Security Standard – Database Management Systems (SS-005)

Chief Security Office

Department for Work & Pensions

Date: 14/06/2023

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	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. 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

3. Approval history

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

This document will be reviewed for continued completeness, relevancy, and accuracy within 1 year of being granted "final" status, and at year 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 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 Appendix 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 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 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 and supplier base (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	Data validation **must** be used to ensure the DBMS's stability and integrity of stored data.	PR.DS-6
11.1.2	New DBMS technologies **must** be approved by the Design Authority prior to use or first deployment.	ID.GV-4
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-1 PR.DS-5
11.1.4	Access to a DBMS **must** apply the principle of least privilege and only have the permissions required 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.AC-4
11.1.5	DBMS links **must** not be defined between production and non-production DBMSs.	PR.DS-7
11.1.6	The DBMS transactions / queries from applications **must** be restricted from accessing the DBMS via any means except those that are provided by the available stored procedures. The use of ad-hoc queries by application users is strictly prohibited.	PR.AC-3
11.1.7	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;	PR.DS-6

	e) Exceeding upper or lower date volume limits. See SS-003 Software Development Security Standard [Ref. D]	
11.1.8	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-6
11.1.9	Vulnerability assessments **must** be completed on a regular basis in line with the Technical Vulnerability Management Policy [Ref. J].	PR.IP-12

11.2 Secure Hardening Configuration

Please refer to the SS-033 Security Patching Security Standard for more detailed guidance. [Ref. B].

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Naming conventions **must** clearly distinguish between production and non-production resources.	PR.DS-7
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.	PR.PT-3
11.2.3	All databases **must** ensure that server-side scripting is disabled if not needed.	PR.PT-3
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.AC-4
11.2.5	Test databases **must** not be installed upon production systems.	PR.DS-7
11.2.6	The versions of DBMS used **must** still be supported by the vendor.	PR.IP-5
11.2.7	All administrator, user or application traffic to and from the DBMS **must** encrypted in line with SS-007 Use of Cryptography security standard [Ref. C].	PR.DS-2

11.2.8	The database **must** not use unencrypted protocols or non-secure services (for example, HTTP, FTP etc.).	PR.DS-2
11.2.9	Unnecessary services or ports **must** be disabled or removed and where possible.	PR.PT-3
11.2.10	Databases **must** be configured to only listen for network connections on authorised interfaces.	PR.PT-3
11.2.11	The database servers **must** restrict network access using IP filtering.	PR.PT-3
11.2.12	The DBMS **must** avoid the need to run services with privileged accounts on the underlying host Operating System.	PR.PT-3
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].	PR.MA-1
11.2.14	Only licensed software which has been verified as being authentic with the supplier can be used for a DBMS.	PR.IP-5
11.2.15	All DMBS software authenticity checks **must** be completed via a cryptographic verification or some other form of secure validation.	PR.DS-6
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.	PR.PT-3
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	PR.AC-4 PR.PT-3

	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.	

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.AC-7
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.AC-7
11.3.3	Central access control systems should be used to manage access to the DBMS.	PR.AC-2 PR.AC-3
11.3.4	User privileges **must** be granted on the basis of inclusion into roles. Privileges **must** not be granted directly to application / user accounts on the DBMS. Please refer to SS-001 pt.2 Privileged User Access Security Standard [Ref. F] for more information.	PR.AC-4
11.3.5	All databases **must** ensure that the HTTP interface is disabled.	PR.PT-3

11.3.6	Role-based access control **must** be enabled and configured appropriately in a fully defined Role Based Access Control (RBAC) model.	PR.AC-4
11.3.7	Each role for each database **must** only grant the necessary privileges as per the principle of least privilege.	PR.AC-4
11.3.8	Each database deployment **must** ensure that access to data/files reflects the defined RBAC model and assigned permissions.	PR.AC-4
11.3.9	Replication slave backups **must** be made for all Authority database systems, and in line with SS-035 Secure Backup & Recovery Security Standard [Ref. G].	PR.IP-4
11.3.10	Databases **must** not be configured with blank passwords.	PR.AC-6
11.3.11	All default passwords **must** be changed, encrypted and verified.	PR.AC-6
11.3.12	Any anonymous, default accounts and sample data **must** be removed from the database.	PR.AC-1

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	The DBMS **must** adhere to the requirements contained within SS-012 Protective Monitoring Security Standard [Ref. H]	PR.PT-1 DE.AE-3 DE.CM-7
11.4.2	The clocks of all Applications **must** be synchronised with the Authority Reference (Master) Clock. 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 Authority Master Clock data with external parties.	DE.CM-1 DE.DP-2 DE.DP-4

11.4.3	Logs may be appended to the Operating System logs or be self-contained within the application.	DE.AE-3 DE.CM-7
11.4.4	At a minimum, the following Application Administration / Operator items **must** be recorded and logged: - All system alarms raised; - start up; - shutdown; - The creation, alteration, or deletion (drop) of: databases, any database storage structure, and database tables, indexes, accounts and objects; - 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; - Any action that grants or revokes object privileges from a DBMS role or DBMS account; - All modifications to the data dictionary or DBMS system configuration; - All DBMS connection failures are audited. Where possible, the DBA will ensure that both successful and unsuccessful connection attempts are audited; - Failed Logon attempts, password locks. - Failed commands -	DE.AE-3 DE.DP-2

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.IP-4
11.5.2	Verification of backups **must** be in place for all Authority databases.	PR.IP-4
11.5.3	Replication slave backups **must** be made for all Authority database systems.	PR.IP-4

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 as per Authority standards for all data transmitted between systems via TLS or SSL.	PR.DS-2
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-2
11.6.3	The database files and data **must** be encrypted.	PR.DS-1
11.6.4	All encrypted channels and stored data **must** not use a default or example certificate.	PR.DS-1
11.6.5	All encryption keys **must** be generated for a specific use case.	PR.DS-1
11.6.6	All encryption keys **must** be fully protected.	PR.DS-1
11.6.7	All encryption certificates **must** be provided by the Authority Enterprise Certificate Authority (CA).	PR.DS-1

11.7 Authentication & Authorisation

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
11.7.1	All databases **must** not allow a bypass of authentication via the localhost exception.	PR.AC-7
11.7.2	Authentication **must** be enabled, including instances that are deployed via a shared cluster.	PR.AC-7
11.7.3	Any authentication mechanisms used **must** be Authority approved.	PR.AC-7
11.7.4	Database credentials **must** provide access only to functionality and operations required to discharge the function for which those credentials are issued	PR.AC-4

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 an Authority 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
ID.GV-4	Governance and risk management processes address cybersecurity risks	11.1.2
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.3.12
PR.AC-2	Physical access to assets is managed and protected	11.3.3
PR.AC-3	Remote access is managed	11.1.6, 11.3.3
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.4, 11.2.4, 11.2.17, 11.3.4, 11.3.6, 11.3.7, 11.3.8, 11.7.4
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.3.10, 11.3.11
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.3.1, 11.3.2, 11.7.1, 11.7.2, 11.7.3
PR.DS-1	Data-at-rest is protected	11.1.5, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.6.7
PR.DS-2	Data-in-transit is protected	11.2.7, 11.2.8, 11.6.1, 11.6.2
PR.DS-5	Protections against data leaks are implemented	11.1.3
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.1.1, 11.1.7, 11.1.8, 11.2.15
PR.DS-7	The development and testing environment(s) are separate from the production environment	11.1.5, 11.2.1, 11.2.5

PR.IP-4	Backups of information are conducted, maintained, and tested	11.3.9, 11.5.1, 11.5.2, 11.5.3
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	11.2.6, 11.2.14
PR.IP-12	A vulnerability management plan is developed and implemented	11.1.9
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.2.13
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.4.1
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.2.2, 11.2.3, 11.2.9, 11.2.10, 11.2.11, 11.2.12, 11.2.16, 11.2.17, 11.3.5
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.4.1, 11.4.3, 11.4.4
DE.CM-1	The network is monitored to detect potential cybersecurity events	11.4.2
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	11.4.1, 11.4.3
DE.DP-2	Detection activities comply with all applicable requirements	11.4.2, 11.4.4
DE.DP-4	Event detection information is communicated	11.4.2

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

Requests to access non-publicly available documents **should be made to an Authority Contracts/Supplier Manager.*

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 v8 Critical Security Controls

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 of 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:

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