Security Standard – Firewall Security (SS-013)

Chief Security Office

Date: 21/11/2023

Department for Work & Pensions

This Firewall Security Standard is part of a suite of standards, designed to promote consistency across the Department of Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the terms 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 relevant suppliers in delivering the DWP and HMG Digital Strategy. The suit of 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 - List of 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. Table of Contents

2. Revision history

Version	Author	Description	Date
1.0		First Published Version	02/06/2017
1.1		Updated as per review comments	16/10/2017
1.2		Updated to bring into closer alignment with ISO 27022, NIST-41r1 and PCI DSS.	18/12/2018
1.3		External Review of amended version	29/01/2019
1.4		2nd published version	04/03/2019
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 11.1 New section 11.2 Wherever possible 11.2.3 Backout / rollback plan 11.2.4 Network infrastructure 11.2.5 Network infrastructure 11.3.1 & 11.3.32 'Must'; exceptions 11.3.3 Capacity Management planning 11.3.4 New implementations 11.4.1 Vulnerability and config mgmt, and rules assurance 11.4.2 Physical firewalls 11.4.4 Where available and where reliable 11.4.6 Unnecessary rules 11.4.10 Overly permissive access 11.4.13 Benchmarks and exclusions 11.4.14 Centralised documentation 11.4.16 Invalid addresses 11.4.18 Protocol types removed; deny all access by default 11.5.1 Added ref to Protective Monitoring standard 11.5.3 Where supported 11.5.4 or ITHC 11.5.5 NAT reporting 11.5.6 Log retention, Protective Monitoring standard 11.6.1 Authentication at appropriate points	21/11/2023

		11.6.2 default usernames and passwords 11.6.4 Appendix G 11.6.5 must 11.7.1 Prefer CC certified 11.7.2 Cloud provider time sources, stratum level 11.7.3 Unused ports and interfaces disabled 11.9.1 Removed 11.9.3 & 11.9.5 Certificate pinning 11.9.7 Automated notifications 11.9.14 & 11.9.15 removed 11.9.17 Added DNS protection 11.9.21 Defined personal firewalls	

3. Approval history

Version	Approver	Role	Date
1.0		Chief Security Officer	02/06/2017
1.1		Chief Security Officer	18/12/2017
1.2		Chief Security Officer	18/12/2018
1.3		Chief Security Officer	29/01/2019
1.4		Chief Security Officer	04/03/2019
2.0		Chief Security Officer	21/11/2023

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

4. Compliance

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

- controls tests performed by first-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. G].
- independent external audit

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

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 measure's details 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 standard is intended for, but not limited to, architects, network engineers, system administrators, projects managers, security teams, and relevant suppliers who have responsibility for the technical aspects of preparing, operating, and securing remote access solutions.

7. Accessibility Requirements

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

8. Introduction

This firewall security standard defines the minimum security measures that **must** be implemented when deploying firewalls both virtualised and physical. For the purposes of this standard, a firewall can be described as a network security device that monitors and filters incoming and outgoing network traffic based on the Authority's established security policies. At its most basic, a firewall is essentially a network barrier that sites between networks with different security profiles.

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 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 upon the technology choices and business requirements in question.

The aim of this standard is to:

- *ensure firewalls are configured and deployed to meet the Departments security requirement.*
- *support technical teams in securing firewalls using a consistent set of security controls.*

Technical security standards ultimately support the achievement of security outcomes sought by the Department. 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 firewall solutions utilised by the Department or contracted third parties including suppliers, 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 Department can be assured that security obligations are being met or exceeded.

10. Scope

This standard provides security measures that apply to all firewall deployments in the Authority, physical, virtual, and cloud, or those owned or managed by an Authority supplier or contracted third party as part of an Authority contract.
Any queries regarding the security measures laid out in this standard **must** be sent to the Authority.

11. Minimum Technical Security Measures

The following section defines the minimum-security measures that **must** be implemented when deploying remote access controls, so that the outcomes described in Appendix A can be achieved. For ease of reference, the relevant NIST sub-category ID is provided against each security measure e.g. **PR.AC-3** to indicate which outcome(s) it contributes towards. Refer to Appendix A for full descriptions of security outcomes.

11.1 General design and principles

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Firewall configurations **must** be designed and implemented according to SS-006 – Security Boundaries [Ref. I].	PR.PT-4
11.1.2	All traffic allowed by firewall **must** be related to devices that are identified, managed and monitored.	ID.AM-1
11.1.3	Firewall Policies **must** take in consideration the sensitivity of the resource/data. Least privilege principles must be applied to restrict both visibility and accessibility.	PR.AC-4
11.1.4	Firewall configuration and rulesets **must** be managed by a formal change management process - see Section 11.2.	PR.IP-3
11.1.5	Firewalls **must** be hardened and configured securely in accordance with this standard, and where available, using guidance from vendors and third parties i.e., CIS Benchmarks Network Devices, also SANS Firewall Check list.	PR.PT-4

11.2 Firewall Change Management

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	All firewalls **must** be subject to formal change control, this include any changes being made to the associated infrastructure, ruleset, or user ACLs.	PR.IP-1, PR.IP-3
11.2.2	Introduction of firewalls **must** be tested wherever possible, and evaluated, including for compatibility with the wider ICT estate before deployment, this is to ensure correct working and compliance with this standard prior to go live.	ID.RA-1, PR.IP-7

11.2.3	The change control procedure **must** include the records of configuration management activities to be maintained, who is responsible for writing/keeping the record and the information to be included in each type of record that **must** include as a minimum: ▪ Why the change was required ▪ A Backout/Rollback Plan ▪ Who authorised the change ▪ When the change was made ▪ The outcome of the change	PR.IP-1, PR.IP-3
11.2.4	There **must** be a current network diagram which identifies all network infrastructure components (excluding end user devices but including wireless).	ID.AM-4
11.2.5	Network diagrams **must** be maintained to reflect new infrastructure changes including those removed.	ID.AM-4

11.3 Test Firewall Rule Changes

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Testing **must** confirm that the firewall is allowing and blocking network traffic according to the rulesets. All tests must follow a formal procedure and be documented. Any deviation from this requirement **must** be raised as an exception.	ID.RA-1, PR.IP-7
11.3.2	Rule changes **must** be tested in a suitable non-production environment before being pushed to the live environment. Any deviation from this requirement **must** be raised as an exception.	PR.DS-5, PR.IP-2, PR.PT-3
11.3.3	Capacity management planning **must** be performed to ensure firewalls provide adequate performance both at normal and peak periods.	ID.RA-1, PR.IP-7
11.3.4	New firewall implementations **must** be tested for component interoperability with the wider ICT estate, this is particularly important where firewall solutions contain components from multiple vendors.	ID.RA-1, PR.IP-7

11.4 Firewall Rule Management

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Rulesets **must** be regularly reviewed at least every 6 months. Technical controls **must** be in place to ensure the collection of data regarding vulnerability management, configuration management, and rules assurance, processing that data and use any insight gained to improve policy creation and enforcement.	PR.IP-1, PR.PT-3
11.4.2	When physical firewalls are decommissioned, any associated rules and settings **must** be removed. The decommission must follow SS-036 Sanitisation and Destruction Security Standard [Ref. H].	PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1
11.4.3	Firewalls **must** be routinely assessed for unnecessary or insecure services, protocols, or ports. Where vulnerabilities are identified, they **must** either be remediated or formally managed via the organisational security risk management processes.	ID.RA-1, ID.RA-6, PR.IP-12, DE.CM-8, RS.AN-5, RS.MI-3
11.4.4	Where available and where reliable, geolocation checks **must** be carried out on IP addresses in order to identify offshore IP addresses. This check **should** be automated where possible to identify traffic originating from nations known to be active in hacking.	PR.PT-4
11.4.5	The default deny principle **must** be applied to both inbound and outbound traffic. In other words, all inbound and outbound traffic which is not expressly permitted by the firewall policy **must** be blocked.	PR.AC-4, PR.DS-5
11.4.6	Rules which have the highest chance of matching the traffic pattern **should** be placed at the top of the list to minimise unnecessary rules being evaluated.	PR.PT-4
11.4.7	Any changes to the firewall rulesets **must** be alerted on in accordance with SS-012 Protective Monitoring Security Standard [Ref. A] by generating a security event which subsequently generates an alert.	DE.CM-1
11.4.8	All rules **must** be quality assured and approved before being implemented. Separation of duties **must** be enforced for this process i.e., the persons creating or amending the rule **must** not also be tasked with carrying out quality assurance activities.	ID.RA-1, PR.IP-3

11.4.9	All rules **must** be linked to a formal change reference so that it is possible to cross refer to the change record and identify the approver.	PR.IP-1, PR.IP-3
11.4.10	The use of the rule "ANY" (or any term representing *all traffic*) **must** be avoided for source address, destination address or port number unless authorised as an agreed exception. Overly permissive access **must** be avoided wherever possible.	PR.IP-1, PR.PT-3
11.4.11	Expiry dates **must** be added to temporary rules. These **must** be reviewed regularly to ensure they are removed within the timescales specified. The removal of temporary rules should be automated where possible.	PR.IP-1, PR.PT-3
11.4.12	Major project changes **must** be accompanied by a review of the associated firewall rules.	PR.IP-1, PR.PT-3
11.4.13	The entire firewall ruleset **must** be reviewed against a suitable security benchmark and/or manufacturer official documentation at least every 6 months to remove redundant rules and check for vulnerable configurations. A hit counter may be used to identify those rules which are not utilised. (This may not apply to DR rules, which may only be tested annually for example).	PR.IP-1, PR.PT-3
11.4.14	If the firewall management tool supports documentation of the rules, then this facility **must** be used. Otherwise, an alternative method **must** be used to document the firewall ruleset. All firewall documentation must be centralised and accessible regardless of the specific platform used as firewall. If supported by the management tool, rules can be also documented on the firewall infrastructure, however controls **must** be in place to ensure all information is synced and current.	PR.IP-1
11.4.15	Incoming traffic with a destination address of the firewall itself **should** be blocked unless the firewall is offering services for incoming traffic that require direct connections – for example, if the firewall is acting as an application proxy.	PR.PT-4

11.4.16	The following types of traffic **should** be blocked by the firewall at the perimeter: ▪ Traffic containing IP source routing information, which allows a system to specify the routes that the packets will employ while travelling from source to destination. This could potentially permit an attacker to construct a packet that bypasses network security controls. ▪ Traffic from outside the network containing broadcast addresses that is directed to insider the network. Any system that responds to the directed broadcast will then send its responses to the system specified by the source, rather than to the source system itself. ▪ Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) ▪ Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address)	PR.PT-4
11.4.17	Firewalls at the network perimeter **must** block all incoming traffic to networks and hosts that should not be accessible from external networks. These firewalls **must** also block all outgoing traffic from the Department's network and hosts that should not be permitted to access external networks.	PR.PT-4
11.4.18	Network perimeter firewalls **must** deny all incoming and outgoing traffic by default unless specifically requested under the full change and security approval process.	PR.PT-4, PR.AC-5
11.4.19	For IPsec VPNs, Encapsulating Security Payload (ESP) and Authentication Headers (AH) **must** be blocked at the firewall except to and from specific addresses on the internal network (those addresses that belong to IPsec gateways that are allowed to be VPN endpoints.)	PR.PT-4, PR.AC-5
11.4.20	There **must** be an implicit default deny rule for traffic destined to critical internal addresses from external sources.	PR.PT-4, PR.AC-5

11.5 Firewall Security Audits

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Audit events (which includes admin access, system event, and threat event log data) generated by the firewall infrastructure **must** be forwarded to an Authority approved centralised monitoring tool in line with SS-012 Protective Monitoring Security Standard [Ref. A].	DE.CM-1, PR.PT-1
11.5.2	For the purposes of auditing policies and rulesets, read-only accounts **must** be created only when needed. The account **must** be disabled upon completion of the audits.	PR.PT-1
11.5.3	Legible comments **must** be added to rules to support ruleset auditing, where the firewall supports inline comments.	PR.IP-1
11.5.4	Penetration testing or an ITHC **must** be carried out in addition to regular firewall security audits. This **must** include testing of those controls set out in other parts of this standard – e.g. Section 11.3.	ID.RA-1 PR.IP-7
11.5.5	When Network Address Translation (NAT) functionalities are used, the device **must** report the private address in the logs instead of the translated public address.	PR.PT-4
11.5.6	Audit events (including admin access, system event, and threat event log data) **must** be retained in line with SS-012 Protective Monitoring Security Standard [Ref. A].	PR.PT-1

11.6 Firewall User Access and Authorisation

It is important to implement stringent network-access security and user-permission controls to ensure that only authorised administrators have access to change firewall rules.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	The administration capability **must** support the following: ▪ Identification and authentication of firewall administrators ▪ Trustworthy communication path for administrative traffic - e.g., console-based, encrypted, and separate management network ▪ Remote administration **must** be via strong authentication at appropriate points (e.g., two-factor authentication utilising separate hard tokens) and encrypted channels. See SS-016 Remote Access Security Standard [Ref. B] for further comprehensive measures. ▪ Alert logs **must** be sent to an Authority approved centralised monitoring tool in line with SS-012 Protective Monitoring Security Standard [Ref. A]. ▪ Granular access permissions to enforce the principle of least privilege.	PR.AC-1, PR.AC-6, PR.AC-7, DE.CM-1
11.6.2	All default usernames and passwords on accounts **must** be changed. Where accounts are not needed, they **must** be removed or disabled.	PR.AC-1
11.6.3	Remote administration of firewalls **must** comply with SS-016 Remote Access Security Standard [Ref. B] and implement cryptography in line with SS-007 Use of Cryptography Security Standard [Ref. C].	PR.AC-3
11.6.4	Log in banners/disclaimers **must** present a warning message when a user logs into a firewall device, see Appendix G.	PR.AC-7
11.6.5	Configuration management tools **must** be used to identify deviations against approved baseline configurations.	PR.IP-1, DE.AE-1

11.7 Firewall Architecture

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Use products which are certified through Common Criteria in favour of those that have not. Only use non-certified products where there is no acceptable certified product.	ID.SC-3
11.7.2	All firewalls **must** be synchronised to the Authority Reference (Master) Clock. For cloud-based systems, the cloud providers' time services (provided at the Stratum Level required by the Authority) are sufficient for time reference synchronisation, as the Authority does not have reliable means to share Master Clock data with external parties.	PR.PT-1
11.7.3	Firewalls **must** be physically protected in accordance with the Authority Physical Security Policy [Ref. D]. Any unused ports and interfaces **must** be disabled if not used.	PR.AC-2

11.8 Firewall Maintenance including Patching

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Firewalls **must** be updated and patched in accordance with SS-033 Security Patching Standard [Ref. E].	ID.RA-1 PR.IP-2 RS.MI-3
11.8.2	Vulnerability assessments **must** be conducted on firewalls to assess hardware or software issues. All Internet-facing firewalls **must** be subject to a full IT Health check (ITHC) at least annually.	ID.RA-1, PR.IP-7
11.8.3	The performance of firewall solutions **must** be monitored in accordance with SS-012 Protective Monitoring Security Standard [Ref. A] to ensure that any potential resource issues are identified and addressed. This is necessary as performance degradation may be indicative of an attack.	DE.CM-1
11.8.4	Firewall logs and alerts **must** be monitored in accordance with SS-012 Protective Monitoring Security Standard [Ref. A], to ensure early detection of threats.	DE.CM-1, DE.AE-2
11.8.5	Firewall policies and rules **must** be backed up regularly in accordance with SS-035 Secure Backup and Restore Security Standard [Ref. F]. Backups **should** be taken in both binary and human-readable forms.	PR.IP-4
11.8.6	Firewall Optimisation tools **should** be used to automate reviews of policies and rulesets where possible.	PR.IP-1

11.9 Firewall Types and Specific Measures

Reference	Minimum Technical Security Measures	NIST ID
Application Firewall and Proxy		
11.9.2	Application firewalls must be application aware - e.g. Web Application Firewalls must be capable of detecting attempts to exploit application vulnerabilities such as SQL injection attacks.	PR.PT-3
11.9.3	Application firewalls **must** be capable of terminating TLS connections in order to carry out inspection of application data in the clear, except where certificate pinning is being utilised. This **must** be carried out using back-to-back encrypted data channels between the source and the destination.	PR.DS-2
11.9.4	Application firewalls **must** have the ability to limit threats by exposing a smaller number of identifiable application functions within the proxy.	PR.PT-3
11.9.5	Application firewalls **must** have the ability to carry out anti-virus scanning on the traffic which traverses the firewall, except where certificate pinning is being utilised.	DE.CM-4
11.9.6	Application firewalls **must** be capable of carrying out content inspection - e.g. - protocol analysis - signature based antivirus scanning - investigative analysis (analysing code for malicious characteristics) - sandbox technology (quarantining)	DE.AE-2 DE.AE-5 DE.CM-1 DE.CM-4
Intrusion Detection and Prevention Systems		
11.9.7	Network-based Intrusion Detection and Prevention Systems (NIDPS) **must** be protected from attack by the following means: • NIDPS **should** be deployed on a management network or a virtual management network so that it is concealed from attackers; • All components **must** be kept up-to-date and hardened; • Separate administrator and user accounts for all users; Restrict network access to the NIDPS;	PR.AC-5 DE.CM-1

	• Administrators **must** verify and record that the NIDPS is functioning correctly every 6 months, supported by automated notifications if any issues are detected; • Monitoring and alerting of NIDPS components **must** be via automated tooling; • Configuration settings **must** be backed up in line with SS-35 Secure Backup and Restore Security Standard [Ref. F].	
11.9.8	NIDPS **must** be capable of forwarding logs to a DDA approved centralised monitoring system in accordance with SS-012 Protective Monitoring Security Standard [Ref. A].	PR.PT-1
11.9.9	The NIDPS **must** be capable of detecting or preventing a signature-based attack.	DE.AE-3 DE.CM-4
11.9.10	The NIDPS **must** be capable of anomaly-based detection.	DE.AE-3 DE.CM-4
11.9.11	The NIDPS **must** be capable of protocol-based analysis.	DE.AE-3 DE.CM-4
11.9.12	Wireless NIDPS **must** be capable of identifying suspicious activity relating to wireless protocols.	DE.AE-3 DE.CM-4
11.9.13	NIDPS **should** be capable of Network Based Analysis to detect unusual traffic flows, Denial of Service attacks and malware.	DE.AE-3 DE.CM-4
Virtual Firewall		
11.9.16	The virtual firewall **must** support packet filtering.	PR.PT-4
11.9.17	The virtual firewall **should** support a richer set of firewall functionality such as: • Antivirus • Web filtering • Content filtering • Anti-spam • IDPS • DNS protection • Application firewall • Deep packet inspection • Quarantining • Email analysis • Threat intelligence	PR.PT-4

Host-based Application Firewall		
11.9.18	The host-based application firewall **must** provide socket filtering.	PR.PT-4
11.9.19	The host-based application firewall **should** provide sandboxing - the ability to execute software (particularly untrusted software) in a restricted operating system environment.	PR.PT-4
11.9.20	The host-based application firewall **should** be integrated with a centralised solution such as an IDPS.	PR.PT-4
Authority Controlled Personal Firewalls (e.g. engineering, cloud first, link2, or mobile devices)		
11.9.21	Personal firewalls **must** support stateful filtering	PR.PT-4
11.9.22	Personal firewalls **must** support application firewalling - e.g., access control based on the applications or services launched.	PR.PT-4
11.9.23	Personal firewalls **should** be managed centrally	PR.PT-4

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-1	Physical devices and systems within the organization are inventoried	11.1.2
ID.AM-4	External information systems are catalogued	11.2.4, 11.2.5
ID.RA-1	Asset vulnerabilities are identified and documented	11.2.2, 11.3.1,11.3.3, 11.3.4, 11.4.3, 11.4.8, 11.5.4, 11.8.1, 11.8.2
ID.RA-6	Risk responses are identified and prioritized	11.4.3
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	11.7.1
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.6.1, 11.6.2
PR.AC-2	Physical access to assets is managed and protected	11.7.3
PR.AC-3	Remote access is managed	11.6.3
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.3, 11.4.5
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.4.2, 11.4.18, 11.4.19, 11.4.20, 11.9.7
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.6.1
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)	11.6.1, 11.6.4
PR.DS-2	Data-in-transit is protected	11.9.3
PR.DS-5	Protections against data leaks are implemented	11.3.2, 11.4.2, 11.4.5

PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	11.2.1, 11.2.3, 11.4.1,11.4.9, 11.4.10, 11.4.11, 11.4.12, 11.4.13, 11.4.14, 11.5.3, 11.6.5, 11.8.6
PR.IP-2	A System Development Life Cycle to manage systems is implemented	11.3.2, 11.4.3
PR.IP-3	Configuration change control processes are in place	11.1.4, 11.2.1, 11.2.3, 11.4.8, 11.4.9
PR.IP-4	Backups of information are conducted, maintained, and tested	11.8.5
PR.IP-7	Protection processes are improved	11.2.2, 11.3.1, 11.3.3, 11.3.4, 11.5.4, 11.8.2
PR.IP-12	A vulnerability management plan is developed and implemented	11.8.1
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.5.1, 11.5.2, 11.5.6, 11.7.2, 11.9.8
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.3.2, 11.4.1, 11.4.10, 11.4.11, 11.4.12, 11.4.13, 11.9.2, 11.9.4
PR.PT-4	Communications and control networks are protected	11.1.1, 11.1.5, 11.4.2, 11.4.4, 11.4.6, 11.4.15, 11.4.16, 11.4.17, 11.4.18, 11.5.5 11.4.19, 11.4.20, 11.5.5, 11.9.16, 11.9.17, 11.9.18, 11.9.19, 11.9.20, 11.9.21, 11.9.22, 11.9.23
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	11.6.5
DE.AE-2	Detected events are analyzed to understand attack targets and methods	11.8.4, 11.9.6
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.9.9, 11.9.10, 11.9.11, 11.9.12, 11.9.13
DE.AE-5	Incident alert thresholds are established	11.9.6
DE.CM-1	The network is monitored to detect potential cybersecurity events	11.4.2, 11.4.7, 11.5.1, 11.6.1, 11.8.3, 11.8.4, 11.9.6, 11.9.7
DE.CM-4	Malicious code is detected	11.9.5, 11.9.6, 11.9.9, 11.9.10, 11.9.11, 11.9.12, 11.9.13
DE.CM-8	Vulnerability scans are performed	11.4.3

RS.AN-5	Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	11.4.3
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	11.4.3, 11.8.1

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*
A	SS-012 Protective Monitoring Security Standard	Yes
B	SS-016 Remote Access Security Standard	Yes
C	SS-007 Use of Cryptography Security Standard	Yes
D	DWP Physical Security Policy	Yes
E	SS-033 Security Patching Standard	Yes
F	SS-035 Secure Backup and Restore Security Standard	Yes
G	Security Assurance Strategy	No
H	SS-036 Sanitisation and Destruction Security Standard	Yes
I	SS-006 – Security Boundaries	Yes

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

External Documents List
CIS Critical Security Controls v8 controls set
NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

Appendix D. Abbreviations

Table 5 - Abbreviations

Abbreviation	Definition
AH	Authentication Headers
CSF	Cyber Security Framework
DDA	Digital Design Authority
DMZ	Demilitarised Zone
ESP	Encapsulating Security Payload
IP	Internet Protocol
ITHC	IT Healthcheck
NAC	Network Access Control
NIDPS	Network-based Intrusion Detection and Prevention Systems
NIST	National Institute of Standards and Technology
OS	Operating System
PII	Personally, Identifiable Information
RDP	Remote Desktop Protocol
SIEM	Security Incident Event Management
SP	Special Publication
SSH	Secure Shell
TLS	Transport Layer Security
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

Appendix E. Glossary

Table 6 - Glossary

Term	Definition
Stateless Packet Filtering Firewall	Stateless Packet Filtering Firewalls must be able to make a decision whether to allow or deny a packet based on data within the packet - e.g., Source and destination IP address Payload the packet is carrying - e.g. TCP, UDP or ICMP Source and destination port for the packet Time of packet departure and arrival Network interface card departure and arrival.
Stateful Packet Filtering Firewall	Stateful Packet Inspection Firewalls carry out the same function as Stateless Packet Filtering Firewalls but are also capable of retaining context regarding previous packets in the dialogue. This enables more subtle decisions to be made.
Application Firewall and Proxy	A firewall capability that combines lower-layer access control with upper layer-functionality, and includes a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other.
Personal Firewall	Personal firewalls are similar to host-based firewalls except that they are deployed onto personal computers rather than servers. They provide an additional layer of security against network-based attacks. These firewalls are software-based, residing on the computers they are protecting—each monitor and control the incoming and outgoing network traffic for a single PC or laptop.
Host-based Application Firewall	A host-based application firewall can monitor any input, output and system service call made from or to an application. This is done by examining information passed through system calls. A host-based application firewall can only provide protection to applications running on the same host.
Unified Threat Management	Unified Threat Management Firewalls consolidate a number of functions from a varied set of network products and enable them to be delivered as an integrated solution.

Next Generation Firewall	A third generation firewall technology, designed to address advanced security threats at the application level through intelligent, context-aware security features, combining the ability to filter packets based on applications and to inspect the data contained in packets (rather than just their IP headers). It operates at up to layer 7 (the application layer) in the OSI model, whereas previous firewall technology operated only up to level 4 (the transport layer).
Virtual Firewall	A virtual firewall is a network firewall service or appliance running entirely within a virtualised environment. The virtual firewall can be realised as a software firewall on a guest VM, a purpose-built virtual security appliance, a virtual switch or a managed kernel process running within a hypervisor. A virtual firewall operates in two different modes: Bridge mode: Like a traditional firewall, this mode operates by monitoring all incoming and outgoing traffic bound for other virtual networks or machines. Hypervisor mode: This mode is isolated from the actual network, resides in the hypervisor and monitors the virtual host machine's incoming and outgoing traffic.
Protect Surface	A protect surface is the inverse of the attack surface: It is the catalogue of all assets requiring protection, rather than a record of all possible avenues of attack.

Appendix F. Accessibility artefacts
A variety of accessibility guidance is available from the below URL, that includes:

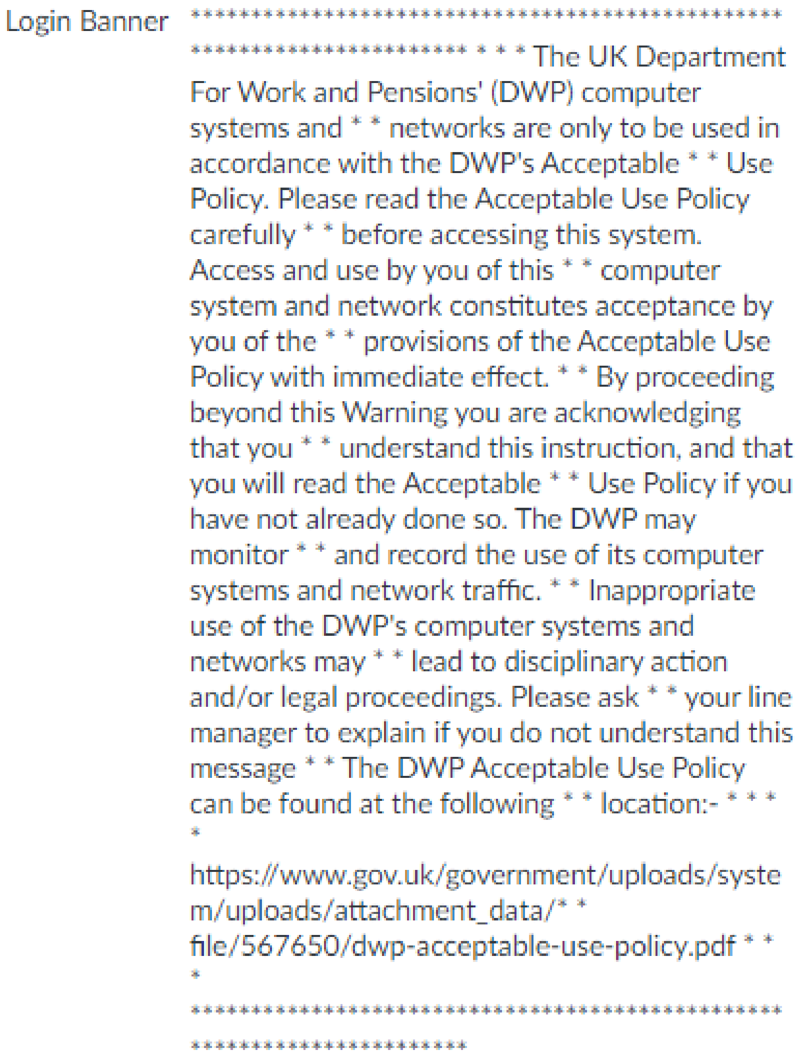
DWP Digital Accessibility Policy | DWP Intranet

https://accessibility-manual.dwp.gov.uk/

Guidance and tools for digital accessibility - GOV.UK (www.gov.uk)

Understanding accessibility requirements for public sector bodies - GOV.UK (www.gov.uk)

Appendix G. Login Warning Message



Login Banner

****
*********************** * * * The UK Department For Work and Pensions' (DWP) computer systems and * * networks are only to be used in accordance with the DWP's Acceptable * * Use Policy. Please read the Acceptable Use Policy carefully * * before accessing this system. Access and use by you of this * * computer system and network constitutes acceptance by you of the * * provisions of the Acceptable Use Policy with immediate effect. * * By proceeding beyond this Warning you are acknowledging that you * * understand this instruction, and that you will read the Acceptable * * Use Policy if you have not already done so. The DWP may monitor * * and record the use of its computer systems and network traffic. * * Inappropriate use of the DWP's computer systems and networks may * * lead to disciplinary action and/or legal proceedings. Please ask * * your line manager to explain if you do not understand this message * * The DWP Acceptable Use Policy can be found at the following * * location:- * * * * https://www.gov.uk/government/uploads/system/uploads/attachment_data/* * file/567650/dwp-acceptable-use-policy.pdf * * *
****
****