Security Standard – Securely Serving Web Content (SS-029)

Department for Work & Pensions

Chief Security Office

Date: 26/10/2023

This Securely Serving Web Content 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 Authority 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	26/05/2017
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 11.1.7 Encryption of data 11.1.8 User and server access controls 11.1.9 CVM and Web Check; DDOS protection 11.2.1 User facing portion 11.2.5 Allowlisted 11.2.8 Content must be encrypted 11.2.9 Web server process account 11.3 User Interface / User Experience (UI/UX) 11.3.4 Secure cookies 11.3.6 Sensitive data, session cookies 11.3.8 Held in memory, encrypted on disk 11.3.9 Added ref to secure sanitisation and destruction standard 11.3.10 Added refs to access control standards 11.4.6 occur server side, enforce client side 11.4.10 Input validation, file types, malware scanning 11.5 HTTP(S) 11.5.5 Xframe options:DENY 11.5.8 max-age 63072000 11.5.9 Required http methods 11.6.3 Transform files 11.6.6 Client-side technologies 11.7.1 On the server 11.7.5 Added ref to Business Audit standard 11.7.6 Web server logging 11.7.7 Added ref to Protective Monitoring standard	26/10/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	26/05/2017
2.0		Chief Security Officer	26/10/2023

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. O].
- 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 Securely Serving Web Content 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 Securely Serving Web Content are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with Securely Serving Web Content, 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 applies to all Internet-facing web application systems that are provisioned for Authority use and supplier base (contracted third party providers), including those provisioned in Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments. It also applies to any 'web-based' services hosted internally to the Authority.

This standard makes reference to User Experience Functions and Microservices (see SS-028 Microservices Architecture Security Standard [Ref. I]) as defined in the Authority's Digital Blueprint. Where the application does not make use of a three-tier architecture (i.e. presentation, application and data) and one or more of these layers is not used, the relevant controls in this standard may be considered "not 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 Web Application System Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	All applicable software (web server, database, etc.) **must** adhere to SS-033 Security Patching Standard [Ref. A].	PR.IP-12 PR.MA-1
11.1.2	Web applications in a virtualised environment, **must** adhere to SS-025 Virtualisation Security Standard [Ref. B].	ID.GV-1
11.1.3	All components involved in serving web content **must** be compliant with the relevant security standard for that component or system (e.g. Operating system configuration controls in SS-008 Server Operating System Security Standard [Ref. C]).	ID.GV-1
11.1.4	Client-triggered processes or actions **must** adhere to the principle of least privilege design concept, providing users the minimum levels of access or permissions needed to perform their task.	PR.AC.4
11.1.5	All dependencies (e.g. software libraries, external systems) **must** be identified and documented wherever possible.	ID.AM-2
11.1.6	All default passwords for application administration **must** be changed and set in accordance with SS-001 pt.1 Access & Authentication Security Standard [Ref. D] and SS-001 pt.2 Privileged User Access Security Standard [Ref. E].	PR.AC-6
11.1.7	Information classified at OFFICIAL or above **must** be encrypted at rest in accordance with the controls in SS-007 Use of Cryptography Security Standard [Ref. G]. Web servers **must** not be used to store PII or business data at OFFICIAL or above.	PR.DS-1

11.1.8	User and server access controls **must** be in line with SS-001 pt.1 Access and Authentication [Ref. D] and SS-001 pt.2 Privileged User Access [Ref. E] security standards.	PR.AC-1 PR.AC-4
11.1.9	Services **must** be onboarded to the Continuous Vulnerability Monitoring Web Application Vulnerability Scanning service and the NCSC Web Check service, and **must** include protection against DDoS attacks.	PR.IP-12 DE.CM-8

11.2 Architectural Considerations

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	The user-facing portion of the web application (the "user experience functions" or "UI/UX functions") **must** be logically or physically separated from all other components.	PR.DS-5 PR.AC-5
11.2.2	The business logic functions (the "microservices layer") **must** be logically or physically separated from all other components.	PR.DS-5 PR.AC-5
11.2.3	The systems storing necessary data (the "application") **must** be logically or physically separated from all other components.	PR.DS-5 PR.AC-5
11.2.4	Each layer **must** have access to an administration interface that is separate from the pre-existing communication paths. Software updates and other necessary Internet access outbound **must** be directed through this interface.	PR.DS-5 PR.AC-5
11.2.5	Software updates and other necessary Internet access outbound **must** either: a) Be directed through the administration interface; or b) Be allowlisted to travel via the untrusted network with all other unnecessary destinations implicitly blocked.	PR.DS-5 PR.AC-5
11.2.6	Access control and error handling logic **must** deny access by default.	PR.AC-4
11.2.7	Communication between components **must** be cryptographically protected in transit if travelling to or via a less trusted security domain. This cryptographic protection **must** be applied in accordance with SS-007 Use of Cryptography Security Standard [Ref. G].	PR.DS-2

11.2.8	Content served by the web server **must** be cryptographically protected by an approved implementation of Transport Layer Security (TLS). SP-006 Channel Encryption and Mutual Authentication Security Pattern [Ref. H] **must** be consulted for implementation.	PR.DS-2
11.2.9	The web server process **must** run as its own user account in its own user group with the minimum necessary privileges to successfully operate.	PR.AC-4

11.3 User Interface / User Experience (UI/UX) Functions

Further information for UI/UX requirements can be found in the Architecture Blueprint.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	The security controls between an untrusted network and the UI/UX functions **must** only permit connections on necessary and allowlisted TCP and UDP ports.	PR.AC-4
11.3.2	When using a Content Delivery Network (CDN), the security controls between an untrusted network and the UI/UX functions **must** restrict inbound traffic to that originating from the CDN provider.	PR.AC-3 PR.AC-5
11.3.3	The security controls between an untrusted network and the UI/UX functions **must** deny new connections originating from the UI/UX functions by default.	PR.AC-3 PR.AC-5
11.3.4	When a user requests the http:// version of a page, the web server **must** return a 301 redirect to the https:// version of the same page. Ensure that cookies are set to 'secure' so that they are not transmitted over http.	PR.DS-5
11.3.5	The error messages sent over the untrusted network **must** be limited to generic information containing no more than the error condition itself (e.g. HTTP 500 Internal Server Error).	PR.DS-2
11.3.6	Sensitive information (including personal data, session cookies and other secrets) **must** be sent in the HTTPS message body and not in other structures such as URL parameters.	PR.DS-2
11.3.7	Caching of personal information **must** be disabled with the use of "cache-control" and "pragma" HTTP headers.	PR.DS-1

11.3.8	Cached copies of personal information held on the server **must** be protected from unauthorised access (either held in memory or encrypted if written to disk) or otherwise immediately purged / invalidated.	PR.DS-1
11.3.9	If server infrastructure is being decommissioned, any resident data **must** be deleted in line with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. L].	PR.IP-6
11.3.10	Access via all interfaces **must** be controlled in line with SS-001 pt.1 Access & Authentication Security Standard [Ref. D] and SS-001 pt.2 Privileged User Access Security Standard [Ref. E].	PR.AC-3

11.4 Input Handling

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Input validation **must** be implemented using any programming technique that allows effective enforcement of values for syntactic and semantic correctness.	PR.DS-5 PR.DS-6
11.4.2	XML or JSON **must** be validated against a schema before being accepted as input.	PR.DS-6
11.4.3	User input in any format (e.g. form fields, URL parameters, REST calls) **must** be treated as malicious by default and sanitised or validated appropriately.	DE.CM-4
11.4.4	Where user input is expected in a specific format (e.g. a NINO or a card number), the input **must** also be validated against that schema.	PR.DS-6
11.4.5	Web application front ends **must** provide an adequate defence against automated attacks. Where personal information is transferred, this **must** also include defences against malicious software installed on the client-side.	PR.DS-5
11.4.6	Input validation and sanitisation **must** take place on the server-side, but also be enforced on the client-side.	PR.DS-6
11.4.7	Input validation failures **must** result in request rejection and be logged.	PR.DS-6

11.4.8	The application **must** have defence against HTTPS parameter pollution attacks, e.g., receiving unexpected values in cookies or headers.	PR.DS-6
11.4.9	Where an application already holds personal information about a customer, the application **must** not ask for the re-keying of that information except to check if it is up to date.	PR.DS-1
11.4.10	Input validation **must** be implemented to ensure uploaded filenames use an expected file type, files are not larger than a defined maximum file type, and ZIP file uploads (if supported by websites) **must** be checked for malware before unzipping.	PR.DS-6

11.5 HTTP(S) Security

The security measures in this section refer to HTTPS security.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Every HTTP response **must** contain a content-type header specifying a safe character set.	PR.DS-2
11.5.2	HTTP headers added by a trusted proxy or CDN provider **must** be authenticated by the application.	PR.AC-7
11.5.3	A Content-Security-Policy **must** be applied to prevent the loading of third-party scripts, stylesheets and plugins.	PR.PT-4
11.5.4	HTTP headers or any part of the HTTP response **must** not reveal version information of system components.	PR.PT-3
11.5.5	The HTTP headers **must** include “X-Frame-Options: DENY”. This header is used to prevent clickjacking attacks.	PR.PT-4
11.5.6	The HTTP headers **must** include “X-Content-Type-Options: nosniff”. This header is used by the server to indicate to the browsers that the MIME types advertised in the Content-Type headers should be followed and not guessed.	PR.PT-4
11.5.7	The HTTP headers **must** include “X-XSS-Protection: 1; mode=block”. This header is used to stop pages from loading when they detect reflected cross-site scripting (XSS) attacks.	PR.PT-4

11.5.8	The HTTP headers **must** include “Strict-Transport-Security: max-age=63072000; includeSubdomains; preload”	PR.DS-2
11.5.9	Required HTTP methods (e.g. GET, POST) **must** be explicitly allow listed with all other methods denied.	PR.PT-3
11.5.10	Requests containing unexpected User-Agent values or User-Agents from known exploitation tools **must** be filtered.	PR.DS-6
11.5.11	All JavaScript libraries, cascading style sheets and web fonts **must** be hosted by the application and not retrieved from an external provider.	PR.DS-1

11.6 Files and Resource Verification

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	URL redirects and links **must** show a warning when redirecting to potentially untrusted content.	PR.DS-5
11.6.2	Untrusted file data submitted to the application **must** not be used directly with file input / output commands.	PR.DS-5
11.6.3	Files obtained from an external source **must** be transformed into another format in order to disable any malicious content, before the file is passed to its destination, in line with NCSC Secure Design Principles [see External References].	DE.CM-4
11.6.4	Untrusted data **must** not be used within cross-origin resource sharing (CORS).	PR.PT-4
11.6.5	Files obtained from untrusted sources **must** be stored outside of the web root, with limited permissions.	PR.AC-4
11.6.6	Client-side technologies not supported natively by W3C browser standards **must** not be used.	PR.PT-4

11.7 Logging Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Input validation failures **must** result in request rejection on the server and be logged.	PR.PT-1
11.7.2	All customer authentication failures **must** be logged, as well as details of any decisions made to rate-limit or lock-out the login attempts, without storing sensitive session IDs or passwords.	PR.PT-1
11.7.3	Access control decisions for all components **must** be logged, including ones with a successful outcome.	PR.PT-1
11.7.4	Access to sensitive data, such as a customer's record, **must** be logged.	PR.PT-1
11.7.5	Customer transactions **must** be logged in line with SS-034 Business Audit Security Standard [Ref. F].	PR.PT-1
11.7.6	Log information **must** also be logged for web servers that support the execution of programs, scripts, and plug-ins.	PR.PT-1
11.7.7	All components in the application deployment **must** be configured to log events in accordance with SS-012 Protective Monitoring Security Standard [Ref. K].	PR.PT-1

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	11.1.2, 11.1.3
ID.GV-1	Organizational cybersecurity policy is established and communicated	11.1.5
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.1.8
PR.AC-3	Remote access is managed	11.3.2, 11.3.3, 11.3.10
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.4, 11.1.8, 11.2.6, 11.2.9, 11.3.1, 11.6.5
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.3.2, 11.3.3
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.1.6
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)	11.5.2
PR.DS-1	Data-at-rest is protected	11.1.7, 11.3.7, 11.3.8, 11.4.9, 11.5.11

PR.DS-2	Data-in-transit is protected	11.2.7, 11.2.8, 11.3.5, 11.3.6, 11.5.1, 11.5.8, 11.5.12
PR.DS-5	Protections against data leaks are implemented	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.3.4, 11.4.1, 11.4.5, 11.6.1, 11.6.2
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.4.1, 11.4.2, 11.4.4, 11.4.6, 11.4.7, 11.4.8, 11.4.10, 11.5.10
PR.IP-6	Data is destroyed according to policy	11.3.9
PR.IP-12	A vulnerability management plan is developed and implemented	11.1.1, 11.1.9
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.1.1
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.7.1, 11.7.2, 11.7.3, 11.7.4, 11.7.5, 11.7.6, 11.7.7
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.5.4, 11.5.9
PR.PT-4	Communications and control networks are protected	11.5.3, 11.5.5, 11.5.6, 11.5.7, 11.6.4, 11.6.6
DE.CM-4	Malicious code is detected	11.4.3, 11.6.3
DE.CM-8	Vulnerability scans are performed	11.1.9

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-033 Security Patching Standard	Yes
B	SS-025 Virtualisation Security Standard	Yes
C	SS-008 Server Operating System Security Standard	Yes
D	SS-001 pt.1 Access & Authentication Security Standard	Yes
E	SS-001 pt.2 Privileged User Access Security Standard	Yes
F	SS-034 Business Audit Security Standard	Yes
G	SS-007 Use of Cryptography Security Standard	Yes
H	SP-006 Channel Encryption and Mutual Authentication Security Pattern	No
I	SS-028 Microservices Architecture Security Standard	Yes
J	SS-005 Database Management Systems Security Standard	Yes
K	SS-012 Protective Monitoring Security Standard	Yes
L	SS-036 Secure Sanitisation and Destruction Security Standard	Yes
M	SS-015 Malware Protection Security Standard	Yes
N	Cookies and DWP Digital Services Policy	No
O	Security Assurance Strategy	No
P	SS-027 Security Testing Standard	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
CESG Good Practice Guide No. 44 – "Authentication and Credentials for use with HMG Online Services"
NCSC Secure Design Principles
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
XSS	Cross-Site Scripting
CDN	Content Delivery Network
UI/UX	User Interface / User Experience
NINO	National Insurance Number
URL	Uniform Resource Locator
CORS	Cross-Origin Resource Sharing
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
LoA	Level of Assurance
TLS	Transport Layer Security
XML	Extensible Markup Language
NACL	Native Client
W3C	World Wide Web Consortium
SOAP	Simple Object Access Protocol
JSON	JavaScript Object Notation
CSRF	Cross-Site Request Forgery
REST	Representational State Transfer
WS-Security	Web Service - Security

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Content Delivery Network (CDN)	A distributed network of proxy servers used to serve content to end users with high availability and high performance.
Content-Security-Policy	A HTTP response header which helps to mitigate cross-site scripting risks by declaring what dynamic resources are allowed to load.
Cross-Origin Resource Sharing (CORS)	A mechanism which allows restricted resources (e.g. fonts) on a web page to be requested from another domain.
Cross-Site Request Forgery (CSRF)	An attack that tricks the user into submitting a malicious request, inheriting the identity and privileges of the victim to perform an undesired function on the victim's behalf.
Cross-Site Scripting (XSS)	A type of injection attack in which malicious scripts are injected into otherwise trusted web sites.
DDoS	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Entropy	A measure of unpredictability. Low entropy indicates a highly predictable stream, while high entropy indicates a random or pseudo-random nature.
Level of Assurance (LoA)	The level of confidence we have that a user's claimed identity is authentic. Defined in CESG Good Practice Guide No. 44 – "Authentication and Credentials for use with HMG Online Services".
Microservices Layer	Components that implement the business logic underpinning DWP products and services, presented to the customer via the UI/UX functions. Also known as the "business logic tier".
REST	Representational State Transfer; an API architecture allowing requesting systems to access and / or manipulate textual representations of resources using a predefined set of stateless operations.
RESTful Web Service	A web service implementing REST.
Transport Layer Security (TLS)	An IETF-standardised suite of protocols used to protect the confidentiality and integrity of application-layer communication during transit.
User Interface / User Experience (UI/UX) Functions	Components that serve to present various types of user interfaces (UIs) to the end users of the service. Also known as the "presentation tier".

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/

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

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