Security Standard – Domain Management (SS-031)

Chief Security Office

Date: 27/01/23

Department for Work & Pensions

This Domain Management Security 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 term 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. 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 element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

2. Revision History

Version	Author	Description	Date
1.0		First published version	13/11/2017
1.1		10.3.1 added - An alias defined in a CNAME RR MUST have no other resource records of other types (e.g. MX, A), except any DNSSEC-related records used to protect the integrity of the CNAME record. Domains that are used for e-mail must not have a CNAME record. 10.3.2 changed the reporting email addresses 10.3.4 updated the links and added - DKIM keys MUST be rotated at least every 12 months.	17/12/2021
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 • Compliance changed to Security Assurance 11.2.1 Clarified TTL value. 11.2.2 Added requirement that internal domains hosted in cloud environments must not be publicly resolvable. 11.2.3 Changed to 'allow' listed 11.2.6 Requirement added for Certification Authority Authorisation 11.2.7 Requirement added for MFA on DNS admin accounts	27/01/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	13/11/2017
2.0		Chief Security Officer	27/01/2023

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted "final" status, and at yearly 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. C].
- 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 Statement

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 Domain Management Security 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:

- ensure security controls that are applicable to domain management are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with domain management, to an acceptable level for operation.
- 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

This standard provides security measures that apply to all Authority owned or operated domain names, or those owned or managed by a Authority supplier or contracted third party as part of a Authority activity.

Throughout this document, the term *domain* should be interpreted the same as the term *Internet domain name* – a hierarchical structure of human-readable names resolved by Domain Name System (DNS) servers.

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 Technical Security Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	When registering a domain for the first time, that domain **must** be added to a central domain management asset register.	ID.AM-2
11.1.2	Central government guidance for naming and registering websites **must** be followed. [see Appendix C, External References]	ID.GV-3
11.1.3	Each domain **must** have a responsible and accountable owner. This owner **must** be named on the domain management asset register.	ID.AM-6
11.1.4	The domain registrant contact details **must**: a) Be hidden from public view in the WHOIS repository using a by-proxy registration service; or b) Be populated with the details of a central asset management function.	PR.DS-1
11.1.5	Contact information in the central domain management asset register and in the WHOIS database **must** be kept up to date.	PR.DS-3 ID.AM-2
11.1.6	The chosen DNS Provider(s) (DNSP(s)) **must** specify Service-Level Agreements (SLAs) in a signed contract pertaining to: a) The resolution time of any issues, technical or otherwise; and b) The completion time for any requested changes; and c) The availability level of their nameservers.	ID.SC-3 ID.SC-5
11.1.7	The chosen DNSP **must** provide a level of availability commensurate with the availability requirement for the system or service. Multiple DNSPs may be used where appropriate to provide redundancy.	ID.SC-3

11.1.8	The domain itself and supporting services **must** be monitored for expiry at appropriate time intervals. The central asset management function should support this task through the issuance of automated alerts.	ID.SC-4 PR.DS-4

11.2 General DNS

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Each DNS Resource Record (RR) **must** have an appropriate Time to Live (TTL) value. For the majority of cases, this should be 1 hour (3600s), except for records that rarely change such as TXT or MX records.	PR.AC-5
11.2.2	Internal nameservers **must** only respond to queries originating from inside Departmental networks. DNS zones for 'internal domains' hosted in cloud environments should not be publicly resolvable.	PR.AC-7
11.2.3	Internal nameservers **must** restrict zone transfer using the Authoritative Transfer (AXFR) protocol to only 'allow listed' locations.	PR.AC-7
11.2.4	Results returned by nameservers **must** not bypass any necessary security enforcing devices. For example, MX records **must** point to mail scanning / spam filtering devices rather than the receiving Mail Transfer Agent (MTA).	PR.PT-4
11.2.5	For all online digital services, the domain name registrant **must** also register similar domain names (including under different Top-Level Domains (TLDs)) to prevent phishing and potential embarrassment.	ID.AM-2 PR.DS-3
11.2.6	Certification Authority Authorisation (CAA) DNS Resource Records **must** be implemented to allow DNS Domain Name holders to specify the Certification Authorities (CAs) authorised to issue certificates, and thus implement additional controls where required, as per RFC 8659 [see External References].	PR.DS-5
11.2.7	DNS management systems must enforce Multi Factor Authentication (MFA) for any account with the ability to modify DNS records.	PR.AC-4 PR.AC-7

11.3 Record-specific DNS

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	An alias defined in a CNAME RR **must** have no other resource records of other types (e.g. MX, A), except any DNSSEC-related records used to protect the integrity of the CNAME record. Domains that are used for e-mail **must not** have a CNAME record.	PR.DS-6
11.3.2	All Authority-registered domains **must** implement Domain-based Message Authentication, Reporting and Conformance (DMARC) as follows: • The overarching policy and subdomain policy **must** be set to "reject"; • The forensic reporting mode **must** be set to generate reports upon both SPF and DKIM failures; • All domains implementing DMARC **must** forward aggregate (rua) reports to: ○ dmarc-rua@dmarc.service.gov.uk; and ○ 5spd6hq3@ag.eu.dmarcadvisor.com • All domains implementing DMARC **must** forward forensic (ruf) reports to: ○ dmarc.rua@dwp.gov.uk; and ○ 5spd6hq3@fr.eu.dmarcadvisor.com	PR.DS-2 PR.DS-6 PR.PT-4
11.3.3	All Authority-registered domains **must** implement Sender Policy Framework (SPF) as follows: • Domains not sending any email **must** implement an SPF record that returns a "fail" result for all email traffic. A DNS record of "v=spf1 -all" needs to be set to achieve this. Other domains **must** identify all authorised mail-sending agents and explicitly identify these in the SPF record. Emails not matching the SPF criteria **must** result in a "softfail" or "fail" result.	PR.PT-4
11.3.4	All Authority-registered domains **must** implement DomainKeys Identified Mail (DKIM) as follows: • Asymmetric key pairs MUST use algorithms and key lengths defined in SS-007 Use of Cryptography Security Standard [Ref. A].	PR.PT-4

	• Cryptographic keys **must** be protected in accordance with SS-002 PKI & Key Management Security Standard [Ref. B]. • DKIM keys **must** be rotated at least every 12 months.	

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 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-2	Software platforms and applications within the organization are inventoried	11.1.1 11.1.5 11.2.5
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	11.1.2
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	11.1.3
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	11.1.6 11.1.7
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.	11.1.8
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	11.1.6

PR.DS-1	Data-at-rest is protected	11.1.4
PR.DS-2	Data-in-transit is protected	11.3.2
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	11.1.5 11.2.5
PR.DS-4	Adequate capacity to ensure availability is maintained	11.1.8
PR.DS-5	Protections against data leaks are implemented	11.2.6
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.3.1 11.3.2
PR.AC-4	Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties	11.2.7
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.2.1
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.2.2 11.2.3 11.2.7
PR.PT-4	Communications and control networks are protected	11.2.4 11.3.2 11.3.3 11.3.4

Appendix B Internal References

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

Table 2 – Internal References

Ref	Document	Publicly Available*
A	SS-007 Use of Cryptography Security Standard	Yes
B	SS-002 PKI & Key Management Security Standard	Yes
C	Security Assurance Strategy	No

Requests to access 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 3 – External References

External Documents List
CIS Critical Security Controls v8 controls set
Central government guidance for naming and registering websites
https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white
RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record (rfc-editor.org)

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
AXFR	Authoritative Transfer
CDN	Content Delivery Network
CNAME	Canonical Name
DDA	Digital Design Authority
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DNSP	DNS Provider
DNSSEC	Domain Name System Security Extensions
FQDN	Fully-Qualified Domain Name
MTA	Mail Transfer Agent
MX	Mail Exchanger
RR	Resource Record

SLA	Service Level Agreement
SPF	Sender Policy Framework
TLD	Top-level Domain
TTL	Time to Live

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
WHOIS	A query and response protocol used for querying databases that store registered users or assignees of an Internet resource, such as a domain name.
A Record	A DNS Resource Record (RR) which maps a domain name to an Internet Protocol version 4 (IPv4) address.
AAAA Record	A DNS Resource Record (RR) which maps a domain name to an Internet Protocol version 6 (IPv6) address.
PTR Record	A DNS Resource Record (RR) which maps an IP address to a hostname. Used in reverse DNS lookups.
Nameserver	A server component of the Domain Name System (DNS) which provides resolution of domain names and hostnames into Internet Protocol (IP) addresses.
Authoritative Nameserver	A nameserver which answers queries for a specified set of zones and satisfies queries from its own data without needing to reference another source.
DNS Provider (DNSP)	The entity which operates authoritative nameservers for a particular domain. This may also be a Content Delivery Network (CDN) provider (e.g. Akamai).
Domain, Domain Name	A hierarchical structure of human-readable names resolved by Domain Name System (DNS) servers.

Appendix F Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

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

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