Security Standard
Cloud Computing
(SS-023)

Chief Security Office

Date: 21/11/2023

Department
for Work &
Pensions

This Cloud Computing 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 issue	20/03/2017
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 • All security measures have been updated and document reformatted • Split between CSP and SO responsibilities for easer of reference	21/11/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	14/03/2017
2.0		Chief Security Officer	21/11/2023

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. I].
- 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 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 that utilise cloud computing.

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 Cloud Computing Security Standard defines the minimum technical security measures that **must** be implemented to secure Cloud based services to an Authority approved level of security.

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 cloud computing requirements are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with cloud computing, 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 systems and services utilising cloud computing processing Authority data 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 use of cloud computing within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

Throughout this document, the terms Authority System or Service Owner (SO) and Cloud Service Provider (CSP) are used extensively. Where security measures are split between the SO and CSP, these are described alongside each other to clearly show differing responsibilities.

A guiding principle for this document is that for any cloud deployment, the cloud services control plane, and the data plane of the Authority /SO **must** have strong separation.

The following standards **must** be read in conjunction with SS-023 Cloud Computing.

- SS-001 pt.1 Access & Authentication
- SS-001 pt.2 Privileged User Access
- SS-003 Software Development
- SS-006 Security Boundaries
- SS-007 Use of Cryptography
- SS-012 Protective Monitoring (SaaS)
- SS-025 Virtualisation
- SS-035 Backup and Recovery
- SS-036 Secure Sanitisation and Destruction

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

11. Minimum Technical Security Measures

The following sections define 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.

Please note that for ease of reference, the security measures below have been split to indicate which are the responsibility of the Cloud Service Provider (CSP) and those of the System Owner (SO).

12. Protection of Data in Transit

12.1 Encryption and Authentication

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
12.1.1	The cloud service provider (CSP) **must** use Transport Layer Security (TLS) 1.2 or higher to provide data confidentiality and integrity for communications between the customer and the cloud, and internally between their own systems and data centres. The CSP should also deploy certificate pinning and HTTP Strict Transport Security where possible. Please refer to SS-007 Use of Cryptography for approved Cryptographic controls [Ref. A].	(No additional security measures)	PR.DS-2
12.1.2	The CSP **must** provide assurances that data is protected in transit within their service, as well as when it is accessed via external interfaces. This includes where data is moved between physical data centres.	SOs **must** request assurances from the CSP that data is protected in transit within their service, as well as when it is accessed via external interfaces. This includes where data is moved between CSP physical data centres.	PR.DS-2

12.1.3	The CSP **must** not be able to access the data plane (i.e., customer-based resources). Only access to the control plane (management and orchestration to cloud environments) is permitted.	SOs must commission an ITHC along with a Controls Assessment to ensure that this requirement is satisfied.	PR.AC-2
12.1.4	(No additional security measures)	Bare metal cloud services **must** be avoided, and IaaS **must** be the preferred choice for utilising virtualisation.	PR.DS-5
12.1.5	(No additional security measures)	It **must** only be possible to connect to the KMS (Key management service) using an approved protocol with secure settings, in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-2
12.1.6	(No additional security measures)	All accesses made to a cloud service **must** be authenticated and SOs **must** be confident that all data flows are authenticated and encrypted as described above. Please also refer to SS001-1 Access & Authentication [Ref. J] for approved controls.	PR.AC-7

12.2 Cryptographic Controls

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
12.2.1	Cryptographic controls implemented by the CSP **must** be in line with SS-007 Use of Cryptography Security Standard [Ref. A].	SOs **must** implement cryptographic controls in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-1

12.3 PKI & Key Management

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
12.3.1	If the CSP provides PKI & Key Management services, it **must** be responsible for the encryption and key management used to protect data in transit. This also includes backup of keys, rotation of keys, deletion and revocation of keys, and monitoring and logging access to encryption keys.	SOs **must** use the Authority Enterprise Key Management solution and not implement their own, and **must** prohibit the CSP from storing and managing the same cryptographic keys. Please refer to SS-002 PKI & Key Management Security Standard [Ref. B] for the minimum-security measures.	PR.DS-2

13. Asset Security and Resilience

13.1 Encryption for Data at Rest

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
13.1.1	Data at rest **must** be adequately safeguarded against unauthorised access by parties with physical access to infrastructure, in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. J].	SOs **must** implement cryptographic controls for data at rest in line with SS-007 Use of Cryptography Security Standard [Ref. A]. See minimum security requirements and 12.2 Cryptographic Controls within this standard for further guidance.	PR.DS-1

13.2 Physical Sites and Legal Authority

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
13.2.1	There **must** be assurances that the CSP or any third parties do not retain copies of sensitive data or PII for such purposes as machine learning, marketing, and advertising.	Data sovereignty **must** be within the UK region. SOs **must** obtain assurances from the CSP that if data is being stored, processed, and maintained within the UK, their actions **must** comply with contractual obligations and all applicable laws, such as the UK Data Protection Act (DPA) 2018 and Regulation (EU) 2016/679: The General Data Protection Regulation (GDPR). If for any reason, data is located outside the UK region, exceptions **must** be raised through the correct procedures.	PR.DS-1

13.2.2	(No additional security measures)	Application software used within a PaaS or IaaS cloud computing platform will be owned by the SOs/Authority. The Authority's Data Protection Policy and any relevant legal frameworks **must** be adhered to when transferring any data that contains personally identifiable information (PII) or any other sensitive information.	ID.AM-2

13.3 Data Centre Security

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
13.3.1	The CSP **must** provide evidence, such as a SOC 2 report, that their physical security measures to their data centres mitigate against unauthorised access, tampering, theft, or reconfiguration of systems.	SOs **must** have assurances that these security measures are in place.	PR.AC-2

13.4 Sanitisation of Data and Disposal of Equipment

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
13.4.1	The CSP **must** disclose information about the processes and techniques they (or their suppliers) use to sanitise data and destroy equipment prior to disposal.	SOs **must** request confirmation that the CSP has policies and procedures in place for secure disposal of resources in line with SS-036 - Secure Sanitisation and Destruction [Ref. C].	PR.DS-3 PR.IP-6
13.4.2	Unauthorised access to Authority data **must** not occur during the provisioning, transferring, or de-provisioning of resources.	(No additional security measures)	PR.DS-1 PR.DS-3
13.4.3	When resources are transferred, re-provisioned, or requested for data to be sanitised or securely destroyed, there **must** be assurances from the CSP that these actions have been completed successfully.	(No additional security measures)	PR.DS-3 PR.IP-6
13.4.4	At the end of its life, storage media **must** be sanitised or securely destroyed in line with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. C], and assurances from the CSP **must** be provided when this has been achieved.	SOs **must** ensure that CSPs meet this requirement.	PR.DS-3 PR.IP-6

13.4.5	The CSP **must** provide proof of a recognised standard for equipment disposal or the use of a third-party destruction service that has been assessed against a recognised standard, in line with SS-036 Secure Sanitisation and Destruction Security Standard [Ref. C].	(No additional security measures)	PR.DS-3 PR.IP-6

13.5 Availability

For information on backups in cloud environments, please refer to SS-035 Secure Backup and Recovery Security Standard [Ref. D].

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority/System Owner Responsibility**	
13.5.1	There **must** be assurances that the CSPs commitment to availability, particularly its capacity for outages, satisfies the Authority's requirements as per commercial agreement.	(No additional security measures)	PR.DS-4
13.5.2	There **must** be service level agreements (SLAs) or contractual commitments from the CSP that will meet the Authority's availability requirements as per commercial agreement.	(No additional security measures)	ID.SC-3

14. Separation Between Users

14.1 Boundary Protection

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
14.1.1	The CSP **must** provide assurances that security boundaries implemented by themselves allow SOs control of who can access data and how, in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. J], SS-001 pt.2 Privileged User Access Security Standard [Ref. M], and SS-006 Security Boundaries Standard [Ref. L].	(No additional security measures)	PR.AC-4
14.1.2	(No additional security measures)	Boundary controls **must** be implemented, (as per SS-006 Security Boundaries Standard [Ref. L]) as custom code can be executed within these services.	PR.AC-4
14.1.3	(No additional security measures)	SOs **must** be aware of the separation methods utilised for each service they employ, and suitability for their purposes.	PR.AC-4

14.2 Separation of Storage

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
14.2.1	Cloud services that are utilised **must** have a deny access to stored objects by default and **must** be integrated with role-based access controls in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. J].	(No additional security measures)	PR.AC-4
14.2.2	Cloud services that are utilised **must** use encryption for stored data by default. See section 13.1 Encryption for Data at Rest for minimum security requirements.	(No additional security measures)	PR.DS-1

14.3 Separation Flow of Network

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
14.3.1	Cloud services that are utilised **must** allow greater control over data flows managed by the CSP, as well as the ability to detect anomalous traffic more easily.	(No additional security measures)	ID.AM-3

15. Hypervisor and Virtualisation Security

(SS-023 Cloud Computing Standard **must** be read in conjunction with SS-009 Hypervisor Security Standard [Ref. G] and SS-025 Virtualisation Security Standard [Ref. H]).

15.1 Segregation in Virtual Computing Environments

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
15.1.1	The SOs virtual environment running on a cloud service **must** be protected from access by other cloud service customers and unauthorised persons.	(No additional security measures)	ID.SC-3
15.1.2	The CSP must prevent any co-tenants (i.e. other customers) from monopolising shared resources such as bandwidth or CPU.	(No additional security measures)	ID.AM-5
15.1.3	The CSP **must** apply information security controls where the cloud service involves multi-tenancy to ensure proper resource isolation between tenants, such as customer data, virtualised applications, operating systems, storage, and network infrastructure.	(No additional security measures)	ID.SC-3
15.1.4	The CSP **must** consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the CSP.	(No additional security measures)	ID.SC-3

15.2 Virtual & Physical Machine Hardening

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
15.2.1	When configuring virtual machines, SOs and CSPs **must** ensure that appropriate aspects are hardened (e.g. underlying hardware, BIOS, only necessary ports, protocols, and services are enabled etc.) and that appropriate technical measures (e.g., anti-malware, logging) are in place for each virtual machine used. (For minimum security controls please refer SS-025 Virtualisation Security Standard [Ref. H]).		PR.DS-5
15.2.2	Mechanisms and safeguards **must** be developed and implemented by SOs and CSPs, to prevent human interference from accidentally or intentionally erasing, shutting down virtual servers, or destroying virtual assets as stipulated in the standards scope (i.e. CSPs manage the control plane, SOs manage the data plane).		PR.DS-5
15.2.3	The CSP is responsible for all elements of physical security e.g. access to data centres and physical assets),	(No additional security measures)	PR.AC-2 PR.AC-5 PR.IP-5
15.2.4	(No additional security measures)	The SO **must** verify the CSP is providing all the agreed secure services/components, supported by a risk assessment or ITHC.	ID.SC-3

16. Governance Framework

It **must** be defined between SOs and the CSP which information security controls are managed by whom.

16.1 Co-ordination and Management of Cloud Services

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
16.1.1	(No additional security measures)	SOs **must** define or expand existing system-specific policies and procedures to reflect its use of cloud services and make cloud service users aware of their roles and responsibilities in the cloud service's use.	ID.GV-1 ID.GV-2
16.1.2	The management of the cloud service and the data it contains **must** be coordinated and directed by the CSPs security governance framework.	(No additional security measures)	ID.SC-3
16.1.3	The CSP **must** have a framework for security governance and risk management that is formalised, with regulations governing important information security issues that are pertinent to the service.	SO **must** understand the CSPs operating procedures in order to design Authority services that take account of these in order to meet Authority business requirements.	ID.SC-1

17. Operational Security

17.1 Vulnerability & Patch Management

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
17.1.1	The CSP **must** have a vulnerability management process in place to identify, triage and mitigate vulnerabilities in all components of the service that they are responsible for, in line with SS-033 Security Patching Standard [Ref. E].	SOs **must** identify the technical vulnerabilities and patch management tasks they will be responsible for, and clearly define a process for overseeing them. Please Refer to SS-033 Security Patching Standard [Ref. E] for minimum security requirements.	PR.IP-12

17.2 Protective Monitoring & Logging

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
17.2.1	There **must** be assurances that the CSP monitors for attacks, misuse, and malfunctions to assist it in detecting successful and unsuccessful attacks on the CSP service.	SOs **must** define monitoring and event logging requirements when utilising SaaS offerings and ensure that the CSP meets those requirements. Please refer to SS-012 Protective Monitoring Security Standard [Ref. F].	DE.CM-1 DE.CM-7
17.2.2	SOs **must** be assured that the CSP generates enough audit events to enable effective detection of suspicious activity, that these events are analysed to uncover potential breaches or improper usage of the service, and that the CSP reacts to incidents in a prompt and appropriate manner.	(No additional security measures)	PR.PT-1

17.2.3	(No additional security measures)	SOs **must** be able to monitor specific aspects of the operation of the cloud services that they utilise.	DE.CM-6
17.2.4	To prevent information security incidents caused by resource shortages, the CSP **must** monitor total resource capacity, and generate alerts to SOs accordingly.	(No additional security measures)	PR.DS-4

17.3 Configuration and Change Management

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
17.3.1	In order to identify and manage changes that could affect the security of the service and mitigate known vulnerabilities, the CSP **must** be aware of the assets that comprise their service, as well as their configurations and dependencies.	(No additional security measures)	PR.IP-3
17.3.2	(No additional security measures)	SOs **must** be confident that CSP service changes are managed and monitored through to completion after being evaluated for potential security impacts.	PR.IP-3
17.3.3	(No additional security measures)	SOs **must** be confident that unauthorised CSP changes to deployed service components and their configuration will be detected and prevented.	PR.IP-3
17.3.4	The CSP **must** give SOs appropriate notice before making changes that could affect how they use the service, or their ability to use the service.	(No additional security measures)	PR.IP-3

17.3.5	CSPs **must** implement all technical changes automatically and consistently throughout their infrastructure.	(No additional security measures)	PR.IP-3

17.4 Incident Management

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
17.4.1	The CSP **must** have incident management processes in place in line with SS-014 Security Incident Management Standard [Ref. N], and supported by appropriate Service Level Agreements to increase the likelihood of effective and timely decisions being made when security incidents occur.	(No additional security measures)	PR.IP-9
17.4.2	(No additional security measures)	SOs and outside parties **must** have a clear method and contact point to report security issues and vulnerabilities to the CSP.	RS.CO-2
17.4.3	The CSP **must** inform SOs if they detect a security incident that affects their data in an acceptable agreed timescale.	(No additional security measures)	RS.CO-2

18. Personnel Security

18.1 Employees & Security Culture

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
18.4.1	The CSP **must** conduct security screening and regular security training for employees that have the ability to modify the service and **must** all be commensurate to their position and privileges.	(No additional security measures)	PR.AT-1 PR.AT-2 PR.AT-3
18.4.2	CSP staff **must** not have access to Authority data.	(No additional security measures)	PR.AC-2
18.4.3	CSP **must** implement the necessary access & authorisation controls for change management purposes.	SOs **must** be cognisant of CSP access and authorisation controls.	PR.AC-4

19. Secure Development

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
19.1.1	(No additional security measures)	The SO **must** request assurances from the CSP that their design, development, and deployment of their cloud services minimises and mitigates security vulnerabilities.	ID.SC-3 PR.IP-2

20. Secure User Management

20.1 Restriction of Permissions

Please refer to SS-001 pt.1 Access and Authentication Security Standard [Ref. J] for more detail on managing user access.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
20.1.1	The CSP **must** provide administration tools and access controls to enable SOs in maintaining the identities they use, limiting access to cloud services, cloud service features, and cloud service customers' data stored in those services.	(No additional security measures)	PR.AC-4
20.1.2	To avoid inconsistencies between various access controls, which may lead to confusion and unforeseen accesses, the CSP **must** have a single, cohesive access control system implemented.	(No additional security measures)	PR.AC-1 PR.AC-4
20.1.3	(No additional security measures)	SOs **must** be aware of all mechanisms by which the CSP accepts management or support requests from the Authority (telephone, web portal, etc.), and that only authorised personnel are permitted to use those mechanisms to affect the service.	PR.AC-3
20.1.4	CSPs **must** provide SOs the ability to apply time-bounded permissions for highly privileged accesses.	(No additional security measures)	PR.AC-4

20.1.5	Access to service interfaces **must** only be granted to those who have been authenticated and authorised.	(No additional security measures)	PR.AC-1 PR.AC-7
20.1.6	(No additional security measures)	Identity, authentication, and authorisation measures **must** provide SOs with the assurance that users have the right to access a given interface.	PR.AC-1 PR.AC-4 PR.AC-7
20.1.7	(No additional security measures)	SOs **must** be confident that: o they understand how access to external interfaces is authenticated. o the CSP enforces an up-to-date password policy and requires Authority users to employ multi-factor authentication (MFA) before they may access any resources. o the CSP performs equally robust authentication of Authority service identities as it does for users. o Authority user authentication will be integrated with Authority processes for managing joiners, movers, and leavers. o processes are in place for the management lifecycle of service credentials.	PR.AC-1 PR.AC-4 PR.AC-6 PR.AC-7

21. External Interface Protection

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
21.1.1	(No additional security measures)	All external or untrusted service interfaces **must** be identified and protected.	ID.AM-4
21.1.2	(No additional security measures)	SOs **must** have confidence that they know what physical and logical interfaces allow for access to information and how that access is restricted.	ID.AM-3
21.1.3	(No additional security measures)	SOs **must** have confidence that the cloud service identifies and authenticates users at the appropriate level across those interfaces.	PR.AC-7
21.1.4	(No additional security measures)	SOs **must** have assurances that interfaces from the CSP are designed to be resistant to attacks, especially interfaces exposed publicly (over the internet).	PR.PT-4
21.1.5	(No additional security measures)	SOs **must** be confident that the CSP has a continuous testing regime in place to ensure that CSP-owned external interfaces are secure.	ID.SC-4 DE.DP-3

22. Logging Information and Alerting

22.1 Audit Information

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
22.1.1	CSPs **must** enable the production and collection of log data required to investigate incidents involving the use of a service and the data contained within it.	SO's **must** be confident that these have been onboarded and are actioned appropriately.	PR.PT-1 DE.AE-3
22.1.2	The log information that is made available **must** meet the needs for investigating misuse or security incidents.	(No additional security measures)	DE.DP-2
22.1.3	Log information **must** be made available by the CSP for any personnel actions that have an impact on the service in use (or the data held within it).	(No additional security measures)	DE.CM-3 DE.DP-4
22.1.4	Log information **must** not be deleted by SOs or the CSP during a defined retention period.		PR.PT-1

22.2 Security Alerts

Please note Protective Monitoring of SaaS platforms falls within this standard.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
22.2.1	The CSP **must** alert SOs when compromises, malicious activity or vulnerabilities in the CSP services have been identified.	(No additional security measures)	DE.DP-4
22.2.2	CSP **must** notify the **Authority** of any security events that may impact the service, in line with SS-014 Security Incident Management Standard [Ref. N], and supported by appropriate Service Level Agreements.	(No additional security measures)	DE.DP-4

23. Secure Use of the Service

23.1 Security by Design and by Default

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider Responsibility	**Authority /System Owner Responsibility**	
23.1.1	The CSP **must** make it simple for SOs to deliver their services in a secure manner that is resistant to common attacks.	SOs are responsible for ensuring their services in the cloud environment are designed securely.	ID.SC-3
23.1.2	(No additional security measures)	SOs **must** understand which of the above security measures in this standard are met by the service's default configurations, and what **must** be done for those security measures that are not currently compliant.	PR.DS-5 PR.PT-4

23.1.3	(No additional security measures)	Authority staff **must** be appropriately trained in using and administering the service in accordance with Authority information security policies and standards.	PR.AT-1
23.1.4	The CSP **must** be responsible for updating the default settings for their service to address new risks (this may include altering the configuration of existing customers, as well as changing the starting point for new customers).	(No additional security measures)	ID.RM-1 ID.SC-1

24. 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	13.2.2
ID.AM-3	Organizational communication and data flows are mapped	14.3.1, 21.1.2
ID.AM-4	External information systems are catalogued	21.1.1
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	15.1.2
ID.GV-1	Organizational cybersecurity policy is established and communicated	16.1.1
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	16.1.1
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	23.1.4
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	16.1.3, 23.1.4

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.	13.5.2, 15.1.1, 15.1.3, 15.1.4, 15.2.4, 16.1.2, 19.1.1, 23.1.1
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.	21.1.5
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	20.1.2, 20.1.5, 20.1.6, 20.1.7
PR.AC-2	Physical access to assets is managed and protected	12.1.3, 13.3.1, 15.2.3, 18.4.2
PR.AC-3	Remote access is managed	20.1.3
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	14.1.1, 14.1.2, 14.1.3, 14.2.1, 18.4.3, 20.1.1, 20.1.2, 20.1.4, 20.1.6, 20.1.7
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	15.2.3
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	20.1.7
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)	12.1.6, 20.1.5, 20.1.6, 20.1.7, 21.1.3
PR.AT-1	All users are informed and trained	18.4.1, 23.1.3
PR.AT-2	Privileged users understand their roles and responsibilities	18.4.1
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	18.4.1

PR.DS-1	Data-at-rest is protected	12.2.1, 13.1.1, 13.2.1, 14.2.2
PR.DS-2	Data-in-transit is protected	12.1.1, 12.1.2, 12.1.5, 12.3.1
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5
PR.DS-4	Adequate capacity to ensure availability is maintained	13.5.1, 17.2.4
PR.DS-5	Protections against data leaks are implemented	12.1.4, 15.2.1, 15.2.2, 23.1.2
PR.IP-2	A System Development Life Cycle to manage systems is implemented	19.1.1
PR.IP-3	Configuration change control processes are in place	17.3.1, 17.3.2, 17.3.3, 17.3.4, 17.3.5
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	15.2.3
PR.IP-6	Data is destroyed according to policy	13.4.1, 13.4.3, 13.4.4, 13.4.5
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	17.4.1
PR.IP-12	A vulnerability management plan is developed and implemented	17.1.1
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	17.2.2, 22.1.1, 22.1.4
PR.PT-4	Communications and control networks are protected	21.1.4, 23.1.2
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	22.1.1

DE.CM-1	The network is monitored to detect potential cybersecurity events	17.2.1
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	22.1.3
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	17.2.3
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	17.2.1
DE.DP-2	Detection activities comply with all applicable requirements	22.1.2
DE.DP-3	Detection processes are tested	21.1.5
DE.DP-4	Event detection information is communicated	22.1.3, 22.2.1, 22.2.2
RS.CO-2	Incidents are reported consistent with established criteria	17.4.2, 17.4.3

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	Yes
B	SS-002 PKI & Key Management	Yes
C	SS-036 Secure Sanitisation and Destruction	Yes
D	SS-035 Secure Backup and Recovery	Yes
E	SS-033 Security Patching	Yes
F	SS-012 Protective Monitoring	Yes
G	SS-009 Hypervisor Security	Yes
H	SS-025 Virtualisation	Yes
I	Security Assurance Strategy	No
J	SS-001-1 Access & Authentication	Yes
K	DWP Data Protection Policy	No
L	SS-006 Security Boundaries	Yes
M	SS-001-2 Privileged User Access	Yes
N	SS-014 Security Incident Management Standard	Yes

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
Cloud Security Alliance Cloud Controls Matrix
CIS Critical Security Controls v8 controls set
UK General Data Protection Regulation (UK GDPR)
Data Protection Act 2018 (DPA)
NCSC 14 Cloud Security Principles
Operational Best Practices for NCSC Cloud Security Principles - AWS Config (amazon.com)
Azure UK Governments - 14 compliance controls.pdf (microsoft.com)

Appendix D - Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
DWP	Department of Work and Pensions.	UK Government
NCSC	National Cyber Security Centre	UK Government
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OWASP	Open Web Application Security Project	Open Source

Appendix E - Glossary

Table 5 – Glossary

Term	Definition
Bare Metal	A bare-metal environment is a specific kind of virtualisation environment built with bare-metal hypervisors that do not rely on a host OS in order to function.
Burst/Surge processing	Processing that exceeds regular processing capacity for short periods of time
Control Plane	The control plane provides management and orchestration across an organisation's cloud environment.
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, nonrepudiation, and accountability; including, but not limited to devices, products, systems, key variables, and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).
Data Plane	The data plane houses and transports application and data traffic.
DDA	Digital Design Authority (part of Digital Group)
IaaS	Infrastructure as a Service - The supply of basic infrastructure, such as networks, processing, and storage, on which users can base their applications, CSP is responsible.
PaaS	Platform as a Service - The level of responsibility shared with the CSP varies greatly in PaaS services. At one end of the spectrum, the distinction between IaaS and PaaS is blurred because the provider helps manage the operating system. Customers submit the source code for their application, and the service handles the rest.

SaaS	Software as a Service - The SaaS model enables CSC to provide the CSP the greatest amount of responsibility while taking full advantage of the increased security provided by the provider's large-scale operation.

Appendix F – Accessibility Artefacts

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

DWP Digital Accessibility Policy | DWP Intranet

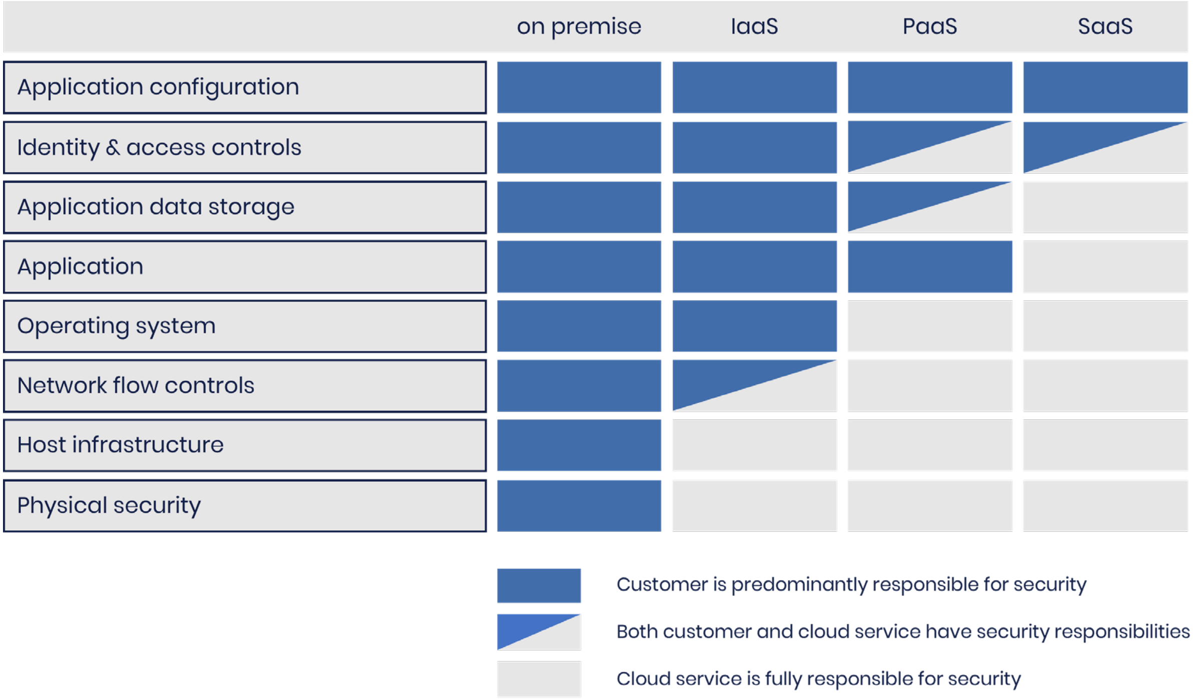
https://accessibility-manual.dwp.gov.uk/

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

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

Appendix G - Cloud Responsibility Service Model

The responsibility allocation options for the four basic deployment methodologies are broken down in the table below. Please use the following table only as guidance and confirm responsibilities with the CSP.



	on premise	IaaS	PaaS	SaaS
Application configuration	■	■	■	■
Identity & access controls	■	■	◪	◪
Application data storage	■	■	◪	□
Application	■	■	■	□
Operating system	■	■	□	□
Network flow controls	■	◪	□	□
Host infrastructure	■	□	□	□
Physical security	■	□	□	□

■	Customer is predominantly responsible for security
◪	Both customer and cloud service have security responsibilities
□	Cloud service is fully responsible for security