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

Chief Security Office

Date: 11/12/2025

Department for Work & Pensions

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 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:

Government Publications 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).

(Important note for screen reader users.) Paragraphs that contain a **'must'** statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains 'must' activities.

Table – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
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. 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 security controls 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	26/10/2023

Version	Author	Description	Date
		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	
2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments	11/12/2025

Version	Author	Description	Date
		Approval history - Review period changed to up to 2 years Scope – wording change for clarity; added references to other security standards 11.1.1 Libraries; software update sources 11.1.6 Password reuse 11.1.8 All 11.1.9 Where possible, anti-DDoS attack protection 11.1.10 User training; Refs added to software development standard and Engineering knowledge base 11.1.11 SBoM 11.2.2 API / application layer 11.2.4 Removed separate interface requirement 11.2.5 Ref added to Privileged User Access standard 11.2.8 Post-quantum crypto 11.2.9 Service accounts, machine IDs; unique, not shared 11.2.10 Cloud environment baselines and monitoring 11.2.11 Network controls for traffic flow 11.3.2 CDNs and Anti-DDoS measures 11.3.3 CDN / AntiDDoS functions 11.3.6 Sensitive info in POST and GET requests 11.3.9 ‘Server’ removed 11.4 Input handling and validation	

Version	Author	Description	Date
		11.4.10 ZIP replaced with archive 11.4.11 Validation of variables 11.4.12 Pre-commit hooks 11.5.4 Error pages 11.6.7 Third party libraries and open source components 11.6.8 SBoM and vulnerability scanning tools 11.7 Output Encoding 11.8 API and Microservices Security 11.9 Securing AI & Machine Learning Components 11.10.8 Privileged user actions 11.10.9 Code exfiltration monitoring and filtering Internals Refs – Refs added for Virtualisation; Cloud Computing; Software Development; Engineering knowledge base Internal Refs – Approved Crypto Algorithms External Refs - OWASP Top 10 for LLM Applications	

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	26/05/2017
2.0		Chief Security Officer	26/10/2023
2.1		Chief Security Officer	11/12/2025

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. O].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

(Important) this paragraph contains ‘must’ activities.

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

(Important) this paragraph contains ‘must’ activities.

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

(Important) this paragraph contains ‘must’ activities.

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 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 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

(Important) this paragraph contains ‘must’ activities.

This standard applies to all web-based applications 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.

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”.

Other security standards relevant to this standard that **must** also be read are listed below;

- SS-003 Secure Software Development [Ref. S]
- SS-009 Hypervisor [Ref. Q]
- SS-023 Cloud Computing [Ref. R]
- SS-025 Virtualisation [Ref. B]

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

(Important) this paragraph contains ‘must’ activities.

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

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	All applicable software (web server, database, libraries etc.) **must** adhere to SS-033 Security Patching Standard [Ref. A]. All software updates **must** come from verified sources.	PR.PS-02
11.1.2	Web applications in a virtualised environment, **must** adhere to SS-025 Virtualisation Security Standard [Ref. B]	GV.PO-02
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]).	GV.PO-02
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.AA-05

11.1.5	All dependencies (e.g. software libraries, external systems) **must** be identified and documented wherever possible.	ID.AM-02
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], and **must not** be reused across multiple applications.	PR.AA-01 PR.AA-03
11.1.7	Web servers **must not** be used to store PII or business data at OFFICIAL or above. 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].	PR.DS-01
11.1.8	All 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.AA-03 PR.AA-05

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** where possible include protection against Distributed Denial-of-Service (DDoS) attacks, such as cloud-based scrubbing or content delivery network providers, or implementing rate limiting and traffic filtering at the network edge.	DE.CM-09
11.1.10	Strict adherence to secure development practices **must** be supported by user training, in line with SS-003 Secure Software Development standard [Ref. S] and the DWP Engineering Knowledge Base [Ref. T].	PR.PS-06 PR.AT-02
11.1.11	A complete and up-to-date inventory of all third-party software components, libraries, and upstream services, in the form of a Software Bill of Materials (SBoM), **must** be maintained for the application. This inventory **must** be regularly and automatically monitored against known vulnerability databases, and a formal process **must** be in place to manage the risk from identified vulnerabilities in line with SS-033 Security Patching Standard [Ref. A].	PR.PS-02

11.2. Architectural Considerations

(Important) this table contains 'must' activities.

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-01 PR.DS-02 PR.DS-10
11.2.2	The business logic functions (the "API / application layer") **must** be logically or physically separated from all other components.	PR.DS-01 PR.DS-02 PR.DS-10
11.2.3	The systems storing necessary data (the "application") **must** be logically or physically separated from all other components.	PR.DS-01 PR.DS-02 PR.DS-10
11.2.4	Each layer **must** have access to an administration interface. Software updates and other necessary Internet access outbound **must** be directed through this interface.	PR.DS-01 PR.DS-02 PR.DS-10 PR.IR-01
11.2.5	Software updates and other necessary Internet access outbound **must** either: a) Be directed through the administration interface; or (in line with SS-001-2 Privileged User Access standard [Ref. E]) Be allowlisted to travel via the untrusted network with all other unnecessary destinations implicitly blocked.	PR.IR-01

Reference	Minimum Technical Security Measures	NIST ID
11.2.6	Access control and error handling logic **must** deny access by default.	PR.AA-02 PR.AA-04
11.2.7	Communication between components **must** be cryptographically protected in transit. This cryptographic protection **must** be applied in accordance with SS-007 Use of Cryptography Security Standard [Ref. G].	PR.DS-02
11.2.8	Content served by the web server **must** be cryptographically protected by an approved implementation of Transport Layer Security (TLS) in line with SS-007 Use of Cryptography Security Standard [Ref. G]. SP-006 Channel Encryption and Mutual Authentication Security Pattern [Ref. H] **must** be consulted for implementation. For new systems processing sensitive data with a required confidentiality lifespan exceeding ten years, a technology roadmap for migration to NCSC-approved Post-Quantum Cryptography (PQC) algorithms **must** be developed and maintained as part of the system's security architecture documentation. Please refer to the DWP Approved Cryptographic Algorithms document [Ref. U] for further information.	PR.DS-02
11.2.9	The web server process **must** run as its own user account (including service accounts, machine IDs or real users) in its own user group with the minimum necessary privileges to successfully operate, and **must** be unique to this service and not shared.	PR.AA-05

Reference	Minimum Technical Security Measures	NIST ID
11.2.10	All Authority cloud environments (IaaS/PaaS) **must** be configured in accordance with a documented, Authority -approved secure baseline and in line with SS-023 Cloud Computing Security Standard [Ref. R]. These environments **must** be continuously monitored for configuration drift and security misconfigurations using an approved Cloud Security Posture Management (CSPM) capability.	PR.PS-06
11.2.11	Network security controls in cloud environments **must** leverage cloud-native capabilities (e.g. Security Groups, Network ACLs, private endpoints) and follow a principle of micro-segmentation to restrict traffic flow between components and tiers to the minimum necessary for operation. For multi-cloud components, a Cloud Access Security Broker (CASB) **must** be used.	PR.IR-01

11.3. User interface /User Experience (UI/UX) Functions

Further information for UI/UX requirements can be found in the Architecture Blueprint (Important) this table contains ‘must’ activities.

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.IR-01
11.3.2	When using a Content Delivery Network (CDN) or Anti-DDoS measures, the security controls between an untrusted network and the UI/UX functions **must** restrict inbound traffic to that originating from the CDN provider. Where utilised, CDNs **must** follow the requirements in this standard.	PR.IR-01
11.3.3	The security controls between an untrusted network and the UI/UX functions **must** deny new connections not originating from the CDN / Anti-DDoS functions.	PR.IR-01
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.IR-01
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.IR-01

11.3.6	When dealing with sensitive information (including personal data, session cookies and other secrets); • In POST / PUT requests sensitive data **must** be transferred in the request body. • In GET requests sensitive data **must** be transferred in an HTTP Header.	PR.DS-02
11.3.7	Caching of personal information **must** be disabled with the use of “cache-control” and “pragma” HTTP headers.	PR.DS-01
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-01 PR.DS-10
11.3.9	If infrastructure is being decommissioned, any resident data **must** be deleted in line with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. L].	PR.DS-01 PR.PS-03
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.AA-02 PR.AA-04

11.4. Input Handling and Validation

(Important) this table contains ‘must’ activities.

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.	ID.RA-09
11.4.2	XML or JSON **must** be validated against a schema before being accepted as input.	ID.RA-09
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.	ID.RA-09
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.	ID.RA-09
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-02 PR.IR-01
11.4.6	Input validation and sanitisation **must** take place on the server-side, but also be enforced on the client-side.	PR.DS-01
11.4.7	Input validation failures **must** result in request rejection and be logged.	PR.DS-01

Reference	Minimum Technical Security Measures	NIST ID
11.4.8	The application **must** have defence against HTTPS parameter pollution attacks, e.g., receiving unexpected values in cookies or headers.	PR.DS-01
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-01
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 archive file uploads (if supported by websites) **must** be checked for malware before opening.	PR.DS-01
11.4.11	All variables in a web application **must** be protected, undergo appropriate validation, and then sanitised.	PR.DS-01
11.4.12	Pre-commit hooks **must** be utilised to enforce secure coding practices and reduce the risk of insider threats or accidental data exposure, including; • Syntax and formatting checks • Secure development focused rules • Code repository hygiene • Code commit integrity • Pipeline execution enforcement • Auditability	PR.DS-01

11.5. HTTP(S) Security

The security measures in this section refer to HTTPS security.

(Important) this table contains must activities

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-02
11.5.2	HTTP headers added by a trusted proxy or CDN provider **must** be authenticated by the application.	PR.AA-03
11.5.3	A Content Security Policy **must** be applied to prevent the loading of third-party scripts, stylesheets and plugins.	PR.PS-05
11.5.4	HTTP headers, error pages, or any part of the HTTP response **must** not reveal version information of system components.	PR.DS-02
11.5.5	The HTTP headers **must** include “X-Frame-Options: DENY”. This header is used to prevent clickjacking attacks.	PR.IR-01
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.IR-01
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.IR-01

Reference	Minimum Technical Security Measures	NIST ID
11.5.8	The HTTP headers **must** include “Strict-Transport-Security: max-age=63072000; include Subdomains; preload”	PR.DS-02
11.5.9	Required HTTP methods (e.g. GET, POST) **must** be explicitly allow listed with all other methods denied.	PR.IR-01
11.5.10	Requests containing unexpected User-Agent values or User-Agents from known exploitation tools **must** be filtered.	PR.IR-01
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.IR-01

11.6. Files and Resource Verification

(Important) this table contains ‘must’ activities.

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.IR-01
11.6.2	Untrusted file data submitted to the application **must** not be used directly with file input / output commands.	PR.IR-01
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].	PR.IR-01

11.6.4	Untrusted data **must** not be used within cross-origin resource sharing (CORS).	PR.IR-01
11.6.5	Files obtained from untrusted sources **must** be stored outside of the web root, with limited permissions.	PR.IR-01
11.6.6	Client-side technologies not supported natively by W3C browser standards **must not** be used.	PR.IR-01
11.6.7	Third party libraries and open source components **must** be checked for vulnerabilities.	ID.RA-09
11.6.8	Software Bill of Materials (SBOM) and dependency vulnerability scanning tools **must** be utilised to assist with mitigating the threat of unpatched components and libraries.	ID.AM-02 ID.AM-07

11.7. Output Encoding

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Output encoding is recommended, as is use of output encoding frameworks or libraries.	PR.IR-01
11.7.2	Variables **must not** be interpreted as code instead of text. All variables used in the user interface **must** be passed through an output encoding function.	PR.IR-01
11.7.3	Ensure the correct output encoding methods are utilised, as browsers parse HTML, JavaScript, URLs and Cascading Style Sheets (CSS) differently, and using the wrong method may introduce weaknesses.	PR.IR-01

11.7.4	HTML sanitisation **must** be employed to strip dangerous HTML from variables to return a safe string of HTML.	PR.IR-01
11.7.5	HTML attribute encoding **must** be applied to variables being placed in HTML attributes.	PR.IR-01
11.7.6	Variables **must** be enclosed within quotation marks in order to make it difficult to change the context a variable operates in, to reduce the risk of cross-site scripting.	PR.IR-01
11.7.7	For JavaScript contexts, variables **must only** be placed inside a ‘quoted data value’. All other contexts are unsafe and variable data **must not** be placed in them.	PR.IR-01
11.7.8	For Cascading Style Sheet (CSS) contexts, variables **must only** be placed in a CSS property value. Other “CSS Contexts” are unsafe and variable data **must not** be placed in them.	PR.IR-01
11.7.9	For URL contexts, all characters **must** be encoded using the %HH encoding format, ensuring any attributes are fully quoted.	PR.IR-01
11.7.10	Content Security Policies (CSPs) that prevent content from being loaded via an allowlist, may be utilised as part of a defence in depth strategy as long as they; • Are custom built for each application • Restrict inline scripts • Restrict remote scripts from arbitrary servers • Restrict unsafe JavaScript • Restrict form submissions • Restrict objects	PR.IR-01

11.8. API and Microservices Security

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	API endpoints that accept object identifiers **must** implement and enforce object-level authorisation checks within the business logic to verify the authenticated user has permission to perform the requested action on the specific object.	PR.AA-03 PR.AA-05
11.8.2	The application **must** validate, filter, and sanitise all user-supplied data in URLs and request parameters used to interact with remote resources.	PR.PS-06
11.8.3	All API requests **must** be made through a dedicated, hardened proxy in line with SS-003 Secure Software Development standard [Ref. S] that enforces layer 4 filtering, throttling, and allows only intended protocols.	PR.DS-02
11.8.4	A comprehensive inventory of all APIs, including their version, environment (e.g., production, staging), and exposure (internal/external), **must** be maintained and regularly reviewed in line with SS-003 Secure Software Development standard [Ref. S]. Deprecated API versions **must** be formally retired and disabled from all environments in a timely manner.	ID.AM-02

11.9. Securing AI & Machine Learning Components

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Systems utilising Large Language Models (LLMs) **must** treat all LLM outputs as untrusted input and subject them to validation and sanitisation before being processed by other system components or displayed to users.	PR.PS-06
11.9.2	Where LLMs are used, systems **must** implement mechanisms to filter user prompts to prevent prompt injection attacks. Furthermore, strict, context-aware access controls **must** be enforced on the data, tools, and APIs the LLM can access, following the principle of least privilege.	PR.AA-05 PR.PS-06

11.10. Logging requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	Input validation failures **must** result in request rejection on the server and be logged.	DE.CM-09
11.10.2	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.	DE.CM-09
11.10.3	Access control decisions for all components **must** be logged, including ones with a successful outcome.	DE.CM-09

11.10.4	Access to sensitive data, such as a customer's record, **must** be logged.	DE.CM-03
11.10.5	Customer transactions **must** be logged in line with SS-034 Business Audit Security Standard [Ref. F].	DE.CM-09
11.10.6	Log information **must** also be logged for web servers that support the execution of programs, scripts, and plug-ins.	DE.AE-03
11.10.7	All components in the application deployment **must** be configured to log events in accordance with SS-012 Protective Monitoring Security Standard [Ref. K].	DE.CM-09
11.10.8	All privileged user actions, including administrative or development access, **must** be logged.	DE.CM-03
11.10.9	Monitoring or content filtering **must** be in place to detect exfiltration of code to external locations or repositories.	PR.DS-02

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
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organisational mission	11.1.2, 11.1.3
ID.AM-02	Inventories of software, services, and systems managed by the organisation are maintained	11.1.5, 11.6.8, 11.8.4
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	11.6.8
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.6.7

PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	11.1.6
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.2.6, 11.3.10
PR.AA-03	Users, services, and hardware are authenticated	11.1.6, 11.1.8, 11.5.2, 11.8.1
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.2.6, 11.3.10
PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.1.4, 11.1.8, 11.2.9, 11.8.1, 11.9.2
PR.AT-02	Individuals in specialised roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	11.1.10

PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.1.7, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.3.7, 11.3.8, 11.3.9, 11.4.6, 11.4.7, 11.4.8, 11.4.9, 11.4.10, 11.4.11, 11.4.12
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.7, 11.2.8, 11.3.6, 11.4.5, 11.5.1, 11.5.4, 11.5.8, 11.8.3, 11.8.9
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.3.8
PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.2.4, 11.2.5, 11.2.11, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.4.5, 11.5.6, 11.5.7, 11.5.9, 11.5.10, 11.5.11, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.7.1, 11.7.2, 11.7.3, 11.7.4, 11.7.5, 11.7.6, 11.7.7, 11.7.8, 11.7.9, 11.7.10
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.1, 11.1.11
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	11.3.9

PR.PS-05	Installation and execution of unauthorised software are prevented	11.5.3
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	11.1.0, 11.2.10, 11.8.2, 11.9.1, 11.9.2
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.10.4, 11.10.8
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.1.9, 11.10.1, 11.10.2, 11.10.3, 11.10.5, 11.10.7
DE.AE-03	Information is correlated from multiple sources	11.10.6

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-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

Ref	Document	Publicly Available*
N	GDS Service Manual guide to cookies	No
O	Security Assurance Strategy	No
P	SS-027 Security Testing Standard	No
Q	SS-009 Hypervisor Security Standard	Yes
R	SS-023 Cloud Computing Security Standard	Yes
S	SS-003 Secure Software Development standard	Yes
T	DWP Engineering Knowledge Base	No
U	DWP Approved Cryptographic Algorithms	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
CIS Critical Security 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
OWASP Top 10 for LLM Applications

Appendix D Abbreviations

Table 5– 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 6 – 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.

Term	Definition
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 Accessibility Policy

DWP Accessibility Manual

Guidance and tools for digital accessibility

Understanding accessibility requirements for public sector bodies