IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

# Security Standard – Domain Management (SS-031)

**Chief Security Office**

**Date: 13/11/2017**

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

**Version Control Table**

| Version | Date | Major Change |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

**Updating policy**

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

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

## Contents

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

## 1. Introduction

1.1. 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.

1.2. This Security Standard provides a list of security controls that apply to DWP owned or operated domain names. This list of requirements ensures a baseline level of security that is approved and accepted by the Department for Work and Pensions (DWP) to afford the necessary level of protection to its systems and data.

1.3. For further clarity and relevance, this standard is aligned to the Department's internal technical strategy paper, the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.4. Furthermore the security controls presented in this standard are taken from examples of international best practice for domain management and have been tailored for Departmental suitability.

## 2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for domain management.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

## 3. Exceptions

3.1. In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

3.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to Design Authority (DA) where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.3. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

3.4. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

## 4. Audience

4.1. This standard is intended for people who are administering or managing domains for departmental use.

## 5. Scope

5.1. The security controls presented in this document are applicable to any domains owned or managed by the DWP, or those owned or managed by a member of staff as part of a DWP activity.

5.2. Additional controls may be applicable based upon the use of a domain.

## 6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

## 7. Technical Security Control Requirements

### 7.1 Domain Registration, Management and Renewal

| Reference | Security Control Requirement |
|---|---|
| 7.1.1. | When registering a domain for the first time, that domain MUST be added to a central domain management asset register. |
| 7.1.2. | Central government guidance for naming and registering websites MUST be followed. |
| 7.1.3. | Each domain MUST have a responsible and accountable owner. This owner MUST be named on the domain management asset register. |
| 7.1.4. | The domain registrant contact details MUST:<br>a) Be hidden from public view in the WHOIS repository using a by-proxy registration service; or<br>b) Be populated with the details of a central asset management function. |
| 7.1.5. | Contact information in the central domain management asset register and in the WHOIS database MUST be kept up to date. |
| 7.1.6. | The chosen DNS Provider(s) (DNSP(s)) MUST specify Service-Level Agreements (SLAs) in a signed contract pertaining to:<br>a) The resolution time of any issues, technical or otherwise; and<br>b) The completion time for any requested changes; and<br>c) The availability level of their nameservers. |

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

| | |
|---|---|
| 7.1.7. | 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. |
| 7.1.8. | 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. |

## 7.2. General DNS

| Reference | Security Control Requirement |
|---|---|
| 7.2.1. | Each DNS Resource Record (RR) MUST have an appropriate Time to Live (TTL) value. In all cases, the TTL MUST be less than or equal to 24 hours. |
| 7.2.2. | Internal nameservers MUST only respond to queries originating from inside Departmental networks. |
| 7.2.3. | Internal nameservers MUST restrict zone transfer using the Authoritative Transfer (AXFR) protocol to only whitelisted locations. |
| 7.2.4. | 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). |
| 7.2.5. | 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 embarrassment. |

## 7.3. Record-specific DNS

| Reference | Security Control Requirement |
|---|---|
| 7.3.1. | 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. |
| 7.3.2. | All DWP-registered domains MUST implement Domain-based Message Authentication, Reporting and Conformance (DMARC) as follows:<br>• The overarching policy and subdomain policy MUST be set to “reject”;<br>• The forensic reporting mode MUST be set to generate reports upon both SPF and DKIM failures;<br>• All domains implementing DMARC MUST forward aggregate (rua) reports to:<br>  • dmarc.rua@dwp.gsi.gov.uk; and<br>  • dmarc-rua@dmarc.service.gov.uk.<br>• All domains implementing DMARC MUST forward forensic (ruf) reports to:<br>  • dmarc.ruf@dwp.gsi.gov.uk; and |

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

| | |
|---|---|
| | • dmarc-ruf@dmarc.service.gov.uk. |
| 7.3.3. | All DWP-registered domains MUST implement Sender Policy Framework (SPF) as follows:<br>• Domains not sending any email MUST implement an SPF record that returns a “fail” result for all email traffic.<br>• 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. |
| 7.3.4. | All DWP-registered domains MUST implement DomainKeys Identified Mail (DKIM) as follows:<br>• Asymmetric key pairs MUST use algorithms and key lengths defined in SS-007 Security Standard – Use of Cryptography.<br>• Cryptographic keys MUST be protected in accordance with SS-002 Security Standard – PKI & Key Management. |

## 8. Compliance

Compliance with this standard MUST occur as follows:

| Compliance | Due Date |
|---|---|
| **On-going** | From the first day of approval |
| **Retrospective** | Within 12 months of the approval of the standard. |

## 9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

## 10. Security Standards Reference List

| Document Name | Location | Version |
|---|---|---|
| Exceptions Process | | |
| DWP Baseline Control Set | | |

## 11. Reference Documents

## 12. Definition of Terms

| 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. |

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

| | |
|---|---|
| **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. |

## 13. Glossary

| Abbreviation | Definition |
|---|---|
| **AXFR** | Authoritative Transfer |
| **CDN** | Content Delivery Network |
| **CNAME** | Canonical Name |
| **DA** | 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 |

## 14. Controls Mapping

The requirements in this standard are derived from the high-level controls prescribed in the DWP Controls Catalogue.