IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Database Management System Security Standard (SS-005)

Chief Security Office

Date: 20/03/2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

1. Introduction

1.1. This document defines the Department of Work and Pensions (DWP) security requirements for the configuration of Database Management Systems (DBMS's).

1.2. This document is an agnostic DBMS security standard and will provide overarching controls for any DBMS new to the departmental estate in lieu of a security standard or pattern e.g the Oracle Database Security Pattern.

1.3. General controls detailed in this document are driven from the need to align to DWP guidance on security, namely, the Security Controls Catalogue* and also overarching DWP Security Policy. System hardening configuration guidelines laid out in this document provides advice and guidance on the secure DBMS deployments in lieu of a DMBS specific security standard or security pattern.

2. Purpose

2.1. The standard lists technical security requirements on how to secure DMBS's securely for Department use with the aim of protecting departmental and citizen data. This Standard covers systems or data at the OFFICIAL tier of the Government Security Classification Policy (including the handling caveat (OFFICIAL-SENSITIVE).

2.2. This standard is intended to have three uses:

- To be used by projects when building DBMS's in lieu of a specific product security standard;
- To be used to assist to providing advice and guidance on secure configuration;
- To provide a means to conduct compliance based technical security audits.

3. Exceptions

3.1. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process*.

3.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.3. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and reporting to senior management.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

4. Audience

4.1. This standard is intended for suppliers, database administrators, developers, security groups, Security Architects and also IT staff such as Security Compliance Teams, involved in securing environments for DWP systems and applications.

5. Scope

5.1. All new DBMS builds MUST meet all the requirements in this standard, attest to meet the standard or be otherwise authorised for exception via a DWP security architectural risk review (see exceptions process).

5.2. The standard applies to the following;

- DBMS's managed by the DWP or Third Party Supplier or other support function
- Any DBMS used to support or host DWP services and/or data.

5.3. In the event of uncertainty on the controls laid out in this standard please contact the Security Advice Centre for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7. Database Management Systems Security Requirements

7.1. The following sections provide the security requirements that MUST be applied to DBMS's prior to deployment.

7.2. The following sections provide the security requirements that MUST be applied to DBMS's prior to the storing or processing production data of any type or classification level

7.3. Each configuration setting is listed with three sections, the first being a control reference number, secondly the security control requirement that is required to be configured to the operating system's default configuration and the third section provides information on change itself.

8. General Security Requirements

Reference	Security Control Requirement
8.1.1.	Data validation MUST be used to ensure the DBMS's stability and integrity of stored data. *
8.1.2.	New DBMS technologies MUST be approved by the Design Authority prior to use or first deployment.
8.1.3.	All server operating systems that the database is installed upon must be hardened to a DWP security pattern, where this is not available a CIS benchmark must be used. ***
8.1.4.	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.
8.1.5.	DBMS links MUST not be defined between production and non-production DBMSs.
8.1.6.	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. *
8.1.7.	Input checks MUST be applied to limit the 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 secure development standard *
8.1.8.	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. *

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

9. Secure Hardening Configuration Requirements

*Please refer to the DWP Patching Policy for more detailed guidance.

Reference	Security Control Requirement
9.1.1.	Naming conventions MUST clearly distinguish between production and non-production resources.
9.1.2.	All databases MUST be hosted on servers which do not perform any other functionality such as “web or application tier” or “Domain Services” functionality.
9.1.3.	All databases must ensure that server-side scripting is disabled if not needed.
9.1.4.	The default passwords for accounts and services that are mandatory, for example SA and Listener, MUST be changed prior to being deployed.
9.1.5.	Test databases must not be installed upon production systems.
9.1.6.	DBMS Versions MUST still supported by the vendor.
9.1.7.	All administrator, user or application traffic to and from the DBMS MUST encrypted.
9.1.8.	The database must not use unencrypted protocols or non-secure services (example, HTTP, FTP etc. must not be used).
9.1.9.	Unnecessary services or ports MUST be disabled or removed and where possible.
9.1.10.	Databases must be configured to only listens for network connections on authorised interfaces.
9.1.11.	The database servers must restrict network access using IP filtering.
9.1.12.	The DBMS MUST avoid the need to run services with privileged accounts on the underlying host Operating System.
9.1.13.	All installations of a DBMS MUST be up to date with all appropriate security patches prior to deployment into service. **
9.1.14.	Only licensed software which has been verified as being authentic with the supplier can be used for a DBMS.
9.1.15.	All DMBS software authenticity checks MUST be completed via a cryptographic verification or secure receipt of tamper proof / tamper evident packaging.
9.1.16.	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.
9.1.17.	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. d) 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.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

10. Database Application Access Control Requirements

For the further guidance on secure development please refer to the SS-003 Secure Development Lifecycle Standard. Also please refer to the DWP SS-001 Secure Access & Authentication Standard for further advice and guidance for this area.

Reference	Security Control Requirement
10.1.1.	Users MUST be authenticated before being granted access to the DBMS application permissions or its resources.
10.1.2.	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.
10.1.3.	The DWP's Central Access Control Systems should be used to manage access to the DBMS.
10.1.4.	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.
10.1.5.	All databases must ensure that the HTTP interface is disabled.
10.1.6.	Role-based access control must be enabled and configured appropriately pre a fully defined Role Based Access Control (RBAC) model.
10.1.7.	Each role for each database must only grant the necessary privileges as per the principle of least privilege.
10.1.8.	Each database deployment must ensure that access to data/files reflects the defined RBAC model and assigned permissions.
10.1.9.	Replication slave backups must be made for all DWP database systems.
10.1.10.	Databases must not be configured with blank passwords.
10.1.11.	All default passwords must be changed, encrypted and verified.
10.1.12.	Any anonymous, default accounts and sample data must be removed from the database.

11. Database Application Logging Control Requirements*

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

Reference	Security Control Requirement
11.1.1.	The DBMS MUST adhere to the requirements contained within the DWP Logging and monitoring standard

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
11.1.2.	The clocks of all Applications MUST be MUST be synchronized with the underlying Operating System clock.
11.1.3.	Logs may be appended to the Operating System Logs or be self-contained within the application.
11.1.4.	At a minimum, the following Application Administration / Operator items MUST be recorded and logged: I. All system alarms raised; II. start up; III. shutdown; IV. The creation, alteration, or deletion (drop) of: databases, any database storage structure, and database tables, indexes, accounts and objects; V. The enabling and disabling of audit functionality; VI. The granting and revoking of DBMS system level privileges; VII. Any action that returns an error message because the object referenced does not exist; VIII. Any action that renames a DBMS object; IX. Any action that grants or revokes object privileges from a DBMS role or DBMS account; X. All modifications to the data dictionary or DBMS system configuration; and XI. All DBMS connection failures are audited. Where possible, the DBA will ensure that both successful and unsuccessful connection attempts are audited. XII. Failed Logon attempts, password locks,

12. Backup and Disaster Recovery

Please refer to the DWP Backup and Disaster Recovery Standard for further advice and guidance for this area.

Reference	Security Control Requirement
12.1.1.	Database systems must have regularly occurring backups installed.
12.1.2.	Verification of backups must be in place for all DWP databases
12.1.3.	Replication slave backups must be made for all DWP database systems.

13. Data Encryption

Please refer to the DWP SS-007 Security Standard - Use of Cryptography Standard and also the SP-006 Channel Encryption Pattern for further advice and guidance for this area.

Reference	Security Control Requirement
13.1.1.	Encryption must be applied per DWP standards for all data transmitted between systems via TLS or SSL*.*
13.1.2.	All encryption material that is required for secure communications must be only accessible via the requesting service as read only access.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control Requirement
13.1.3.	The database files and data must be encrypted.
13.1.4.	All encrypted channels and stored data must not use a default or example certificate.
13.1.5.	All encryption keys must be generated for a specific use case.
13.1.6.	All encryption keys must be fully protected.
13.1.7.	All encryption certificates must be verified from both the provider and the Certificate Authority (CA).

14. Authentication & Authorisation

Please refer to the DWP SS-001 Security Standard - Secure Access & Authentication Standard for further advice and guidance for this area.

Reference	Security Control Requirement
14.1.1.	All databases must not allow a bypass of authentication via the localhost exception.
14.1.2.	Authentication must be enabled and also be enabled for instances that deploy via a shared cluster.
14.1.3.	Any authentication mechanisms used must be DWP approved.

15. Compliance

15.1. Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

16. Accessibility

16.1. No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it deemed that projects implementing this standard are obliged to incorporate accessibility functions.

17. Security Standards Reference List

Document Name	Location	Version
Security Standards Master List		

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

18. Reference Documents

DWP Digital Blueprint

Policy & Standards reference page

CIS for MS Office Access 2013 Benchmark v1.0.1

CIS for MS SQL Server 2012 Benchmark v1.3.0

CIS for Mongo Database Benchmark v1.0.0

CIS for MySQL Benchmark v1.0.2

CIS Oracle Database 12.c Benchmark v2.0.0

19. Definition of Terms

Term	Definition
Database Management System (DBMS)	An application that interacts with the user, other applications, captures and analyse data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).

20. Glossary

The glossary can be found alongside the published standards and patterns.

21. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the control points in ISO/IEC 27002:2013 Section 9.1 – entitled “Controls”.

ISO/IEC 27002:2013 Control	*Database management systems security standard* Control Statement(s)
9.2.3.	11.1.4
9.4.1	17.1.3
12.1.2	11.1.2
12.1.4	11.1.5,12.1.5,12.11
12.3.1	15.1.1,15.1.2,15.1.3
12.4.1	14.1.4
12.5.1	12.1.6, 12.1.14
13.2.1	12.1.8;16.1.1,16.1.4,16.1.5,16.1.17