Security Standard – Network Security Design (SS-018)

Chief Security Office

Date: 19/12/2023

Department for Work & Pensions

The Network Security Design 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 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	18/09/17
1.1		Document updated to include sections on Risk Management and Network Security Architecture. Authority Control References included. A small number of duplicate requirements have been removed.	14/01/19
1.2		Incorporated comments from Security Architecture Team review.	30/01/19
1.3		Following external review by Security Policy, Risk and Digital	04/03/19
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 11.1.1 NCSC Secure Design 11.1.3 & 11.1.5 Network diagrams 11.1.6 Added external reference 11.1.7 RFC1918 and ASNs 11.1.11 private network 11.1.12 Hardened; added external reference 11.1.16 Major network components; red team exercises 11.1.17 In vendor support 11.1.19 Change Mgmt processes 11.1.22 Master Clock 11.2.3 Network requirements instead of underlying transport mechanism 11.2.6 Added risk consideration to purchasing decisions 11.3.2 Encryption 11.3.3 Unused and interface ports 11.4.2 No multi-function servers 11.4.4 Disable unused ports 11.5.1 Security appliance 11.5.2 Reverse proxy server	

		11.5.3 External attack service management 11.5.4 cert-pinned traffic 11.6.1 Security appliances 11.6.2 Modern firewalls 11.6.3 Added ref to firewall standard 11.6.5 must; traffic with different security profiles 11.6.8 Added ref to security boundaries standard 11.8 Intrusion Detection and Prevention 11.10.1 Usernames 11.11.3 & 11.11.4 Security appliances 11.11.5 & 11.11.6 Access Controls 11.11.7 Security appliances 11.12.1 Native encryption 11.12.2 Encrypted 11.12.3 Network mgmt. systems 11.12.8 Point to point 11.12.9 Resilient 11.13.1 Physical or virtualised 11.14.2 Access controls 11.14.4 Usernames 11.14.6 In vendor support 11.16.2 Security appliances; network access control or authentication servers 11.17.1 TPM hardware 11.17.3 & 11.17.4 subject to authorised exceptions 11.17.9 Additional security controls 11.17.10 Internal 11.17.14 Portable media prohibited 11.18.1 native logging and alerting capabilities 11.18.3 Security appliances 11.18.8 Added ref to Protective Monitoring standard	

3. Approval history

Version	Approver	Role	Date
1.0		Chief Security Officer	18/09/17
1.1		Chief Security Officer	14/01/19
1.2		Chief Security Officer	30/01/19
1.3		Chief Security Officer	04/03/19
2.0		Chief Security Officer	19/12/2023

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. R].
- 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 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 Requirements

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 network security design 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:

- Enable technical teams to work towards a set of baseline security measures that are based on industry best practice.
- Ensure networks and network security controls are designed, deployed, and managed consistently across the Authority and supplier base where applicable.
- Ensure network security controls provide effective mitigation against physical and logical threats.
- support the achievement of security outcomes described in Appendix A.

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

All of the Authority's network infrastructure (on-premise and in the cloud) are in scope of this standard, this includes Authority LANs, WANs and networking hardware/software that enables computing and communication between users, services applications and processes.

This standard is also applicable to supplier networks which deliver systems and services on behalf of the Authority.

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

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 Network Security Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	The following design principles **must** be considered: • Provide for defence-in-depth – create layered security controls such that, if one control fails, other controls will protect valuable assets • Keep solutions simple – the objective of the design process is to produce the simplest possible outcome. Simple solutions are easier to describe and most likely to be reliable, deliverable and maintainable. • Reduce Attack Surface - every feature that is added to an application adds a certain amount of risk to the overall application. The aim for secure development is to reduce the overall risk by reducing the attack surface area. • Fail securely - When a system fails, it should do so securely. This typically involves several things: secure defaults (default is to deny access); on failure undo changes and restore to a secure state; always check return values for failure; and in conditional code/filters make sure that there is a default case that does the right thing. The confidentiality and integrity of a system should remain even though availability has been lost. Attackers must not be permitted to gain access rights to privileged objects during a failure that are normally inaccessible. Upon failing, a system that reveals sensitive information about the failure to potential attackers could supply additional knowledge for creating an attack. Determine what may occur when a system fails and be sure it does not threaten the system. NCSC secure design principles may also be considered to augment those above, https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles [see External References].	PR.AC-5 PR.PT-4

11.1.2	Network Security Design **must** include the following inputs: • The Authority’s documented service requirements • Documentation of any planned architecture, design and implementation • Current network security policy (or relevant parts of the information security policy) preferably based on a risk assessment combined with a management review • Definition of the assets that should be protected • Current and planned performance requirements • Current information regarding the products which implement the network infrastructure	PR.AC-5 PR.PT-4
11.1.3	Network Security Design **must** include the following outputs: • The network technical security architecture; • Service access requirements for each of the security gateways (including firewall rulesets); • Network diagrams showing security enforcing controls; • Security operating procedures; • Conditions for secure connection of third parties; • User guidelines for third parties	PR.AC-5 PR.PT-4
11.1.4	The Network Security Design **must** consider the following scenarios: • Internet access for employees • Enhanced collaboration services • Business to business services • Business to customer services • Outsourced services • Network segmentation (segregation) • Mobile communication • Networking support for travelling users • Networking support for home users	PR.AC-5 PR.PT-4

11.1.5	Technical documentation (including up to date network diagrams) **must** be developed and maintained describing the current network and any planned changes to the network. This **must** be sufficiently detailed to describe connections and services.	PR.IP-1 ID.AM-4
11.1.6	Network devices and supporting network infrastructure (including servers and switches) **must** be hardened (in accordance with the relevant security standards and patterns) to avoid unauthorised access and compromise - this should include the use of secure protocols, disabling unused services, limiting access to necessary ports and protocols and the enforcement of authentication and access control where appropriate. [see External References].	PR.IP-1
11.1.7	The enterprise network IP address range **must** be 'non-routable' from the Internet i.e. using NAT, in line with RFC 1918 [see External References]. In addition, there are some addresses (e.g. ex-GSI/PSN) that are currently non-routable, but which might be added to internet Autonomous System Numbers in the future which it would be better not to use.	PR.PT-4
11.1.8	All configuration details of network devices (e.g. IP address) **must** be registered against the Authority CMDB or asset repository.	PR.IP-1 ID.AM-3
11.1.9	Traffic routing **must** be identified during design to avoid transiting insecure network environments.	ID.AM-3
11.1.10	Warning banners or disclaimers **must** be displayed to enforce legal and regulatory requirements. These **must** be presented on privileged and normal user access accounts.	PR.AC-7
11.1.11	Remote access into the Authority private network **must** be in accordance with SS-016 Remote Access Security Standard [Ref. A].	PR.AC-3 PR.PT-4

11.1.12	Network services including Domain Name System (DNS), Network Time Protocol (NTP) and Dynamic Host Configuration Protocol (DHCP) **must** be hardened in accordance with manufacturer and industry best practices or in accordance with relevant standards/patterns [see External References].	PR.IP-1
11.1.13	Network configurations **must** be audited at least annually (or sooner after significant changes) and include network asset scanning. These checks **must** reference against group policy and network configuration rule-base(s).	PR.IP-7 DE.CM-8
11.1.14	Access to network configuration including backup, authentication databases and administrative services **must** only be available to authorised personnel. The network configuration **must** be protected from unauthorised modification.	PR.AC-4
11.1.15	The network infrastructure **must** be subject to formal change control processes, this process should link to CMDB management.	PR.IP-3
11.1.16	Major network infrastructure components **must** be subject to a regular IT health check (ITHC) on a rolling basis, or at the point of major change or following changes that may have a significant effect on the network security controls. This is required to ensure that network security posture has not been weakened by the change. Red Team exercises may also be conducted where required, as per SS-027 Security Testing Standard [Ref. S].	ID.RA-1 ID.SC-4
11.1.17	Network components, applications and services **must** be in vendor support, maintained (updated and patched) in accordance with the SS-033 Security Patching Standard [Ref. B] and DWP Technical Vulnerability Management Policy [Ref. C].	ID.RA-1 PR.IP-12
11.1.18	The network **must** meet availability requirements (in accordance with the SLA requirement for that part of the network). It **should** be designed to minimise single point of failures.	ID.BE-4 PR.PT-4

11.1.19	Networking equipment **must** not be disconnected or removed without explicit authorisation, and in line with change management processes.	PR.MA-1
11.1.20	Security incident management plans and procedures **must** be implemented for the network in accordance with the Security Incident Management Policy [Ref. D].	PR.IP-9
11.1.21	Routing sessions **must** be restricted to trusted peers and the origin and integrity of routing updates **must** be validated. This should include authenticating all routing peers and disabling routing on all unauthorised interfaces by default.	ID.AM-3
11.1.22	All network devices **must** be synchronised to the Authority Reference (Master) Clock so that its timestamp matches to those generated by other systems. NTP protocol **must** be used to synchronise log source time with the Authority Master Clock, in line with SS-012 Protective Monitoring Security Standard [Ref. M]. For cloud based systems, the cloud providers' time services 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

11.2 Risk Management

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Documentation **must** be available to describe the current network and planned changes to the network. This **must** be sufficiently detailed to describe connections and services and form a basis for consideration of network-related risks	ID.RM-1
11.2.2	Characterise the network on the basis of the community of users: - Unknown community of users - A known community of users from a closed business community comprising members from more than one organisation Then consider whether they are using a public or private network.	ID.RA-4
11.2.3	Consider the type of network: data, voice or hybrid. Also consider network requirements such as bandwidth, loss, latency, jitter etc.	ID.RA-3
11.2.4	Collect other information to scope the network security design, as follows: - Information types - Business processes - Actual or potential hardware components; software, services and connections - Potential environments (locations and facilities) - Activities (Operations)	ID.RA-3
11.2.5	The network security design **must** take account of the following types of risks; Loss of; - Confidentiality of information and code - Integrity of information and code - Availability of information and network services - Non-repudiation of network transactions - Authenticity of information, users and administrator - Reliability of information and code - Ability to control unauthorised use of information and resources	ID.RA-4

11.2.6	Network products and services **must** be purchased through a process where security is one of the evaluation criteria. They **must** not be purchased if the risks of adoption are outside risk appetite and, in those situations where the evaluation team have major reservations, every effort **must** be made to choose more secure alternatives.	ID.RM-2 ID.RM-3

11.3 Physical Security

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	All network devices **must** be secured in an area with physical access controls in accordance with the Authority's Physical Security Standards as appropriate. For example, with the use of secure rooms and lockable cabinets.	PR.AC-2
11.3.2	Network devices (including network cabling) **must** be physically protected to the same level as the data they are processing/handling on a daily basis. If physical cabling cannot be protected to the same level then data **must** be encrypted to Authority standards over the physical cabling.	PR.AC-2
11.3.3	Hardware ports in networking equipment **must** be additionally protected where appropriate to deter unauthorised connections. Unused ports **must** be disabled if not removed; Interface port status **must** generate alerts if changed.	PR.AC-2
11.3.4	Ingress and egress to secure areas where network devices reside **must** be protected by appropriate entry controls and monitored using surveillance.	PR.AC-2

11.4 Network Security Architecture

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	The Network Security Architecture **must** support and utilise the following security dimensions: • Access control • Authentication • Non-repudiation • Data confidentiality • Communication security • Data Confidentiality, Integrity & Availability • Privacy • Logging and monitoring	PR.AC-5 ID.AM-3 PR.PT-5
11.4.2	Servers **must** be separated by function during the design and implementation of networks. Multi-function servers **must** not be utilised.	PR.AC-5
11.4.3	The Network Security Design **must** define the roles and responsibilities which relate to network security.	PR.AT-2
11.4.4	The following steps **must** be taken to secure infrastructure devices where applicable: • The accessible ports and access services **must** be limited. Unused ports **must** be disabled • Access to authorised services **must** be restricted from authorised originators only. • Session management **must** be enforced (e.g. enforce idle timeouts, time to live) • Vulnerability to dictionary and DoS attacks **must** be minimised (e.g. Limit the rate of login attempts, Restrict the maximum number of concurrent sessions, enforce a lockout period upon multiple authentication failure attempts, enforce the use of strong passwords, log and monitor user login authentication failures)	PR.IP-1 PR.PT-3

	• Access **must** only be granted to authenticated users, groups, and services in line with SS-001 pt.1 Access & Authentication Security Standard [Ref. F] • The principle of least privilege **must** be adopted for all authorised users in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. E] • Deny outgoing access unless explicitly required • There **must** be role based access control to limit the function the user is permitted to perform.	

11.5 Network Perimeter Requirements

Network perimeter controls **must** be deployed in accordance with SS-006 Security Boundaries Security Standard [Ref. H]. The following controls are the principal, best practice requirements required to secure an external physical network perimeter from outside networks.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	A security appliance (physical or virtual) **must** be deployed between the internet and the perimeter network configured to filter out unsolicited network connections and untargeted attacks, such as port scans.	PR.AC-5
11.5.2	Incoming web browsing, email and media streaming traffic **must** pass through some form of reverse proxy server in the perimeter network before being allowed onto the internal network. The reverse is also true for outcoming traffic. See SS-006 Security Boundaries Security Standard [Ref. H] for further details.	PR.AC-5 PR.DS-5 PR.PT-4 DE.CM-1

11.5.3	Devices in the perimeter network are more vulnerable to attack and so each **must** be configured to run the minimum number of services, supported by external attack service management where available, and their operating systems and applications hardened in accordance with SS-008 Server Operating System Security Standard [Ref. P].	PR.PT-3
11.5.4	There **must** be signature-based and reputation-based malware scanning and URL filtering in place to examine both inbound and outbound data at the perimeter in addition to protection deployed internally (in accordance with SS-015 Malware Protection Security Standard [Ref. Q]). Using different antivirus and malware solutions is good practice to protect the Authority's private network and systems in order to provide additional defence in depth. Due consideration must be made for certificate-pinned traffic, that may not be able to meet this requirement.	DE.CM-4

11.6 Network Segregation

In addition to the below requirements, boundaries between the security zones should conform to the requirements within the SS-006 Secure Boundaries Security Standard [Ref. H].

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Internal security appliances (physical or virtual) **must** be configured with filtering rules to enforce segregation between different segments of the network. For example, desktops in one segment **must** not be permitted to connect to those in another segment unless there is a business need.	PR.AC-5
11.6.2	Modern firewalls (i.e. those with additional security features) **must** be deployed between clients and services and/or between boundaries of each site. Note. Layer 3 firewalls only protect against network layer attacks, not against application layer attacks.	PR.AC-5

11.6.3	Firewalls **must** be configured with rules to define what form of network connections are allowed through (in both directions). Rulesets must be developed and configured to only allow network connections that support the business function. See SS-013 Firewall Security Standard [Ref. I] for more information.	PR.AC-5 PR.PT-4
11.6.4	Segregation **must** be maintained between development, training, and the live environments.	PR.DS-5 PR.IP-2 PR.PT-3
11.6.5	VLANs do not by themselves provide an appropriate level of protection, they **must** not be used as a means to provide separation of traffic with different security profiles, but may be used to separate traffic with the same security profile.	PR.AC-5
11.6.6	Training environments **must** be afforded the same level of security (primarily through access controls and auditing) as the level of data they are handling.	PR.AC-5
11.6.7	Where dummy or anonymous data is used in training environments, the use of generic training accounts is acceptable but the requirement to appropriately separate the training environment from the live system **must** remain.	PR.DS5 PR.IP-2 PR.PT-3
11.6.8	Networks of different risk profiles **must** be located in different security zones: • Devices and computer systems providing services for external networks (e.g., the Internet) **must** be located in different zones (De-Militarized Zone – DMZ) than internal network devices and computer systems. • Application or data assets with higher protective requirement **must** be located in dedicated security zones. • Devices and computer systems of low trust level such as remote access servers and wireless network access points **must** be located in dedicated security zones Please refer to SS-006 Security Boundaries Security Standard [Ref. H] for more information.	PR.AC-5

11.6.9	Networks of different types **must** be located in separate security zones: • User workstations **must** be located in different security zones than servers • Network and security management systems **must** be located in dedicated security zones • Systems in development stage **must** be located in different zones than production systems.	PR.AC-5
11.6.10	Network segmentation **must** be used to: • segregate administrative and maintenance capabilities from routine user access to business applications • segregate applications with higher protective requirements from other applications • segregate databases from ordinary users who do not have business requirements for access.	PR.AC-5
11.6.11	Where there is a shared WAN backbone, Authority private network WAN traffic **must** be separated from other traffic that may be on the WAN to enable the confidentiality and integrity of data.	PR.AC-5

11.7 Wide Area Network (WAN)

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	WAN network domains **must** be secured against attacks. For example, to protect against Layer 3-based network attacks this could include device hardening, anti-spoofing filtering, routing protocol security, protective monitoring, firewalls, and intrusion prevention systems.	PR.AC-5 PR.PT-4
11.7.2	There **must** be data/file integrity verification using algorithms such as hash/checksums, certificates, validating all critical device configurations on the WAN network.	PR.AC-5 PR.DS-6

11.8 Intrusion Detection and Prevention Systems

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Intrusion detection and prevention systems (IDPS) **must** be deployed on appropriate areas of the network (e.g. network boundary, and significant critical applications).	DE.CM-1
11.8.2	An IDPS service **must** be deployed on the links to/from the Authority's private network and external networks. Hosts that are detected via the rule set **must** be automatically blocked from further network access until the cause of the detection is understood and remediated.	DE.CM-1
11.8.3	The IDPS configuration **must** be reviewed at least once a year or sooner where significant changes are made to the configuration.	DE.DP-5
11.8.4	Anti-virus and host based security systems **must** be deployed on perimeter devices (where supported) to monitor malicious behaviour.	DE.CM-4

11.9 Anti-spoofing

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Anti ARP-spoofing technologies **must** be deployed at edge network devices.	DE.AE-1
11.9.2	Features that support DHCP/ARP snooping on network devices **must** be enabled where supported.	DE.AE-1
11.9.3	Route filters **must** be used at the border between the Authority's private network and networks controlled by others to prevent false routing information from being injected.	ID.AM-3 PR.AC-5 PR.PT-4

11.10 Passwords

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	Default administrative usernames and passwords for network equipment **must** be changed or disabled and default accounts removed. Authentication credentials **must** not be shared between users or devices. See SS-001 pt.2 Privileged User Access Security Standard [Ref. E].	PR.AC-1
11.10.2	Passwords **must** be set in accordance with SS-001 pt.1 Access and Authentication Security Standard [Ref. F].	PR.AC-1

11.11 Authentication and Access Lists

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Administrator access to any network component **must** use multi-factor authentication and strong authorisation controls. Refer to SS-001 pt.2 Privileged User Access Security Standard [Ref. E].	PR.AC-7
11.11.2	Any error messages returned to enterprise or external systems, or users **must** not include sensitive information that may be useful to attackers.	PR.AC-7
11.11.3	Security appliances (physical or virtual) **must** be deployed between the client network and any management network.	PR.AC-5
11.11.4	Security appliances (physical or virtual) **must** be deployed to limit access to known and trusted IP addresses only.	PR.AC-5
11.11.5	Access controls **must** be deployed on every router to prevent any compromise of the internal network (primarily from ICMP redirects).	PR.AC-5
11.11.6	Access controls **must** be deployed to restrict SNMP access to specific hosts.	PR.AC-5
11.11.7	Deploy security appliances (physical or virtual), where appropriate, to limit access to known and trusted communication partners.	PR.AC-5
11.11.8	The network **must** be designed to provide authentication and access controls for systems connecting to them. Unauthorised or non-compliant devices **must** be placed in a quarantine area where remediation can occur prior to gaining access to the network.	PR.AC-7

11.12 Network Management

Reference	Minimum Technical Security Measures	NIST ID
11.12.1	To avoid clear text traffic, secure protocols (SSH, SNMPv3, TLS, HTTPS) **must** be used for all sensitive management interfaces and network devices where cryptographic protection is not natively supported. See DWP Approved Cryptographic Algorithms workbook [Ref. G].	PR.DS-2
11.12.2	Management traffic **must** be separated from normal user traffic and encrypted.	PR.DS-2
11.12.3	Network device management interfaces **must** only be accessible through network management systems.	PR.AC-5
11.12.4	Any console ports used for device management **must** be secured by a username/password or other Authority approved authentication method.	PR.AC-7
11.12.5	In the case of remote management of a network device or communication link, you **must** ensure that the management information only flows between the management host and the network devices or communication links that are being managed.	PR.AC-3 PR.MA-2
11.12.6	Configuration information of network devices and communication links **must** be protected against unauthorised modification, deletion, creation, and replication.	PR.AC-5
11.12.7	Steps **must** be taken to ensure management access to network devices or communications links remain accessible in the event of a cyber-attacks e.g. Denial of Service.	PR.PT-4
11.12.8	Control information being transported across the network (e.g. routing updates) **must** flow between the source of the control information and its desired destination, i.e. point to point.	PR.DS-2

11.12.9	Network devices **must** be resilient to always be available to receive control information from authorised sources. This includes protection against deliberate attacks such as Denial of Service (DoS) attacks and accidental occurrences e.g. route flapping.	PR.PT-4
11.12.10	Management access to infrastructure devices **must** be secured. This includes: • Restricting access to authorised terminal and management ports • Restricting access to authorised services and protocols only • Only granting access to authenticated and authorised users	PR.AC-2 PR.AC-4 PR.AC-7
11.12.11	The management network access **must** be deployed using the following best practices: • Enforce access control using a management boundary firewall; • Classify and prioritize management traffic; • Provide network isolation; • Enforce the use of encrypted, secure access, and reporting protocols	PR.AC-5
11.12.12	User privileges **must** be restricted to only those functions required by the individual user to perform their role in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. E].	PR.AC-4

11.13 Data Centre

Reference	Minimum Technical Security Measures	NIST ID
11.13.1	There **must** be separate physical or virtualised external security boundary controls to inspect ingress/egress traffic to the data centre (configured in accordance with SS-006 Secure Boundaries Security Standard [Ref. H]).	PR.PT-4
11.13.2	There **must** be a firewall for datacentre ingress and egress traffic. The firewall **must** be implemented in accordance with SS-013 Firewall Security Standard [Ref. I].	PR.PT-4
11.13.3	The use of shared, virtualised network, server and storage infrastructure to host applications and databases containing Authority data **must** be in compliance with SS-025 Virtualisation Security Standard [Ref. J]	PR.PT-4
11.13.4	Security controls deployed on virtualised networks, server, storage machines and other virtualised network components **must** be commensurate to their physical counterparts.	PR.PT-1 PR.PT-2
11.13.5	A separate services segment is required which can offer firewalling, application delivery scanning/control and additional security inspection capabilities to the hosting segments as appropriate.	PR.AC-5
11.13.6	There **must** be clear demarcation between different hosting segments enabling them to be supported independently.	PR.AC-5 PR.MA-1
11.13.7	All traffic **must** be denied by default. Traffic may only be allowed from explicitly authorised sources, and may only be forwarded to an authorised destination on the core Data Centre network.	PR.PT-5
11.13.8	The Data Centre **must** provide the ability for applications and data to be hosted in separate hosting segments to provide segregation of data and to control interactions between them.	PR.AC-5

11.13.9	Segregated network, compute and storage facilities **must** be provided to manage and monitor the Data Centre infrastructure.	PR.AC-5
11.13.10	Infrastructure and application "Call Home" data flows (i.e. for updating) **must** be subject to risk assessment for protocol break and inspection in transit across boundaries with untrusted networks.	ID.RA-1 DE.AE-1

11.14 Storage Area Networks (SANs) and Network Attached Storage (NAS)

Reference	Minimum Technical Security Measures	NIST ID
11.14.1	Any storage media in use in a SAN or NAS **must** be classified at the highest level of classification applied to the data stored on it (including data that's been stored in the past).	PR.DS-1
11.14.2	Firewalls **must** be deployed to protect storage devices from users on the network they serve and/or setting access controls on the devices to enforce further separation.	PR.AC-4
11.14.3	SAN/NAS devices **must** be locked down by removing all non-essential services, and strictly limiting access to user accounts.	PR.AC-4
11.14.4	Default usernames and passwords on devices in the SAN/NAS **must** be changed, and where available, secure authentication protocols **must** be used. In addition, test accounts **must** be removed.	PR.AC-7
11.14.5	Separate SAN/NAS management network **must** be established to provide separation from the SAN/NAS data network.	PR.AC-5
11.14.6	SAN/NAS OS software (and web interface, where present) **must** be in vendor support and kept updated in accordance with SS-033 Security Patching Standard [Ref. B].	PR.DS-1

11.14.7	If a SAN is being implemented using fibre channel (FC), then the following controls **must** be implemented: • Any unnecessary accesses, ports or services **must** be appropriately locked down (i.e. set/configure FC switch ports, zones (subsets of servers and storage arrays), Logical Unit Number (LUN) masks, and any present proprietary access control mechanisms (such as virtual SANs)) • An assured secure authentication mechanism **must** be used between all FC devices (servers, switches and storage arrays) and make the authentication mutual • Data-in-transit and all communications between FC devices **must** be encrypted in line with SS-007 Use of Cryptography Security Standard [Ref. K].	PR.AC-7 PR.DS-2 PR.PT-4

11.15 Service Resilience

Reference	Minimum Technical Security Measures	NIST ID
11.15.1	The Data Centre **must** have resilient diverse communications. In the event of a power failure, there **must** be provision to maintain continuity of power supply.	ID.BE-5
11.15.2	Core network equipment **must** be attached to an appropriately designed UPS and generator system.	ID.BE-5
11.15.3	Device, link, and geographical diversity **must** be deployed to eliminate single points of failure.	ID.BE-5
11.15.4	WAN resources **must** be protected from exhaustion attacks	ID.BE-5 PR.PT-4

11.16 Wireless Security

Reference	Minimum Technical Security Measures	NIST ID
11.16.1	All new wireless network devices **must** support Authority approved encryption methods in line with SS-007 Use of Cryptography Security Standard [Ref. K].	PR.DS-2
11.16.2	In wireless solutions, security appliances (physical or virtual) **must** be used to restrict access to the network access control or authentication servers, including file and print servers.	PR.AC-5
11.16.3	Wireless Networking **must** be in line with SS-019 Wireless Networking Security Standard [Ref. L].	PR.IP-5

11.17 Virtual Private Networks (VPN)

Reference	Minimum Technical Security Measures	NIST ID
11.17.1	Certificate authentication **must** be used where supported. Private keys **must** be stored in hardware-protected storage (such as a Trusted Platform Module [TPM] using a TPM 2.0 hardware chip for example) if possible.	PR.AC-7 PR.DS-1
11.17.2	Client certificate for machine authentication **must** be used when using a VPN.	PR.AC-7
11.17.3	Forced tunnelling **must** be enabled to ensure apps cannot evade monitoring systems, subject to authorised exceptions.	DE.CM-1
11.17.4	Full-device VPN **must** be used where possible to avoid split tunnelling to minimise the risk of data leaking outside the VPN, subject to authorised exceptions.	PR.DS-2

11.17.5	The Authority recommended cryptographic profiles for IPsec or TLS **must** be applied, as appropriate in line with DWP Approved Cryptographic Algorithms workbook [Ref. G].	PR.DS-2
11.17.6	The confidentiality of data and code in transit in the tunnel between trusted and untrusted networks **must** use encryption of the data when it is in transit, to prevent compromise (see SS-007 Use of Cryptography Security Standard [Ref. K]).	PR.DS-2
11.17.7	The mechanisms used to implement the VPN tunnel should support integrity checking of data and code in transit, using techniques such as message verification codes, message authentication codes and anti-replay mechanisms. Integrity protection controls **must** be implemented in the endpoint systems.	PR.DS-6
11.17.8	Integrity of information crossing public IP networks **must** be ensured between participating peers in a VPN.	PR.DS-6
11.17.9	The tunnel establishment and operating process **must** be supported by authorisation controls and should include additional security controls.	PR.AC-1
11.17.10	Security controls to counter internal denial of service attacks which are specific to tunnel mechanisms **must** be incorporated wherever necessary.	PR.PT-4
11.17.11	The VPN solution **must** maintain appropriate security logs for the analysis of all actions at the endpoint in line with SS-012 Protective Monitoring Security Standard [Ref. M].	DE.AE-3 DE.CM-1
11.17.12	In VPN architectures where endpoint obfuscation is a requirement, controls **must** be implemented to mask source and destination locations of VPN users. The chosen solution will have to be approved by the Authority.	PR.PT-4

11.17.13	The VPN **must** be in compliance with all relevant security measures specified in SS-015 Malware Protection Security Standard [Ref. N] and SS-016 Remote Access Security Standard [Ref. A].	PR.DS-5
11.17.14	VPN deployment **must** be controlled e.g. by creating delivery and receipt log(s) and by implementing restrictions on re-use of media such as a date/time expiration or limitation on the number of times an execution can be performed. VPN deployment via portable media such as CD-ROMs, diskettes, etc. is prohibited.	PR.MA-1
11.17.15	The VPN gateway, which terminates any encryption used to protect the link from the endpoint, **must** be located at the security boundary.	PR.PT-4
11.17.16	The VPN gateway **must** mutually authenticate with the device (with prior authentication of user to device having occurred) before allowing access.	PR.AC-7
11.17.17	A VPN gateway **must** be set up by configuring it to the network configuration and port/application access required, installation of certificates (e.g. for Higher Layer VPNs), and continuous network monitoring of the VPN gateway enabled.	PR.DS-5 PR.MA-1
11.17.18	The VPN gateway **must** be protected against network layer attacks (e.g. through the use of firewalls). Ensure that only VPN traffic (nominally identified by destination port and protocol number) reaches the VPN gateway.	PR.PT-4
11.17.19	VPN endpoint **must** be configured to ensure that there is only communications between an always-on VPN and the hosting network.	PR.DS-2
11.17.20	There **must** only be authorised endpoint connectivity to other networks or devices to avoid an uncontrolled device from another network compromising the VPN.	PR.AC-1

11.18 Logging and monitoring

Reference	Minimum Technical Security Measures	NIST ID
11.18.1	All network devices **must** log to an Authority authorised logging/network management system in accordance with SS-012 Protective Monitoring Security Standard [Ref. M]. If network devices have logging and alerting capabilities built in, these **must** be utilised.	PR.PT-1
11.18.2	All network devices **must** be monitored to ensure they can be reached by a centralised monitoring solution.	DE.AE-3 DE.CM-1
11.18.3	Routers **must** be configured to send log messages to a separate syslog server to preserve the messages. Security appliances (physical or virtual) **must** be configured to record whenever they are hit.	DE.AE-3
11.18.4	There **must** be visibility of what is occurring on the network at any given time. This **m**ust include traffic statistics, system utilisation/status information, Syslog, SNMPv3, ACL logging, accounting, archive configuration change logger, packet capture, device access information etc. as appropriate	DE.AE-1 DE.CM-1
11.18.5	Logs **must** be maintained that include the following types of events: • a record of who accessed network infrastructure components, what occurred, and when, • remote failed log-on attempts with dates and times, • failed re-authentication (or token usage) events, • security gateway traffic breaches, • remote attempts to access audit logs, • system management alerts/alarms with security implications (e.g. IP address duplication, bearer circuit disruptions), • configuration control changes including altering permissions for management interfaces and altering routing tables.	PR.PT-1

11.18.6	Neighbour status changes that may indicate network connectivity and stability issues (due to an attack or general operations problems) **must** be detected and logged.	DE.AE-1
11.18.7	Appropriate filters **must** be deployed at WAN edges where invalid routing information may be introduced.	DE.CM-1 DE.DP-2
11.18.8	Switch and network logs **must** be forwarded to a Authority approved centralised monitoring system, and be analysed to detect unauthorised devices, in line with SS-012 Protective Monitoring Security Standard [Ref. M].	DE.AE-3

11.19 Backups

Reference	Minimum Technical Security Measures	NIST ID
11.19.1	The configuration of network equipment **must** be backed up in accordance with SS-035 Secure Backup and Restore Security Standard [Ref. N].	PR.IP-4
11.19.2	Changes to configuration **must** be associated with an authorised decision and tracked in a change record. Changes **must** be impact assessed for effect on security if not implemented.	PR.IP-3
11.19.3	A template of network configuration **must** be maintained to aid disaster recovery.	ID.AM-3
11.19.4	Configuration files and backups **must** be kept on a secure server approved by the Service Owner.	PR.IP-4
11.19.5	Where possible, the live configuration state of the network **should** be checked against a reference copy of it, this process **should** preferably be automated.	PR.IP-9 PR.PT-5

11.19.6	There **must** be regular back up of network configuration, network devices, and other critical servers or devices. Frequency and retention of the backups should be established according to service delivery requirements or otherwise risk assessment advice. The backed up data **must** be protected to the same level as the live devices that the backups reflect. See SS-035 Secure Backup and Restore Security Standard [Ref. N].	PR.IP-4
11.19.7	An offline copy of a security template providing a baseline configuration of the network **must** be maintained and not kept on the network – this is to facilitate recovery after a major outage or security incident.	PR.IP-4 DE.AE-1
11.19.8	Access to configuration backups **must** be restricted to authorised personnel only in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. E].	PR.AC-4

11.20 Secure Sanitisation and Disposal

Please note these requirements do not apply to cloud-based infrastructure for example where configs are not stored on the device.

Reference	Minimum Technical Security Measures	NIST ID
11.20.1	Secure sanitisation and destruction of network devices **must** be treated at the same level as the data these systems processed or handled. Refer to SS-036 Secure Sanitisation and Destruction Security Standard [Ref. O] for further details.	PR.DS-1 PR.DS-3
11.20.2	Network devices that monitor network traffic may retain some of that data, consequently they **must** be sanitised or disposed of in accordance with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. O]	PR.DS-1 PR.DS-3

11.20.3	When network equipment is to be reused, disposed of, or sent for repair outside of the Authority's security management boundary domain all sensitive data **must** be sanitised in accordance with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. O]	PR.DS-1 PR.DS-3
11.20.4	Any storage media used by the SAN or NAS **must** be re-used or destroyed in accordance with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. O]. Media should be sanitised even if it is to be re-used by a different network that is assured to handle data value at the same classification.	PR.DS-1 PR.DS-3

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 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related security measures
ID.AM-3	Organizational communication and data flows are mapped	11.1.8, 11.1.9, 11.1.21, 11.4.1, 11.9.3, 11.19.3
ID.AM-4	External information systems are catalogued	11.1.5
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	11.1.18
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	11.15.1, 11.15.2, 11.15.3, 11.15.4
ID.RA-1	Asset vulnerabilities are identified and documented	11.1.16, 11.1.17, 11.13.10
ID.RA-3	Threats, both internal and external, are identified and documented	11.2.3, 11.2.4
ID.RA-4	Potential business impacts and likelihoods are identified	11.2.2, 11.2.5
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	11.2.1
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	11.2.6
ID.RM-3	The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	11.2.6

ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	11.1.16
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.10.1, 11.10.2, 11.17.9, 11.17.20
PR.AC-2	Physical access to assets is managed and protected	11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.12.10
PR.AC-3	Remote access is managed	11.1.11, 11.12.5
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.14, 11.12.10, 11.12.12, 11.14.2, 11.14.3, 11.19.8
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.4.1, 11.4.2, 11.5.1, 11.5.2, 11.6.1, 11.6.2, 11.6.3, 11.6.5, 11.6.6, 11.6.8, 11.6.9, 11.6.10, 11.6.11, 11.7.1, 11.7.2, 11.9.3, 11.11.3, 11.11.4, 11.11.5, 11.11.6, 11.11.7, 11.12.3, 11.12.6, 11.12.11, 11.13.5, 11.13.6, 11.13.8, 11.13.9, 11.14.5, 11.16.2
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)	11.1.10, 11.11.1, 11.11.2, 11.11.8, 11.12.4, 11.12.10, 11.14.4, 11.14.7, 11.17.1, 11.17.2, 11.17.16
PR.AT-2	Privileged users understand their roles and responsibilities	11.4.3
PR.DS-1	Data-at-rest is protected	11.14.1, 11.14.6, 11.17.1, 11.20.1, 11.20.2, 11.20.3, 11.20.4

PR.DS-2	Data-in-transit is protected	11.12.1, 11.12.2, 11.12.8, 11.14.7, 11.16.1, 11.17.4, 11.17.5, 11.17.6, 11.17.19
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	11.20.1, 11.20.2, 11.20.3, 11.20.4
PR.DS-5	Protections against data leaks are implemented	11.5.2, 11.6.4, 11.6.7, 11.17.13, 11.17.17
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.7.2, 11.17.7, 11.17.8
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)	11.1.5, 11.1.6, 11.1.8, 11.1.12, 11.4.4
PR.IP-2	A System Development Life Cycle to manage systems is implemented	11.6.4, 11.6.7
PR.IP-3	Configuration change control processes are in place	11.1.15, 11.19.2
PR.IP-4	Backups of information are conducted, maintained, and tested	11.19.1, 11.19.4, 11.19.6, 11.19.7
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	11.16.3
PR.IP-7	Protection processes are improved	11.1.13
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11.1.20, 11.19.5
PR.IP-12	A vulnerability management plan is developed and implemented	11.1.17
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.1.19, 11.13.6, 11.17.14, 11.17.17

PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	11.12.5
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.1.22, 11.13.4, 11.18.1, 1.18.5
PR.PT-2	Removable media is protected and its use restricted according to policy	11.13.4
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.4.4, 11.5.3, 11.6.4, 11.6.7
PR.PT-4	Communications and control networks are protected	11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.7, 11.1.11, 11.1.18, 11.5.2, 11.6.3, 11.7.1, 11.9.3, 11.12.7, 11.12.9, 11.13.1, 11.13.2, 11.13.3, 11.14.7, 11.15.4, 11.17.10, 11.17.12, 11.17.15, 11.17.18
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	11.4.1, 11.13.7, 11.19.5
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	11.9.1, 11.9.2, 11.13.10, 11.18.4, 11.18.6, 11.19.7
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.17.11, 11.18.2, 11.18.3, 11.18.8
DE.CM-1	The network is monitored to detect potential cybersecurity events	11.5.2, 11.8.1, 11.8.2, 11.17.3, 11.17.11, 11.18.2, 11.18.4, 11.18.7
DE.CM-4	Malicious code is detected	11.5.4, 11.8.4
DE.CM-8	Vulnerability scans are performed	11.1.13
DE.DP-2	Detection activities comply with all applicable requirements	11.18.7
DE.DP-5	Detection processes are continuously improved	11.8.3

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-016 Remote Access Security Standard	Yes
B	SS-033 Security Patching Standard	Yes
C	Technical Vulnerability Management Policy	Yes
D	Security Incident Management Policy	TBC
E	SS-001 pt.2 Privileged User Access Security Standard	Yes
F	SS-001 pt.1 Access and Authentication Security Standard	Yes
G	DWP Approved Cryptographic Algorithms workbook	No
H	SS-006 Secure Boundaries Security Standard	Yes
I	SS-013 Firewall Security Standard	Yes
J	SS-025 Virtualisation Security Standard	Yes
K	SS-007 Use of Cryptography Security Standard	Yes
L	SS-019 Wireless Networking Security Standard	Yes
M	SS-012 Protective Monitoring Security Standard	Yes
N	SS-035 Secure Backup and Restore Security Standard	Yes
O	SS-036 Secure Sanitisation and Destruction Security Standard	Yes
P	SS-008 Server Operating System Security Standard	Yes
Q	SS-015 Malware Protection Security Standard	Yes
R	Security Assurance Strategy	No
S	SS-027 Security Testing Standard	No

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
ISO27033 Part 2 contains guidelines for the design of network security. These guidelines should be followed. The design **must** take account of legal and regulatory requirements
Best Practices: Device Hardening and Recommendations - Cisco Blogs
https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles
RFC 1918 - Address Allocation for Private Internets (ietf.org)

Appendix D. Abbreviations

Table 5 - Abbreviations

Abbreviation	Definition	Owner
AAA	Authentication, Authorization and Accounting	
ACL	Access Control List	
ARP	Address Resolution Protocol	
DAM	Database Activity Monitoring	
DHCP	Domain Host Configuration Protocol	
DLP	Data Loss Protection	
DMZ	Demilitarised Zone	
DNS	Domain Name Service	
DA	Design Authority (DA)	

DoS	Denial of Service	
DWP	Department for Work and Pensions (DWP)	
FTP	File transfer protocol	
HIPS/HIDS	Host-based Intrusion Protection/Detection System	
HTTP/HTTPS	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure	
IPS/IDS	Intrusion Protection/Detection System	
LAN	Local Area Network	
MAC	Media Access Control	
MITM	Man-in-the-middle	
MPLS	Multi-protocol label switching	
NAC	Network Admission Control	
NAT	Network Address Translation	
NAS	Network Attached Storage	
NCSC	National Cyber Security Centre	
NIPS/NIDS	Network Intrusion Protection/Detection System	
NTP	Network Time Protocol	
OOB	Out of Band	
PKI	Public Key Infrastructure	
PSN	Public Sector Network	
QoS	Quality of Service	
SAN	Storage Area Network	
SNMP	Simple Network Management Protocol	
SOC	Security Operations Centre	
SQL	Structured Query Language	

STP	Spanning Tree Protocol	
SSD	Solid State Drive	
SSH	Secure Shell	
VLAN	Virtual Local Area Network	
VPN	Virtual Private Network	
WAN	Wide Area Network	
XML	Extensible Markup Language	
XSS	Cross-Site Scripting	

Appendix E. Glossary

Table 6 - Glossary

Term	Definition
Autonomous System Numbers (ASN)	An Autonomous System (AS) is a set of Internet routable IP prefixes belonging to a network or a collection of networks that are all managed, controlled and supervised by a single entity or organization. An AS utilizes a common routing policy controlled by the entity. The AS is assigned a globally unique 16 digit identification number—known as the autonomous system number or ASN—by the Internet Assigned Numbers Authority (IANA).
Denial of service (DoS)	Prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users
Demilitarised Zone (DMZ)	perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks
Firewall	type of security barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorised traffic, as defined by the local security policy, is allowed to pass.
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).
Filtering	process of accepting or rejecting data flows through a network, according to specified criteria
Intrusion Detection & Prevention Systems	technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks, providing active response capabilities.
Network Perimeter	physical or logical subnetwork that contains and exposes an organization's external services to a public network
Network Zoning	the concept that system resources of different sensitivity levels (i.e., different risk tolerance values and threat susceptibility) should be located in different security zones
Network Telemetry	process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis
Router	network device that is used to establish and control the flow of data between different networks by selecting paths or routes based upon routing protocol mechanisms and algorithms
Security Domain	set of assets and resources subject to a common security policy.
Security Gateway	point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.
Switch	device which provides connectivity between networked devices by means of internal switching mechanisms, with the

	switching technology typically implemented at layer 2 or layer 3 of the OSI reference model
Security Boundary	the basic means of keeping network traffic flowing where you want and restricting it where you do not is a security boundary: dedicated firewall devices, firewall functions in IPS devices, and access control lists in network routers and switches.
Tunnel	data path between networked devices which is established across an existing network infrastructure
Virtual Local Area Network	independent network created from a logical point of view within a physical network
VPN Gateway	a type of networking device that connects two or more devices or networks together in a VPN infrastructure. It is designed to bridge the connection or communication between two or more remote sites, networks or devices and/or to connect multiple VPNs together.

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)