Security Standard – Remote Access SS-016

Security Architecture

Date: 04/07/2017

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.

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.

Contents

1. Introduction

1.1. This Security Standard provides a list of security controls that apply to all remote access. This list of requirements ensures a baseline level of security that is 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 remote access* and have 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 devices.

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) where 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 providing remote access to the DWP infrastructure and systems, and provides the security requirements on how to secure such connections.

5. Scope

5.1. This standard applies to all remote access solutions which will be used by DWP staff, contractors and third parties to access DWP infrastructure enterprise 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, the 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.

7. Security Requirements

The following sections provide the security requirements to be applied to remote access solutions prior to deployment for DWP use.

10.1. General Security Requirements

Reference	General Security Requirements
10.1.1	Remote access to the DWP Systems and applications **MUST** only use a DWP approved VPN tunnelling or network remote access solution.
10.1.2	The endpoint device **MUST** be owned and managed by DWP and configured in accordance with appropriate DWP endpoint device security pattern or be a DWP approved third party owned device.
10.1.4	Users **MUST** be provided with guidance on the secure use of endpoint devices and secure remote working as part of their induction training or annual security training.

10.2. Remote Access Security Configurations

Reference	Device Security Configurations
10.2.1	A user **MUST** authenticate to the endpoint device using a DWP approved authentication mechanism, such as two factor authentication.
10.2.2	The authentication password **MUST** comply with DWP password policy, where available, otherwise NCSC guidelines **MUST** be followed.
10.2.3	Where certificates are used for authentication of device or user, they **MUST** comply with DWP Certificate Policy, otherwise NCSC guidelines MUST be followed.
10.2.4	Where certificates or private keys are utilised they **MUST** be housed in a tamper proof module to prevent unauthorised access, including a TPM module for laptop whole disk encryption and smart cards for user access control, where available. Other mechanisms **MUST** be risk assessed prior to implementation.
10.2.5	Where a VPN Client is required, it **MUST** be installed on all endpoints prior to deployment.

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	Device Security Configurations
10.2.6	Whole disk encryption **MUST** be applied to the Device, prior to DWP data being stored on it.

10.3. Endpoint Device Connectivity Security Requirements

Reference	Endpoint Device Connectivity Security Requirements
10.3.1	Connection of the endpoint to Wi-Fi networks requiring login via a landing page **MUST** be denied.
10.3.2	All traffic from the endpoint device **MUST** be routed to the DWP enterprise, or an assured trusted environment using a DWP approved VPN Service.
10.3.3	The connection between endpoint device and the approved VPN service **MUST** be mutually authenticated before accessing DWP internal systems.
10.3.4	The VPN service **MUST** use DWP approved encryption mechanisms.

10.4. VPN Service Security Requirements

Reference	VPN Service Security Requirements
10.4.1	Only DWP approved VPN Services **MUST** manage the remote access for all endpoints connecting to the DWP enterprise network.
10.4.2	The DWP approved VPN Service **MUST** authenticate the endpoint devices before allowing remote access to the DWP enterprise network.
10.4.3	Where possible, the DWP approved VPN Service **MUST** confirm the configuration patching and anti-malware status of the remote connecting device, prior to it connecting to the DWP enterprise network.
10.4.4	After 30 minutes of inactivity the VPN connection **MUST** be terminated automatically.
10.4.5	The VPN service **MUST** include the capability to revoke access for a specific user or device.
10.4.6	Where possible, the VPN service **MUST** support the capability to deploy security patches, fixes and updates to remote end points.

10.5. Logging Requirements

Reference	Logging Requirements
10.5.1	The DWP approved VPN Service or device **MUST** log all events for each endpoint connection.
10.5.2	Where possible the DWP approved VPN Service **MUST** automatically monitor, detect, and report when policy violations occur, such as changes from the approved security configuration baseline, and automatically take action where possible and if appropriate.

8. Compliance

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

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard

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.

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. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		
Channel Encryption Pattern		
Wireless Security Standard		
Security Incident Management Standard		

11. Reference Documents

NIST Special Publication 800-46 Revision 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security dated July 2016

NCSC End User Devices dated 29 December 2016.

12. Glossary

Abbreviation	Definition
VPN	Virtual Private Network

13. Definition of Terms

Term	Definition
Endpoint	Laptops, Tablets, or hybrid 2in1 devices
Remote Access	DWP employees, contractors, business partners, vendors suppliers and any other person(s) accessing DWP Systems and applications to perform work from external locations.

14. 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-016 Remote Access Security Standard	**DWP Controls Catalogue - Baseline Control Set**	
V1.0	DWP Controls Catalogue	Networks shall be managed and controlled to protect information in systems and applications.