4	Event detection information is communicated	11.2.11

Appendix B Internal References

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

Table 2 – 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

Requests to access 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 3 – External References

External Documents List
CIS Critical Security Controls v8 controls set
NCSC Mobile Device Guidance
NIST Special Publication 800-124 2 Revision 2
NIST Mobile Threat Catalogue

Appendix D Abbreviations

Table 4 – 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 5 – 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 of 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:

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps