IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Security Standard Mobile Device SS 017

Security Architecture

Date: 04/07/2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

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

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

Contents

1. Introduction

1.1. This Security Standard provides a list of security controls that apply to all Mobile Device deployments. This list of requirements ensures a baseline level of security that is both approved and accepted by the Department for Work and Pensions (DWP) to afford the necessary level of protection to its systems and data.

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint*, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for Mobile Device security* and been tailored for Departmental suitability.

*Please see the reference section for this document.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for mobile device.

3. Exceptions

3.1. Any exceptions to the application of this standard or where controls cannot be adhered to **MUST** be presented to an assigned Security Architect and considered for submission to Design Authority (DA) were appropriate. This **MUST** be carried out prior to deployment and managed through the design caveats or exception process.

3.2. Such exception requests may invoke the Risk Management process in order to identify and assess the potential impact of any deviation to the configuration detailed in this standard.

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

4. Audience

4.1. This standard is intended for DWP security groups, security compliance staff, technical architects, IT staff and suppliers, involved in securing mobile devices for DWP infrastructure and systems and provides the security requirements on how to secure such devices.

5. Scope

5.1. This standard applies to all Mobile Devices which will be used by DWP staff and contractors to access DWP services and/or data.

In the event of uncertainty on the controls laid out in this standard please contact the Security Front Door for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1 Term used

In this document the term **MUST** is used, and when in upper case have Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7. Security Requirements

The following sections provide the security requirements to be applied to Mobile Devices prior to deployment for use on the DWP network infrastructure.

10.1. General Security Requirements

Reference	Security Control Requirement
10.1.1	The mobile device **MUST** be owned, configured and managed by DWP or its approved supplier.
10.1.2	The mobile device **MUST** be allocated to a named individual for their use only.
10.1.3	Users **MUST** be provided guidance on the secure use of mobile devices and remote working.
10.1.4	Design principles for any DWP mobile device solution, **MUST** follow the NCSC walled garden pattern approach, unless a different approach is approved by DWP Security.

10.2. Mobile Device Security Configurations

Reference	Security Control Requirement
10.2.1	All mobile devices **MUST** be configured in accordance with the relevant NCSC EUD Security Guidance. Exceptions must be approved by the DWP Design Authority.
10.2.2	A user **MUST** authenticate to the device using a passcode containing the minimum of six characters, with at least one special character and one capital letter. Biometric login can be used as an alternative, with an appropriate risk assessment.
10.2.3	After 2 minutes of inactivity the device **MUST** automatically lock.
10.2.4	Notifications and information can be displayed when the screen is locked but only after an appropriate risk assessment has been undertaken.
10.2.5	All usable storage on the device **MUST** be encrypted, using a DWP approved, or the manufacturer's default, method. Where the manufacturer's method does not meet DWP requirements a risk assessment **MUST** be undertaken.
10.2.6	Data on the device **MUST** be wiped after a maximum of ten failed passcode entry attempts.
10.2.7	The data contained on the device **MUST** be able to be remotely wiped, whilst connected to the mobile network, if the device is lost or stolen.
10.2.8	Devices **MUST** not be able to synchronize to non-DWP devices.
10.2.9	Devices **MUST** only back-up data to DWP storage locations.
10.2.10	Anti-malware **MUST** be installed on all mobile devices, where this is deemed not a requirement, there **MUST** be a risk assessment undertaken.
10.2.11	A user **MUST** not be able to modify the boot process of a device and, any attempt should be detected.
10.2.12	A user **MUST** not be able to modify or disable security safe guards.
10.2.13	Devices **MUST** be wiped and all data removed before the device is re-issued to a new user.
10.2.14	At the end of life, the devices **MUST** be sanitised securely in accordance with the manufacturer's guidelines and the DWP sanitisation Policy.

10.3. Mobile Application Security Requirements

Reference	Security Control Required
10.3.1	All applications installed on DWP devices **MUST** be risked assessed and approved via the DWP Application approvals process.
10.3.2	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.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Required
10.3.3	Access to App Stores **MUST** be restricted by DWP MDM settings.
10.3.4	There **MUST** be a mechanism to install, update and remove all applications and to safeguard the mechanisms used to perform these actions.

10.4. Mobile Device Connectivity Security Requirements

Reference	Security Control Required
10.4.1	All traffic to and from the mobile device **MUST** be routed over an approved DWP VPN tunnel.
10.4.2	The VPN between the source endpoint device and the enterprise gateway **MUST** be established using full end to end tunnelling using a DWP approved encryption algorithm.
10.4.3	Devices **MUST** be configured so that the USB interface is only allowed for charging.
10.4.4	Devices **MUST** not be able to transfer DWP data to any other device, unless it is via an approved DWP method. All data transfer protocols **MUST** be disabled by default.
10.4.5	Devices **MUST** not be able to connect to wireless networks requiring login via a landing page.
10.4.6	Only authenticated Devices **MUST** be allowed access to DWP enterprise services.

10.5. Mobile Device Management Security Requirements

Reference	Security Control Required
10.5.1	All DWP mobile devices **MUST** be centrally managed using MDM (Mobile Device Management).
10.5.2	Access to enterprise resources **MUST** be restricted, based on the mobile devices and user access rights.
10.5.3	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.
10.5.4	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.

10.6. Logging Requirements

Reference	Security Control Required
10.6.1	The solution **MUST** enable logging to its maximum required capability, without impacting performance.
10.6.2	Logging of appropriate security related events for each mobile device **MUST** be enabled by default, where available.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

8. Compliance

8.1 Compliance with this standard **MUST** occur as follows:

Compliance	Due Date
For all new mobile devices	From the first day of approval
Retrospective	Within 6 months of the approval of the standard

9. Accessibility

9.1 No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However, it is deemed that projects implementing this standard are obliged to incorporate accessibility functions.

10. Reference Documents

NIST Special Publication 800-124 Revision 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise dated June 2013.

NCSC End User Devices dated 29 December 2016.

11. Glossary

Abbreviation	Definition
MDM	Mobile Device Management
VPN	Virtual Private Network

12. Definition of Terms

Term	Definition
Mobile Device	Smart phones and tablets

13. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27002:2013, NIST 800-53, and the OWASP ASVS.

SS-017 Mobile Device Standard	**DWP Controls Catalogue - Baseline Control Set**	
V1.0	DWP Controls catalogue	Place the catalogue narrative here