Security Standard – Remote Access (SS-016)

Chief Security Office

Date: 27/02/2025

Department for Work & Pensions

This Remote Access 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.

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

1. Contents **3**

2. Revision history **4**

3. Approval history **6**

4. Compliance **6**

5. Exceptions Process **7**

6. Audience **7**

7. Accessibility statement **7**

8. Introduction **7**

9. Purpose **9**

10. Scope **9**

11. Minimum Technical Security Measures **10**

1.1. General Security Requirements 10

1.2. Remote Access Server Security 12

1.3. Remote Access Server Implementation 12

1.4. Authentication and Authorisation 14

1.5. Administration 16

1.6. Client Device Security 17

1.7. Logging Requirements 18

12. Appendices **19**

Appendix A - Security Outcomes 19

Appendix B - Internal references 21

Appendix C - External references 22

Appendix D - Abbreviations 23

Appendix E - Glossary 24

Appendix F - Accessibility artefacts 24

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; Changes to security measures following review Removed reference to Guiding Security Principles Document as previously agreed, and updated all references accordingly Added NIST references Updated Appendix A to reference back to the security measures 11.1 Add requirements regarding encryption, patching and use of NAC. 11.2 Added requirements for remote access server hosting and differing remote access user groups 11.3 Added requirements for hardening of communications traffic, logical placement of RAS servers, security gateway traffic and content inspection 11.4 Consolidated requirements for access and authentication, including mobile devices 11.5 Consolidated administration requirements 11.6 Consolidated requirements for client device security	16/01/2023

2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years Compliance updated in line with other standards Audience – Use of 11.1.2 Supplier users 11.1.3 Added ref to PKI standard 11.1.6 Non-approved VPNs forbidden. 11.4.4 Credentials not shared; modern authentication technologies 11.4.5 Location based conditional access; contracted supplier premises 11.4.10 Ref added to SS-017 for rooting and jailbreaking	27/02/2025

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	04/07/2017
2.0		Chief Security Officer	16/01/2023
2.1		Chief Security Officer	27/02/2025

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.
- 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 limited to, solution architects, security architects, domain architects, technical engineers, developers, security teams, security monitoring teams, project teams, including suppliers engaged in the design, development, implementation or usage of Information and Communications Technology (ICT) systems for Departmental use.

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 Remote Access Security Standard defines the minimum-security measures that **must** be implemented when deploying technical solutions that enable remote access to Authority networks and systems. For the purposes of this standard, remote access

can be described as having the ability to access network resources from locations other than an organisations facility i.e., from home.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, 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]. The security measures also support the enforcement of the Authority's Remote Working Policy [Ref. B] which **should** be read in conjunction with this standard.

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 Authority systems and resources are accessed securely by known subjects or entities irrespective of where they are.
- support technical teams in securing remote access solutions using a consistent set of security controls.
- ensure users and devices are mutually authenticated often, and the integrity of the endpoints are checked prior to granting controlled time-bound access to Authority resources.

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 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 remote access solutions deployed by the Authority or contracted third parties including suppliers, are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

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

10. Scope

(Important) this paragraph contains ‘must’ activities.

This standard applies to all solutions that enable remote access to Authority networks and resources irrespective of where they are hosted or the entity managing them i.e., third-party supplier. The security measures **must** be applied to new and existing installations, and adherence to these measures **must** be included in all contracts for outsourced services where applicable.

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.

1.1. General Security Requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Remote access to Authority networks, applications and resources **must** only use an Authority approved VPN tunnelling or CASB network remote network access solutions.	PR.IR-01
11.1.2	Remote access 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. Written records **must** be maintained to confirm completion of training by end users as these may be subject to audits. Where these users are in the supplier community, this responsibility sits with the Authority Contract/Supplier manager.	PR.AT-01
11.1.3	The remote access service **must** use Authority approved encryption mechanisms in accordance with SS-007 Use of Cryptography Security Standard [Ref. C], the DWP Approved Cryptographic Algorithms workbook [Ref. K], and where relevant SS-002 Public Key Infrastructure & Key Management Security Standard [Ref. E].	PR.DS-02

11.1.4	The remote access service **must** support the capability to deploy security patches, fixes, and updates to remote end points.	ID.AM-08
11.1.5	Network Access Control (NAC) technologies **must** be used where possible to detect security policy violations in remote client devices. However, it **must** not be relied upon to stop determined attackers from gaining network access as malware can circumvent it.	PR.IR-01 DE.CM-01
11.1.6	Use of personal or non- Authority approved VPNs in conjunction with Authority devices is expressly forbidden.	PR.IR-01 DE.CM-01
11.1.7	The remote access service **must** be patched up to date in line with SS-033 Security Patching standard [Ref. M].	ID.AM-08

1.2. Remote Access Server Security

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Remote access servers **must** be hardened in accordance with SS-008 Server Operating System Security Standard where applicable [Ref. D].	PR.IR-01
11.2.2	Remote access servers i.e., VPN Gateways and Portal Servers, **must** be placed on separate dedicated hosts where possible to reduce the attack surface.	PR.IR-01
11.2.3	Separate remote access solutions **must** be deployed where different groups of remote access users have significantly different security needs. This can be either logical or physical depending on the security profile of a given solution.	PR.IR-01

1.3. Remote Access Server Implementation

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Endpoint remote access servers **must** be placed in DMZs where possible to provide logical separation from internal networks. This will allow the firewall(s) to limit access to the servers from both external and internal hosts.	PR.IR-01
11.3.2	Remote access servers **must** not circumvent firewall security policies.	PR.IR-01

11.3.3	Remote access architecture **must** be designed so that communications can be examined by the appropriate network and or host-based security controls (except where an approved Authority Security Pattern[1] is followed).	PR.IR-01 DE.CM-01
11.3.4	Communication between remote access servers and internal networks **must** be restricted to the bare minimum, to reduce impact of compromise of the remote access server.	PR.IR-01
11.3.5	Remote access server communications with internal hosts **must** be hardened, only supporting authenticated and authorised sessions with internal hosts.	PR.AA-03 PR.IR-01
11.3.6	Security gateway policy **must** be hardened only allowing authenticated and authorised communication with remote users and services. For example, constraining incoming traffic to only allow IP address ranges with authorised business partners, vendor networks, supplier networks etc.	PR.AA-03 PR.IR-01

[1] Approved Security Patterns are those published as part of the DWP Blueprint. Access to patterns are strictly controlled by the DWP therefore where required, should be requested via the assigned Security Architect or Contracts/Supplier Manager.

1.4. Authentication and Authorisation

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Users **must** authenticate to the endpoint device using an Authority approved authentication method. The remote access service **must** authenticate each remote end point before granting access to Authority networks and resources, and then use authorisation technologies to ensure that only the necessary resources can be used.	PR.AA-03 PR.IR-01
11.4.2	Remote access solutions **must** implement approved multi-factor authentication for end users.	PR.AA-01 PR.AA-03
11.4.3	Where certificates are used for authentication of device and / or user, they **must** comply with SS-002 Public Key Infrastructure & Key Management Security Standard [Ref. E] otherwise NCSC guidelines **must** be followed.	PR.AA-01 PR.AA-03
11.4.4	Certificates and private keys **must** be protected, e.g., technologies using Trusted Platform Modules to prevent unauthorised access. Typically, modern authentication technologies include TPM module supporting multi-factor authentication. These credentials **must never** be shared with unauthorised users. Other mechanisms **must** be formally risk assessed and approved prior to implementation.	PR.AA-01 PR.AA-03

11.4.5	Remote users should be forced to re-authenticate at least every 8 hours of an active session if working in a trusted location such as a Authority office, contracted supplier premises or user's home. In less trusted locations, conditional access rules should be used to force users to reauthenticate every 2 hours.	PR.AA-01 PR.AA-03 PR.IR-01
11.4.6	After 30 minutes of inactivity (timing **may** be reduced as appropriate), the VPN / remote connection **must** be automatically terminated.	PR.IR-01
11.4.7	Mutual authentication **must** take place between client and the VPN service server before granting access to Authority services. For example, verifying a digital certificate presented by the remote access server to ensure the server is controlled by the Authority or its partners and suppliers.	PR.AA-03 PR.AA-04
11.4.8	Remote Access solution attributes **must** be robust and include multi-factor authentication in accordance with SS-001 (part 1) Access and Authentication Security Standard [Ref. F] and SS-001 (part 2) Privileged User Access Security Standard [Ref. G].	PR.AA-03
11.4.9	The Remote Access Service **must** be subject to timely health checks / security posture checks on remote client devices, e.g., to ensure anti-malware software is up to date, the OS is patched in accordance with SS-033 Security Patching Standard, the device is owned and controlled by the Authority or its partners/suppliers. Failed checks **must** deny access to Authority resources.	ID.AM-08 PR.IR-01

11.4.10	Mobile devices **must** be subject to compliance checks i.e., if the device has been rooted or jail broken, as this can have serious negative security implications. Failed checks **must** deny access to Authority resources. Please refer to SS-017 Mobile Device Security Standard [Ref. I] for further information on rooting / jailbreaking.	PR.IR-01
11.4.11	The remote access service **must** include the capability to revoke access for a specific user and / or device.	PR.IR-01

1.5. Administration

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Administrative access of Authority networks both on premise and Cloud hosted instances **must** be secured via an Authority approved solution. Direct administration through RDP or SSH **must not** be permitted. A hardened authentication and authorisation solution is required via an Authority approved CASB or bastion host as appropriate.	PR.AA-02 PR.AA-03 PR.AA-05
11.5.2	Remote access servers **must** only be managed from the Authority or third party approved hosts e.g., by authenticated and authorised personnel.	PR.AA-03 PR.AA-05
11.5.3	Separate bastion hosts **must** be used to manage systems in each security boundary.	PR.IR-01

11.5.4	Devices such as jump servers or bastion hosts **must** be hardened and maintained to current build level to ensure they are a robust and difficult target. This **must** be carried out in accordance with the SS-033 Security Patching Standard [Ref J].	ID.AM-08 PR.IR-01
11.5.5	Current approved versions of secure protocols **must** be used, configured to use strong authentication.	PR.AA-03 PR.PS-02

1.6. Client Device Security

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Endpoint devices **must** be owned and managed by the Authority or be an approved device where owned by a contracted third party / supplier.	PR.PS-03 PR.IR-01
11.6.2	Endpoint devices **must** be configured in accordance with SS-010 Desktop Operating System Security Standard [Ref. H] and where applicable, SS-017 Mobile Device Security Standard [Ref. I].	PR.PS-03 PR.IR-01
11.6.3	Configuration of the remote access client software **must** be hardened, and a control implemented to prevent unauthorised changes weakening remote access security.	PR.AA-05 PR.IR-01
11.6.4	Split tunnelling **must** be avoided, to minimise risk of data leaking outside secure tunnels.	PR.DS-02
11.6.5	Connection of the endpoint to public Wi-Fi networks requiring login via a landing page (or captive portals) **must** be denied.	PR.AA-03 PR.IR-01
11.6.6	All traffic from the endpoint device **must** be routed to the Authority enterprise, or an assured trusted environment using an Authority approved VPN or remote access service.	PR.DS-02

11.6.7	Where VPN or CASB client software is applicable, the client software **must** be installed on endpoints prior to deployment.	ID.AM-08 PR.PS-02
11.6.8	Whole disk encryption **must** be applied to the Device, prior to Authority data being stored on it, in line with SS-007 Use of Cryptography Security Standard [Ref. C].	PR.DS-01

1.7. Logging Requirements

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	The remote access service **must** log all events for each endpoint connection. Refer to SS-012 Protective Monitoring Security Standard [Ref. J] for the full set of measures that **must** be complied with.	DE.CM-01
11.7.2	Where possible the remote access service **must** automatically monitor, detect, and report when policy violations occur, such as changes from the approved security configuration baseline, and automatically take action as appropriate.	DE.CM-01

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 which can also be cross referenced against DWP approved control set, which itself is based on the CIS Critical Security Controls.

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related security measures
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.1.4, 11.1.7, 11.4.9, 11.5.4, 11.6.7,
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	11.4.2, 11.4.3, 11.4.4, 11.4.5,
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.5.1,
PR.AA-03	Users, services, and hardware are authenticated	11.3.5, 11.3.6, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.7, 11.4.8, 11.5.1, 11.5.2, 11.5.5, 11.6.5,
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.4.7,

PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.5.1, 11.5.2, 11.6.3,
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	11.1.2,
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.6.8
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.1.3, 11.6.4, 11.6.6,
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	11.1.1, 11.1.5, 11.1.6, 11.2.1, 11.2.2, 11.2.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.3.6, 11.4.1, 11.4.5, 11.4.6, 11.4.9, 11.4.10, 11.4.11, 11.5.3, 11.5.4, 11.6.1, 11.6.2, 11.6.3, 11.6.5
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.5.5, 11.6.7
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	11.6.1, 11.6.2,
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.1.5, 11.1.6, 11.3.3, 11.7.1, 11.7.2

Appendix B - Internal references

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

Table 3 – Internal References

Ref	Document	Publicly Available*
B	DWP Remote Working Security Policy	Yes
C	SS-007 Use of Cryptography Security Standard	Yes
D	SS-008 Server Operating System Security Standard	Yes
E	SS-002 Public Key Infrastructure & Key Management Security Standard	Yes
F	SS-001 (part 1) Access and Authentication Security Standard	Yes
G	SS-001 (part 2) Privileged User Access Security Standard	Yes
H	SS-010 Desktop Operating System Security Standard	Yes
I	SS-017 Mobile Device Security Standard	Yes
J	SS-012 Protective Monitoring Security Standard	Yes
K	DWP Approved Cryptographic Algorithms	No
L	DWP Security Assurance Strategy	No
M	SS-033 Security Patching Security Standard	Yes

*Request to access to non-publicly available documents **should** be made to the Authority Contracts/Supplier Manager.

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
A1	NIST Special Publication 800-46 Revision 2 – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, June 2016
A2	NCSC Network Architectures, Published 29 June 2021, Version 1
A3	NCSC Device Security Guidance – Virtual Private Networks (VPN), Published 29 June 2021, Version 1
A4	GPG Protective Monitoring for HMG ICT System, October 2012, Issue No: 1.7
A5	NIST Special Publication 800-207 Zero Trust Architecture, August 2020
A6	Microsoft Security Guidance for Remote Desktop Adoption, April 2020

Appendix D - Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
Mobile Device	A small mobile computer such as a smartphone or tablet	Industry term
Remote Access	The ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.	Industry term
Split Tunnelling	A VPN client feature that tunnels all communications involving the organization's internal resources through the VPN, thus protecting them, and excludes all other communications from going through the tunnel.	Industry term
Tunnelling	A high-level remote access architecture that provides a secure tunnel between a telework client device and a tunnelling server through which application traffic may pass.	Industry term
Virtual Private Network (VPN)	provides a secure communications tunnel for data and other information transmitted between networks	Industry term

Appendix E - Glossary

Table 6 – Glossary

Term	Definition
CASB	Cloud Access Security Broker
CSF	Cyber Security Framework
DDA	Digital Design Authority
DMZ	Demilitarised Zone
IP	Internet Protocol
NAC	Network Access Control
NIST	National Institute of Standards and Technology
OS	Operating System
PII	Personally, Identifiable Information
RDP	Remote Desktop Protocol
SP	Special Publication
SSH	Secure Shell
TLS	Transport Layer Security
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

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