Security Standard – Database Management Systems (SS-005)

Chief Security Office

Department for Work & Pensions

Date: 22/01/2026

This Database Management Systems (DBMS) 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-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	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. Table of Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	18/09/2017
2.0		Full update in line with current best practices and standards; • Updated Intro, purpose, audience, scope • Replaced use of technical control requirements to minimum security measures • Added NIST sub-category references against each security measure • Added new table in Appendix A which lists security outcomes that measures support the achievement of • Updated references and included links to external publications etc. 11.1.9 Vulnerability assessments 11.4.4 Failed commands 11.6.7 Certs from Authority CA 11.7.4 Database credentials	14/06/2023
2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years 11.1.1 DBMS transaction and data storage 11.1.4 Required by the application 11.1.6 SQL queries, not business intelligence or reporting apps; application based stored procedures; data investigation 11.1.7 Application level 11.1.8 Application level 11.1.10 Sending data to personal accounts 11.1.11 DBMS asset inventory 11.1.12 Data and System Owners 11.1.13 Data classification 11.2.13 Maintain patch levels 11.1.14 Mandated in contracts	22/01/2026

		11.2 Platform specific hardening guides 11.2.3 Server side scripting 11.2.6 Active vendor support 11.2.7 Local admin connections 11.2.11 Network controls 11.2.12 OS admin accounts 11.2.18 DoS protection 11.2.19 Pen testing tools 11.3 Replication slave backups moved to 11.5 11.3.3 Wherever possible; must 11.3.4 where technically feasible; unless there is no other option available. 11.3.5 Non-encrypted interfaces 11.3.6 RBAC for system access 11.3.10 Confirmed as no longer default; Added ref to Access & Authentication standard 11.3.11 Or locked; Production / live databases 11.4.1 Log integration with SIEM 11.4.2 Authority time source 11.4.4 DML operations; Privileged user access 11.4.5 Database Activity Monitoring 11.5.3 RTO & RPO > database backups 11.6.1 Ref added to SS-007 11.6.6 Encryption key management 11.6.7 self-generated by native database capabilities. 11.7 Added ref to Priv User standard; requirements 11.7.4 Credential change if indication of compromise 11.7.5 Authentication credential requirements 11.7.6 MFA requirement; refs added to Access & Authentication and Privileged User Access standards 11.8 Secure decommissioning 11.9 Cloud based DBMSs Internal Refs – DWP Crypto algorithms; DWP Security Classification Policy; Secure	

		Sanitisation and Destruction standard; PKI & Key Mgmt standard External Refs - NCSC Cloud Security Principles; NIST CSF; NIST SP 800-53; ISO27001; OWASP Top 10; CISA KEV Catalog	

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	20/03/2017
2.0		Chief Security Officer	14/06/2023
2.1		Chief Security Officer	22/01/2026

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. 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 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 that utilise database technology.

7. Accessibility Requirements

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in **Error! Reference source not found.**F.

8. Introduction

This standard defines the minimum technical security measures that **must** be implemented to secure Authority systems and data utilising database management systems.

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 database management systems are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with databases, 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. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and 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 databases to process 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 database management systems (both on-premise and in the cloud) within the Authority, suppliers and contracted third party providers, for the purposes of delivering applications and services that handle Authority data.

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 General Security Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Validation of the DBMS transaction and data storage **must** be used to ensure the DBMS's stability and integrity of stored data.	PR.DS-01
11.1.2	New DBMS technologies **must** be approved by the Digital Design Authority prior to use or first deployment.	ID.AM-08
11.1.3	All server operating systems that the database is installed upon **must** be hardened in line with SS-008 Server Operating System Security Standard [Ref. A].	PR.DS-01 PR.DS-10 PR.IR-02
11.1.4	Access to a DBMS **must** apply the principle of least privilege and only have the permissions required by the application to achieve the current action. Common applications usually require read access but often write or update access as well. Rarely is "drop table" or other access required by a user interface.	PR.AA-05
11.1.5	DBMS links **must not** be defined between production and non-production DBMSs.	PR.IR-01
11.1.6	The DBMS transactions / queries from applications (e.g. SQL queries but not business intelligence or reporting apps) **must** be restricted from accessing the DBMS via any means except those that are provided by the available application based stored procedures. The use of ad-hoc queries by application users is strictly prohibited. Data investigation may need ad-hoc query access for issue or problem resolution.	PR.IR-01

11.1.7	At an application level, input checks **must** be applied to limit the number of DBMS transactions which contain: a) Missing and/or incomplete data; b) Out of range values; c) Unauthorised or inconsistent data; d) Invalid characters in data fields; e) Exceeding upper or lower date volume limits. See SS-003 Software Development Security Standard [Ref. D]	PR.DS-10
11.1.8	At an application level, dual input or other input checks such as boundary checking (content inspection/URL Filtering) or limiting fields to specific ranges of input data **must** be used.	PR.DS-10
11.1.9	Vulnerability assessments **must** be completed on a regular basis in line with the Technical Vulnerability Management Policy [Ref. J].	ID.RA-01 ID.RA-04
11.1.10	Data or code extracted from DBMSs **must not** be transmitted to personal accounts e.g. via email or external USB devices.	PR.DS-01
11.1.11	A comprehensive inventory of all Authority DBMS instances **must** be created and actively maintained. This inventory **must** include, at a minimum: • DBMS software type and version, • current patch level, • vendor support status, • physical or virtual location (including cloud region/service details), • operating system details, • business criticality, • data types stored, • key application dependencies, • designated Data Owner, and • System Owner.	ID.AM-01 ID.AM-02

11.1.12	A Data Owner for the information within each DBMS, and a System Owner for each DBMS instance, **must** be clearly designated and documented. Their security responsibilities, as defined by UK Government Data Ownership guidance, **must** be formally acknowledged.	GV.OC-04
11.1.13	All data stored in Authority DBMS **must** be classified according to its sensitivity and in adherence to the DWP Security Classification Policy [Ref. L] (e.g. OFFICIAL, and any handling caveats) and personal data status under the DPA 2018/UK GDPR. This classification **must** directly inform the security controls applied, including access controls, encryption, and logging requirements.	ID.AM-07 PR.DS-01
11.1.14	Where third parties access, manage, or support Authority DBMSs, their adherence to this standard **must** be contractually mandated and regularly assured. Risks associated with third party software components within the DBMS or its supporting ecosystem **must** be managed through vulnerability management (see 11.1.9) and secure software development practices (see SS-003 Secure Software Development Standard [Ref. D]).	GV.SC-02

11.2 Secure Hardening Configuration

While this standard provides vendor agnostic minimum measures, platform-specific security hardening patterns or guides **must** be developed, documented, and maintained for each major DBMS technology deployed (e.g., Oracle, Microsoft SQL Server, PostgreSQL, specific NoSQL variants, cloud-native DBaaS etc.). These guides **must** detail the specific configurations required to meet the principles of this standard on that platform, referencing CIS Benchmarks, vendor guidance, and NCSC recommendations. These guides **must** be used to enforce hardening baselines.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Naming conventions **must** clearly distinguish between production and non-production resources.	PR.IR-01
11.2.2	All databases **must** be hosted on servers which do not perform any other functionality such as “web or application tier” or “Domain Services” functionality. This requirement does not apply to native reporting services.	PR.IR-01
11.2.3	Pushing server-side script to database servers through database connectivity **must** be disabled. However, scripting on database servers is permitted to perform standard tasks.	PR.IR-01
11.2.4	The default passwords for accounts and services that are mandatory, for example System Administrator and Listener, **must** be changed prior to being deployed.	PR.AA-01
11.2.5	Test databases **must not** be installed upon production systems.	PR.IR-01
11.2.6	The versions of DBMS used **must** still be within active vendor support.	PR.PS-02
11.2.7	All administrator, user or application traffic (including local admin connections) to and from the DBMS **must** be encrypted in line with SS-007 Use of Cryptography security standard [Ref. C].	PR.DS-02
11.2.8	The database **must** not use unencrypted protocols or non-secure services (for example, HTTP, FTP etc.).	PR.DS-02

11.2.9	Unnecessary services or ports **must** be disabled or removed and where possible.	PR.IR-01
11.2.10	Databases **must** be configured to only listen for network connections on authorised interfaces.	PR.IR-01
11.2.11	Network or protocol level controls **must** be implemented so that only a defined list of endpoints can communicate with DB servers.	PR.IR-01
11.2.12	The DBMS **must** avoid the need to run services with privileged accounts (apart from OS admin accounts) on the underlying host Operating System.	PR.IR-01
11.2.13	All installations of a DBMS **must** be up to date with all appropriate security patches prior to deployment into service in line with SS-033 Security Patching Standard [Ref. B]. Once deployed, DBMS patch levels **must** be maintained in line with the same standard.	ID.AM-08 PR.PS-02
11.2.14	Only licensed software which has been verified as being authentic with the supplier can be used for a DBMS.	ID.RA-09 PR.PS-05
11.2.15	All DBMS software authenticity checks **must** be completed via a cryptographic verification or some other form of secure validation.	ID.RA-09 PR.PS-05
11.2.16	Default accounts, examples, code, files, objects etc. that are no longer required after installation **must** be deleted from the DBMS and also the host operating system.	ID.AM-08

11.2.17	The DBMS configuration **must** not permit default accounts (e.g. PUBLIC) to remain active. These **must** be either: a) Renamed, deleted or disabled (as appropriate); or b) The DBMS / object privileges **must** not be granted to default accounts which cannot be removed (or otherwise disabled) unless there is an explicit vendor requirement to do so; or c) If the default account cannot be renamed, deleted or disabled (such as root) access **must** be restricted to known administrative groups. Access to such accounts / functions (which cannot be renamed, deleted or disabled) **must** prevent direct access and require the user to logon with their individual account and then escalate / change their privilege in a controlled and logged fashion.	PR.AA-01 PR.AA-05
11.2.18	Where available, measures to protect against Denial of Service (DoS) attacks **must** be utilised.	PR.IR-01 PR.IR-03
11.2.19	Access to penetration testing tools **must** be strictly controlled in line with role based access and **must** be disabled when not in use.	PR.IR-01

11.3 **Database Application Access**

For further guidance on secure development please refer to the SS-003 Software Development Security Standard [Ref. D]. Also please refer to the SS-001 pt.1 Access & Authentication Security Standard [Ref. E] for further advice and guidance for this area.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Users **must** be authenticated before being granted access to the DBMS application permissions or its resources.	PR.AA-03
11.3.2	DBMSs **must** authenticate the user (or application requesting access), or if that is not possible, then it **must** record and log the user which requested that function.	PR.AA-03

11.3.3	Wherever possible, central access control systems **must** be used to manage access to the DBMS.	PR.AA-01 PR.AA-05
11.3.4	User privileges **must only** be granted on the basis of inclusion into roles where technically feasible. Privileges **must not** be granted directly to application / user accounts on the DBMS unless there is no other option available. Please refer to SS-001 pt.2 Privileged User Access Security Standard [Ref. F] for more information.	PR.AA-05
11.3.5	Databases **must** ensure any non-encrypted interfaces are disabled.	PR.IR-01
11.3.6	Role-based access control **must** be enabled and configured appropriately in a fully defined Role Based Access Control (RBAC) model where the accessing party is expected to be a system.	PR.AA-02 PR.AA-05
11.3.7	Each role for each database **must** only grant the necessary privileges as per the principle of least privilege.	PR.AA-05
11.3.8	Each database deployment **must** ensure that access to data/files reflects the defined RBAC model and assigned permissions.	PR.AA-02 PR.AA-05
11.3.9	Databases **must** not be configured with blank passwords.	PR.AA-01 PR.AA-02
11.3.10	All default passwords **must** be changed, encrypted and confirmed as no longer default. All passwords **must** be set in line with SS-001 pt.1 Access & Authentication Security Standard [Ref. E].	PR.AA-01 PR.AA-02
11.3.11	Any anonymous, default accounts and sample data **must** be removed or locked from production / live databases.	PR.AA-01 PR.AA-02

11.4 Database Application Logging

For detailed guidance on requirements for logging please refer to SS-012 Protective Monitoring Security Standard [Ref. H]

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Audit logs from all Authority DBMSs **must** be integrated with an Authority approved centralised Security Information and Event Management (SIEM) system. The SIEM **must** be configured with correlation rules and alerting mechanisms relevant to DBMS threats to detect suspicious activities in near real-time, in line with SS-012 Protective Monitoring Security Standard [Ref. H].	DE.AE-02 DE.AE-03
11.4.2	The clocks of all Applications **must** be synchronised with an Authority approved time source. For cloud based systems, the cloud providers' time services are sufficient for time reference synchronisation, as the Authority does not have reliable means to share time source data with external parties.	DE.CM-01 DE.AE-03
11.4.3	Logs may be appended to the Operating System logs or be self contained within the application.	PR.PS-04
11.4.4	At a minimum, the following Application Administration / Operator items **must** be recorded and logged: - start up; - shutdown; - The creation, alteration, or deletion (drop) of: databases, any database storage structure, and database tables, indexes, accounts and objects, and specific Data Manipulation Language (DML) operations (e.g., SELECT, INSERT, UPDATE, DELETE) on tables containing sensitive or personal data (as defined by data classification); - The enabling and disabling of audit functionality; - The granting and revoking of DBMS system level privileges; - Any action that returns an error message because the object referenced does not exist; - Any action that renames a DBMS object;	PR.PS-04 DE.CM-09 DE.AE-03

	- Any action that grants or revokes object privileges from a DBMS role or DBMS account; - All modifications to the DBMS system configuration; - All DBMS connection failures are audited. - Failed Logon attempts, password locks. - Failed commands - All privileged user or administrative operations access (i.e. not data changes)	
11.4.5	For Authority DBMSs identified as highly critical or processing highly sensitive data, the evaluation and deployment of Database Activity Monitoring (DAM) solutions should be considered to provide granular, real-time alerting on suspicious queries and policy violations.	DE.CM-09

11.5 Backup and Disaster Recovery

Please refer to SS-035 Secure Backup and Restore Security Standard [Ref. G] for further advice and guidance for this area.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Database systems **must** take regular backups.	PR.DS-11
11.5.2	Verification that backups can be restored from **must** be in place for all Authority databases.	RC.RP-03
11.5.3	Where required by Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), database replication mechanisms **must** be used to support timely disaster recovery and high availability, in line with SS-035 Secure Backup & Recovery Security Standard [Ref. G].	RC.RP-02 RC.RP-05

11.6 Data Encryption

For further guidance on encryption please refer to the SS-007 Use of Cryptography Security Standard [Ref. C].

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Encryption **must** be applied to all data transmitted between systems in line with SS-007 Use of Cryptography security standard [Ref. C].	PR.DS-02
11.6.2	All encryption material that is required for secure communications **must** be only accessible via the requesting service as read only access.	PR.DS-02
11.6.3	The database files and data **must** be encrypted.	PR.DS-01
11.6.4	All encrypted channels and stored data **must** not use a default or example certificate.	PR.DS-01
11.6.5	All encryption keys **must** be generated for a specific use case.	PR.DS-01
11.6.6	All encryption keys **must** be fully protected throughout their lifecycle (generation, distribution, storage, rotation, revocation/destruction) using approved mechanisms such as Hardware Security Modules (HSMs) or Authority approved key management services, where appropriate for the data sensitivity and risk. Access to key management functions **must** be restricted based on least privilege. Please refer to SS-002 PKI & Key Management standard [Ref. N] for more information.	PR.DS-01
11.6.7	All encryption certificates **must** be provided by the Authority's Enterprise Certificate Authority (CA), unless self-generated by native database capabilities.	PR.DS-01

11.7 Authentication & Authorisation

Please refer to SS-001 pt.1 Access & Authentication Security Standard [Ref. E] and SS-001 pt.2 Privileged User Access Security Standard [Ref. F] for further requirements for this area.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	All databases **must not** allow a bypass of authentication via the localhost exception.	PR.AA-03
11.7.2	Authentication **must** be enabled, including instances that are deployed via a shared cluster.	PR.AA-03
11.7.3	Any authentication mechanisms used **must** be Authority approved.	PR.AA-03
11.7.4	Database credentials **must** provide access only to functionality and operations required to discharge the function for which those credentials are issued. These credentials **must** be changed on indication or suspicion of compromise.	PR.AA-01 PR.AA-02 PR.AA-05
11.7.5	Authentication information which grants authorised access to asset(s) **must**: a) not be stored in plain text or in any reversible format; b) be salted with at least 128 bits of pseudorandom data; c) be hashed using a method described in the DWP Approved Cryptographic Algorithms Document [Ref. K].	PR.AA-04
11.7.6	Multi-Factor Authentication (MFA) **must** be utilised for all database access, including privileged or administrative access, regardless of the connection method although not necessarily at every stage of the connection process, in line with SS-001 pt.1 Access & Authentication [Ref. E] and SS-001 pt.2 Privileged User Access Security Standards [Ref. F]	PR.AA-03 PR.AA-05

11.8 Secure Decommissioning

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Secure decommissioning procedures **must** be followed for all retired Authority DBMSs and their associated storage media.	ID.AM-08
11.8.2	All Authority data, especially sensitive or personal data, **must** be cryptographically erased or otherwise verifiably destroyed from the DBMS and media before disposal or repurposing, in line with NCSC guidance and SS-036 Secure Sanitisation and Destruction Security Standard [Ref. M]. For databases in cloud environments, please follow the requirements defined in SS-023 Cloud Computing Security Standard [Ref. O], section 13.4 Sanitisation of Data and Disposal of Equipment.	PR.DS-01

11.9 Cloud-based DBMSs

Please also refer to SS-023 Cloud Computing Security Standard [Ref. O] for further information on cloud specific security requirements.

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	For Authority DBMSs hosted in cloud environments (IaaS, PaaS, or DBaaS), adherence to the NCSC Cloud Security Principles [see External References] **must** be demonstrated.	GV.OC-03
11.9.2	The shared responsibility model for security **must** be clearly understood, documented, and the Authority 's responsibilities **must** be fully addressed for each cloud service used.	GV.SC-02 GV.SC-05
11.9.3	Secure configuration of cloud service provider management consoles and APIs used to administer DBMS services **must** be enforced, including strong authentication (MFA) and least privilege in line with SS-001-1 Access & Authentication [Ref. E] and SS-001-2 Privileged User Access [Ref. F] security standards.	PR.AA-03 PR.AA-05

11.9.4	Network security configurations for cloud DBMSs (e.g., security groups, private endpoints, firewall rules) **must** be implemented to restrict access based on least privilege and protect from public exposure unless explicitly required and risk assessed.	PR.AA-05 PR.IR-01
11.9.5	Specific hardening guidance in section 11.2, as well as detailed platform-specific guides **must** be applied to cloud-native database services, considering vendor best practices.	PR.IR-01
11.9.6	Reliance on external cloud service providers increases the attack surface and likelihood of exploitation through human error, therefore configurations **must** be regularly audited.	PR.PS-01

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 which can also be cross referenced against the Authority's approved control set, which itself is based on the CIS Critical Security Controls [see External References].

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related Security measure
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	11.9.1
GV.OC-04	Critical objectives, capabilities, and services that stakeholders depend on or expect from the organisation are understood and communicated	11.1.12
GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	11.1.14, 11.9.2
GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritised, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	11.9.2
ID.AM-01	Inventories of hardware managed by the organisation are maintained	11.1.11
ID.AM-02	Inventories of software, services, and systems managed by the organisation are maintained	11.1.11
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	11.1.13
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.1.2, 11.2.13, 11.2.16, 11.8.1
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	11.1.9

ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	11.1.9
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	11.2.14, 11.2.15
PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	11.2.4, 11.2.17, 11.3.3, 11.3.9, 11.3.10, 11.3.11, 11.7.4
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.3.6, 11.3.8, 11.3.9, 11.3.10, 11.3.11, 11.7.4
PR.AA-03	Users, services, and hardware are authenticated	11.3.1, 11.3.2, 11.7.1, 11.7.2, 11.7.3, 11.7.6, 11.9.3
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.7.5
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, 11.2.17, 11.3.3, 11.3.4, 11.3.6, 11.3.7, 11.3.8, 11.7.4, 11.7.6, 11.9.3, 11.9.4
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.1.1, 11.1.3, 11.1.10, 11.1.13, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.6.7,11.8.2
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.6.1, 11.6.2
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.1.3, 11.1.7, 11.1.8
PR.DS-11	Backups of data are created, protected, maintained, and tested	11.5.1
PR.PS-01	Configuration management practices are established and applied	11.9.6
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.2.6, 11.2.7, 11.2.8, 11.2.13
PR.PS-04	Log records are generated and made available for continuous monitoring	11.4.3, 11.4.4
PR.PS-05	Installation and execution of unauthorised software are prevented	11.2.14, 11.2.15

PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.1.5, 11.1.6, 11.2.1, 11.2.2, 11.2.3, 11.2.5, 11.2.18, 11.2.9, 11.2.10, 11.2.11, 11.2.12, 11.2.18, 11.2.19, 11.3.5, 11.9.4, 11.9.5
PR.IR-02	The organisation's technology assets are protected from environmental threats	11.1.3
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	11.2.18
DE.AE-02	Potentially adverse events are analysed to better understand associated activities	11.4.1
DE.AE-03	Information is correlated from multiple sources	11.4.1, 11.4.2, 11.4.4
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.4.2
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.4.4, 11.4.5
RC.RP-02	Recovery actions are selected, scoped, prioritised, and performed	11.5.3
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	11.5.2
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	11.5.3

Appendix B. Internal references

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

Table 3 – Internal References

Ref	Document	Publicly Available*
A	SS-008 – Server Operating System Security Standard	Yes
B	SS-033 – Security Patching Security Standard	Yes
C	SS-007 – Use of Cryptography Security Standard	Yes
D	SS-003 – Software Development Security Standard	Yes
E	SS-001 (part 1) – Access and Authentication Security Standard	Yes
F	SS-001 (part 2) – Privileged User Access Security Standard	Yes
G	SS-035 – Secure Backup & Recovery Security Standard	Yes
H	SS-012 - Protective Monitoring Security Standard	Yes
I	Security Assurance Strategy	No
J	Technical Vulnerability Management Policy	Yes
K	DWP Approved Cryptographic Algorithms	No
L	DWP Security Classification Policy	Yes
M	SS-036 Secure Sanitisation and Destruction Security Standard	Yes
N	SS-002 PKI & Key Management Security Standard	Yes
O	SS-023 Cloud Computing Security Standard	Yes

Requests to access non-publicly available documents **should be made 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
NCSC Cloud Security Principles
NIST Cyber Security Framework
NIST SP 800-53 Security and Privacy Controls for Information Systems and Organisations
ISO 27001 Information Security Management Mystems
OWASP Top 10
CISA Known Exploited Vulnerabilities Catalog

Appendix D. Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
CMDB	Configuration Management Database	Industry term
DBMS	Database Management System	Industry Term
DDA	Digital Design Authority	DWP term
DWP	Department for Work and Pensions.	UK Government
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OS	Operating System	Industry term

Appendix E. Glossary

Table 6 – Glossary

Term	Definition
OFFICIAL	Information classification mark, identified in the Government Security Classification Policy.

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