Security Standard –

Security Boundaries

(SS-006)

Chief Security Office

Department for Work & Pensions

Date: 22/08/2024

This Security Boundaries standard is part of a suite of standards, designed to promote consistency across the Department for 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 – Terms

Term	Intention
must	denotes a requirement: a mandatory requirement
should	should denotes a recommendation: an advisory element
may	denotes approval
might	denotes a possibility
can	denotes both capability and possibility
Is/are	denotes a description

1. Table of Contents

1. Table of Contents 3
2. Revision history 4
3. Approval history 5
4. Compliance 6
5. Exceptions Process 6
6. Audience 6
7. Accessibility Requirements 6
8. Introduction 7
9. Purpose 8
10. Scope 8
11. Minimum Technical Security Measures 9

11.1 Supporting Technical Documentation 9

11.2 Implementation 10

11.3 Network Perimeter Controls 12

11.4 Encryption 14

11.5 Authentication 15

11.6 Authorisation 16

11.7 Service Restriction 16

11.8 Administration 17

11.9 Logging and Monitoring 18

12. Appendices 19

Appendix A Security Outcomes 19

Appendix B Internal references 22

Appendix C External references 22

Appendix D Abbreviations 23

Appendix E Glossary 24

Appendix E Accessibility artefacts 24

Table 1 – Terms 2
Table 2 – List of Security Outcomes Mapping 19
Table 3 – Internal References 22
Table 4 – External References 22
Table 5 – Abbreviations 23
Table 6 – Glossary 24

2. Revision history

Version	Author	Description	Date
1.0		First published version	26/05/2017
2.0		Full update in line with current best practices and standards; • Changes made updating security requirements to become security measures. • Removed reference to Guiding Security Principles Document as previously agreed, and updated all references accordingly • Added trusted/untrusted definition in intro • Added zero trust context @ Introduction and 11.1.1 • Acknowledged context inspection exceptions 11.3.x & 11.4.1 • Added NIST references • Updated Appendix A to reference the security measures • 11.2.2 Cloud and virtual environments • 11.2.3 Boundary device configuration review frequency • 11.2.4 Trusted and untrusted networks • 11.2.8 Added exceptions • 11.2.9 Minor rewording regarding separate management network • 11.3.2 Added implications of using third party sandboxing services • 11.3.4 Differentiated requirements between	16/01/2023

		inbound and outbound scanning. • 11.3.8 Added an exception for certificate-pinned services • 11.3.9 Clarified this statement • 11.4.4 & 11.4.5 Differentiated between inbound and outbound connections	
2.1		All NIST references reviewed and updated to reflect NIST 2.0. Approval history - Review period changed to up to 2 years Compliance – Ref added to Security Assurance Strategy Scope – Reference added for Authority Cloud-to-Cloud Security Guidance for Software-as-a-Service 11.3.8 – mTLS and HSTS 11.4.1 – exception 11.4.2 – exception 11.4.5 – Time Stamp Authority 11.7.3 – exception	22/08/2024

3. Approval history

Version	Approver	Role	Date
1.0		Chief Security Officer	26/05/2017
2.0		Chief Security Officer	16/01/2023
2.1		Chief Security Officer	22/08/2024

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

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

- controls tests performed by 1st line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. K].
- 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 standard defines a set of minimum-security measures that **must** be implemented to secure the Authority's security boundaries, including consumption of cloud services. For the purposes of this standard, a security boundary can be described as the demarcation line between any two environments (domains) that have different security requirements or needs e.g., the internal network and a DMZ or DMZ and the Internet.
As the 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 data in question, and in keeping with latest security enhancements. See Appendix C for recommended external references.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to security boundaries are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with security boundaries, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.
- ensure Authority ICT systems are protected from intrusions and unauthorised access from environments (domains) traditionally considered trusted as well as non-trusted environments.
- minimise data leakage risks by ensuring traffic traversing the Authority's security boundaries is being proportionality monitored.
- ensure internal and external security boundaries are secured with a consistent set of boundary security controls.
- Recognise Zero Trust security requirements.

For the purposes of this standard, trusted and untrusted networks are defined as follows;

- **Trusted networks** are those owned or managed by the Authority, and are open only to trusted i.e. authorised users. Trusted networks contain inherent security capabilities that afford a layer of protection to traffic traversing them.

- **Untrusted networks** are those outside the security perimeter and not under the control of the Authority, and may be open to untrusted or even unknown users. Untrusted networks may or may not contain inherent security capabilities, but should be treated as if there is no inherent security, thus security controls must be built in to the data, connections, endpoints, and users.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and are enabled by the implementation of controls from the CIS Critical Security Controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure 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

This standard applies to any security boundary where Authority data leaves one logical network and enters another. This includes boundaries deployed internally, facing externally, and where logically extended i.e., into cloud provisioned services. The Authority's Cloud-to-Cloud Security Guidance for Software-as-a-Service [Ref. L] **must** be followed for cloud-to-cloud connections. These security measures **must** be applied to new and existing installations.

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 when deploying boundary security outcomes, described in Appendix A. For ease of reference, the relevant NIST sub-category ID is provided against each security measure e.g., PR.IP-1, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full descriptions of security outcomes.

11.1 Supporting Technical Documentation

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Boundary security devices **must** be supported by up to date technical documentation that describes the following as a minimum: ▪ Details of the ruleset that the gateway is required to administer ▪ Configuration details of the gateway ▪ Constraints and rules applied to traffic passing into and out of the security gateway ▪ Management and configuration parameters ▪ Specify any boundary inspection bypass rules / exception where zero trust and cloud solutions have been suitably governed by the Authority.	PR.PS-01

11.2 Implementation

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	The security boundary **must** prevent the passing of live traffic until its compliance with applicable Authority policies and standards (including this standard) have been verified through formal assurance methods, and approval provided in advance by the Authority and the relevant Authority Risk Owner.	PR.PS-01 GV.PO-01
11.2.2	The outer perimeter of a security boundary, between any Authority managed network[1] and an untrusted network (e.g. the internet), **must** be built upon an infrastructure that is physically separate from the network infrastructure from which it is connected. For cloud or virtualised environments where physical separation is not possible, logical networks with separate management domains **must** be implemented.	PR.IR-01
11.2.3	The configuration of the devices that form the security boundary **must** be reviewed at least monthly and validated by performing routine technical compliance checks to confirm device health and patch status. This can be performed via automated means, and supplemented by performing timely IT Health Checks, e.g. after a security breach, compromise or significant system changes.	PR.PS-01
11.2.4	All requests for Authority information system resources – files, connections, web pages, or services originating from both trusted and untrusted networks[1], **must** require authenticated, authorised and inspected handling sessions, the design for which must approved by the Authority.	PR.IR-01 PR.AA-03

[1]A network managed by the Authority or a third-party supplier contracted to provide managed services on its behalf.

[1] An untrusted network refers to any network that is not under the direct control or management of the Authority

11.2.5	The security boundary **must** include the capability to consume cloud-based security services where these are deemed appropriate.	PR.PS-01
11.2.6	Devices (both physical and virtual) performing the security enforcing functions **must** themselves be resistant to compromise. The devices **must** expose only those services required to fulfil the required capability. ▪ Authentication and authorisation are required to access data and services ▪ Logging of all administrative events **must** take place ▪ Alerting of events **must** be sent to a host that resides outside the Boundary Service (to a secure service) ▪ Consideration **must** be given to generating Alerts on changes to the device configuration. (Integrity Testing) ▪ All administrative access to the devices shall make use of Multi-Factor Authentication Technology, see SS-001 (part 2) – Privileged User Access Security Standard [Ref. B] ▪ Access must be granted in a granular fashion enforcing the principle of least privilege	PR.AA-05 PR.PS-01 DE.CM-01 DE.CM-06 PR.AA-01 PR.IR-01
11.2.7	Where service load is required to be distributed across several components within the boundary, the load balancing capability **must** be provided from within the security boundary perimeter.	PR.IR-01 PR.IR-04
11.2.8	Separate subnets **must** be created at the boundary when exposing services to untrusted networks, including partner and supplier networks. This does not apply to Internet facing connections, e.g. ZScaler Internet Access.	PR.IR-01
11.2.9	A separate management network **must** be implemented to administer boundary components so that normal user communications are kept separate from management communications.	PR.IR-01 PR.AA-05

11.2.10	The defence-in-depth concept **must** be applied to management networks. In other words, the same number of tiers **should** be implemented in the management plane to that of the supported data plane.	PR.IR-01

11.3 Network Perimeter Controls

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	The Boundary Service **must** provide a filter service to ensure that only authorised users and endpoints may communicate across it.	PR.IR-01
11.3.2	Where packet inspection is required at the boundary as part of risk mitigation or compliance reasons, the inspection capability **must** include the ability to carry out deep packet inspection and be cognisant of application layer protocols. The content analysis applied **must** consider as a minimum: • Protocol analysis; (where possible, layer 2 to 7 of the OSI model) • Signature-based scanning (searching for known patterns) • Behavioural analysis (analysing code for functions and behaviour known to be associated with malicious code) • Where possible, utilise Sandboxing technology (executing suspect code within a safe environment to assess the behaviour), being cognisant of the security implications of sending packets to external 3rd party providers, potentially exposing Authority data. • Message Structure and Format; (is the message structure as expected, - length, field structure, character set for example) • Message Payload. (Does the payload conform to allowed characteristics, file types, Size, for example).	DE.CM-01

11.3.3	Anti-virus and anti-malware solution with heuristic and signature-based capabilities **must** be deployed at the boundaries. Suspicious or infected objects **must** be quarantined for further analysis.	DE.CM-01 DE.CM-06 DE.AE-02
11.3.4	All inbound objects **must** be scanned for viruses and malware, with recursive checks being carried out to ensure that any embedded files are also checked. All inbound file types and content **must** also be checked. Outbound scanning should be determined based on the results of a risk assessment.	DE.CM-01
11.3.5	Where the boundary service malware detection process triggers any deletion or quarantine actions, they **must** take place within the same security boundary.	PR.IR-01 DE.CM-01
11.3.6	The ability to identify and block the egress of specific data assets e.g., national insurance numbers, credit card details etc., **must** be implemented where the boundary lies between two different security domains.	PR.DS-02
11.3.7	Where there is a requirement for Data and Message Transformation mechanisms to be employed, then these mechanisms **must** maintain the integrity of the transformed data.	PR.DS-02
11.3.8	Except for Authority approved Certificate-pinned services (or equivalents, such as mutually authenticated TLS (mTLS) or HTTP Strict Transport Security (HSTS)), internal client systems **must** be prevented from connecting directly to systems hosted on untrusted networks e.g. the internet (including third party supplier networks). All connections **must** go via an approved proxy service. Any exceptions to this must be submitted to the Authority.	PR.IR-01
11.3.9	Services exposed to external networks **must** be protected by perimeter network controls that ensure that external connections cannot gain direct access i.e., **must** be proxied.	PR.IR-01

11.4 Encryption

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	The boundary **must** provide the capability to inspect all encrypted traffic on ingress into the boundary unless an approved Authority Pattern[2] dictates otherwise. These are published as part of the Authority's Architectural Blueprint. Where packet inspection is not possible due to the connection method, an exception **must** be raised and submitted to the Authority for review.	DE.CM-01
11.4.2	Encryption capabilities within the boundary **must** support as a minimum, all the Authority approved encryption algorithms and implementations in line with SS-007 Use of Cryptography Security Standard [Ref. C]. Where this is not possible, an exception **must** be raised and submitted to the Authority for review.	PR.DS-02
11.4.3	The boundary **must** not allow encrypted session parameters to be negotiated outside the approved values (e.g. algorithm, key length). For details regarding approved values, refer to SS-007 Use of Cryptography Security Standard [Ref. C].	PR.DS-02
11.4.4	For inbound connections, where the boundary lies between an Authority managed network and an external service that utilises departmental encryption capabilities, then the boundary **must** support the ability to enable departmental encryption services, e.g. a Hardware Security Module, to external consumers. Typically, these services would include: • CRL (Certification Revocation lists or an OCSP (Online Certificate Status Protocol service). • Key distribution service – to allow external consumption of keys mastered within the Authority.	PR.IR-01 PR.DS-02

[2] Authority Security Patterns are considered sensitive to the Department therefore are not publicly accessible. If further guidance is required regarding approved DWP Patterns, please contact the Authority.

11.4.5	For outbound connections where the boundary lies between an Authority managed network and an external service, where the Authority services utilise an external provider's encryption, these services should include: • CRL (Certification Revocation lists or an OCSP (Online Certificate Status Protocol service). • Key distribution service – to allow external consumption of keys mastered within the Authority. Use of a Time Stamp Authority may also be considered, where appropriate.	PR.IR-01

11.5 Authentication

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	The boundary **must** as a minimum support authentication of all sessions, connections and flows into the boundary using Authority approved authentication mechanisms. For details on approved authentication mechanisms, refer to SS-001 pt.1 Access and Authentication Security Standard [Ref. D] and SS-001 pt.2 Privileged User Access Security Standard [Ref. B].	PR.AA-03
11.5.2	Where applicable, the security boundary **must** support external consumption of authentication tokens or other federation mechanisms. Note. The Authority network infrastructure is seen as the Identity Provider for internal Authority users.	PR.AA-02 PR.AA-03
11.5.3	All administrative access to boundary devices and components **must** make use of multi-factor authentication technology in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. B].	PR.AA-03

11.6 Authorisation

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	The security boundary **must** have the capability to control access to end points based upon the access control policy applied to the user or service requesting access to the endpoint.	PR.AA-05 PR.IR-01
11.6.2	The security boundary **must** be able to provide administrative access to its components based upon authorised profiles of individual users. Refer to SS-001 pt.2 Privileged User Access Security Standard [Ref. B]. for further measures.	PR.AA-05
11.6.3	All authorised access **must** be in accordance with the Department's User Access Control Policy [Ref. E].	PR.IR-01 PR.AA-05
11.6.4	Conditional access policies **must** be implemented at the boundary where these are supported and profile hardened checks e.g., identity, authorisation, network location, device health etc. (not an exhaustive list).	PR.IR-01

11.7 Service Restriction

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	The security boundary **must** expose at its internal and external perimeters only the minimum set of services necessary to support business processing.	PR.DS-02
11.7.2	Components within the boundary **must** only expose the minimum set of services that are required to support business processing.	PR.DS-02

11.7.3	Packet filtering **must** be implemented at the boundary, to deny unauthorised packets that are outside gateway policy and reduce the workload of security gateways. Where packet inspection is not possible due to the connection method, an exception **must** be raised and submitted to the Authority for review.	PR.IR-01 DE.CM-01

11.8 Administration

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Administrative accounts for boundary components **must** be managed in accordance with the Authority's Privileged Users Security Policy [Ref. F] and the Privileged User Access Controls Security Standard (part 2) [Ref. B].	PR.AA-05
11.8.2	All components within the boundary service **must** be executing on supported hardware and software versions.	PR.PS-02 PR.PS-03
11.8.3	All components within the boundary service **must** have an appropriate support contract with the vendor.	PR.PS-02 PR.PS-03
11.8.4	All components within the boundary service **must** be maintained to the supported patch level determined in accordance with SS-033 Security Patching Standard [Ref. G].	PR.PS-02
11.8.5	Administration **must** only be performed using dedicated management devices and control traffic and protocols authorised by boundary configuration policy.	PR.IR-01
11.8.6	Remote administration of boundary components **must** comply with SS-016 Remote Access Security Standard [Ref. H].	PR.IR-01 PR.AA-03
11.8.7	All communication traffic to management interfaces **must** be denied by default, access being granted only in accordance with the boundary configuration policy and RBAC rule	PR.IR-01 PR.AA-05
11.8.8	Administrative access **must** not bypass any traffic separation measures established within the boundary.	PR.IR-01

11.9 Logging and Monitoring

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Logging of activities relating to the services and systems within the security boundary **must** be carried out in line with the Authority's Protective Monitoring Policy [Ref. I] and associated SS-012 Protective Monitoring Security Standard [Ref. J].	DE.CM-01 DE.CM-09
11.9.2	Where the security boundary interfaces to external or cloud services, log and event information **must** be capable of being relayed to the authorised Authority's monitoring service.	DE.AE-03 DE.CM-01 DE.CM-06
11.9.3	Logging **must** take place of all administrative activities carried out upon boundary components.	DE.CM-03

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 Measure
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	11.2.1
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	11.2.6
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.5.2
PR.AA-03	Users, services, and hardware are authenticated	11.2.4, 11.5.1, 11.5.2, 11.5.3, 11.8.6

PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.2.6, 11.2.9, 11.6.1, 11.6.2, 11.6.3, 11.8.1, 11.8.7
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.3.6, 11.3.7, 11.4.2, 11.4.3, 11.4.4, 11.7.1, 11.7.2
PR.PS-01	Configuration management practices are established and applied	11.1.1, 11.2.1, 11.2.3, 11.2.5, 11.2.6
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.8.2, 11.8.3, 11.8.4
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	11.8.2, 11.8.3
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	11.2.2, 11.2.4, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.2.10, 11.3.1, 11.3.5, 11.3.8, 11.3.9, 11.4.4, 11.4.5, 11.6.1, 11.6.3, 11.6.4, 11.7.3, 11.8.5, 11.8.6, 11.8.7, 11.8.8

PR.IR-04	Adequate resource capacity to ensure availability is maintained	11.2.7
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.2.6, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.4.1, 11.7.3, 11.9.1, 11.9.2
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.9.3
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	11.2.6, 11.3.3, 11.9.2
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.9.1
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	11.3.3
DE.AE-03	Information is correlated from multiple sources	11.9.2

Appendix B Internal references

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

Table 3 – Internal References

Ref	Document	Publicly Available
B	SS-001 (part 2) – Privileged User Access Security Standard	Y
C	SS-007 Use of Cryptography Security Standard	Y
D	SS-001 (part 1) Access & Authentication Security Standard	Y
E	DWP User Access Control Policy	Y
F	DWP Privileged Users Security Policy	Y
G	SS-033 Security Patching Security Standard	Y
H	SS-016 Remote Access Security Standard	Y
I	SS-012 Protective Monitoring Security Standard	Y
J	DWP Protective Monitoring Policy	Y
K	DWP Security Assurance Strategy	No
L	DWP Cloud-to-Cloud Security Guidance for Software-as-a-Service (Architecture Blueprint)	No

Requests to access non-publicly available documents **should be made to the Authority.*

Appendix C External references

The following publications and guidance were used in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

Ref	Document
A1	ISO/IEC 27001:2013 – Information Security Management Systems
A2	NCSC – Security Architecture 'Anti-patterns'
A3	NIST SP 800-53 Rev.5 – Security and Privacy Controls for Information Systems and Organisations
A4	NIST SP 800-207 – Zero Trust Architecture
A5	ISO/IEC 27033 – Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways
A6	CESG Good Practice Guide No. 8 – Protecting External Connections to the Internet.
A7	NCSC Cloud Security Principles

Appendix D Abbreviations

List of abbreviations used in this standard.

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CA	Certificate Authority	Industry term
CRL	Certificate Revocation List	Industry term
DDA	Digital Design Authority	Internal term
DMZ	Demilitarized Zone	Industry term
GSCS	Government Security Classification Scheme	UK Government
HSTS	HTTP Strict Transport Security	Industry term
IaaS	Infrastructure as a Service	Industry term
IP	Internet Protocol	Industry term
ISO	International Organization for Standardization	Industry term
mTLS	Mutually authenticated TLS	Industry Term
NCSC	National Cyber Security Centre	UK Government
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OCSP	Online Certificate Status Protocol	Industry term
OSI	Open Systems Interconnections	Industry term
OWASP	Open Web Application Security Project	Open source
PaaS	Platform as a Service	Industry term
PII	Personally, Identifiable Information	Industry term
SaaS	Software as a Service	Industry term
SSH	Secure Shell	Industry term

Appendix E Glossary

Table 6 – Glossary

Term	Definition
Application Proxy	Server application that acts as an intermediate between a client requesting a resource and the server providing that resource.
Application Layer Protocols	Shared communication protocols and interface methods used by hosts in a communication network
Certificate Revocation List	List of digital certificates that have been revoked by the issuing certificate authority (CA).
OFFICIAL	Information classification mark, identified in the Government Security Classification Policy.
Security gateway	Networking hardware or software used in networks that allows data to flow from one discrete network to another.
Proxy Service	A server application that acts as an intermediary between a client requesting a resource and the server providing that resource.
Data Plane	Part of the network that carries user traffic.
Management Plane	All the functions used to control and monitor devices.
OSI Model	A conceptual framework that characterises and standardises the communication functions of a computing system without regard to underlying internal structure and technology.
Sandbox	A security mechanism for separating running programs.
Payload	Part of the transmitted data that is the actual intended message. Heads and metadata are sent only to enable delivery of the payload.
Time Stamp Authority	A time stamping authority ensures that data stored or processed carry a date and time synchronized with a time server. These time settings may be evidence in a legal procedure.

Appendix E 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/

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps