Technical Security Baseline – Database Management Systems

WHAT EVERY EMPLOYEE NEEDS TO KNOW ABOUT THIS TSB	
Intended Audience	This TSB applies to everyone using Database Management Systems (DBMS) to support a business process.
Scope and Expectations	This document outlines the minimum security requirements for securing Database Management Systems.
Key Points	This TSB addresses DBMS and the following topics: • Technology Specific Requirements ○ DBMS Configuration ○ Access Requirements ○ Roles and Permissions ○ Other • Post Configuration Review

	Requirement	Purpose	Implementation Notes	References
Technology Specific Requirements				
DBMS Configuration				
1.	Database connection scripts encrypt the password.	This reduces the risk of compromise from stolen credentials.	All installation software and scripts are removed from production systems following implementation.	Encryption Technical Security Baseline (TSB)
2.	Database service accounts are configured for unlimited login attempts when directed by database vendor or industry best practices.	Some database service accounts need to be configured with unlimited login attempts that are outside of normal policy requirements to avoid creating high availability data access issues.	Follow database vendor's or industry best practices for service account login attempt limitations.	Microsoft account lockout threshold guidance. OWASP brute force guidance
3.	All database components not required for a system, are disabled.	This reduces the attack surface of a system and therefore the risk of unauthorised access to data.		
Access Requirements				
4.	Access to all accounts and binaries follows the principle of least privilege.	This reduces the risk of unauthorised access to data.	Users do not have the ability to read trace files. Access to database restore capabilities is provided only after approval from the application owner. Developers are not granted unrestricted access to the production environment. Access to the PUBLIC role is limited to approved users only. Access to the data dictionary is restricted to administrators only.	

	Requirement	Purpose	Implementation Notes	References
5.	Alternate means of connectivity to the database (HTTP servers, XML databases, etc.) are disabled if not required.	This reduces the attack surface of a system and therefore the risk of unauthorised access to data.		
6.	Network access is restricted to database servers via firewall rules.	Failure to implement strict network access controls increases the opportunity for potential attacks.		
Roles and Permissions				
7.	The database instance owner is not part of any administrator-level group or configured as a local system account.	Failure to restrict the privileges of the database instance can increase the level of access an attacker would obtain on the host operating system in case of database compromise.		
8.	Default database account are disabled and replaced with approved accounts using Experian naming conventions.	Using default account names increases the risk of successful brute forcing attack leading to unauthorized access.	For Oracle only, SYS account can be enabled if it is an operational requirement for a specific system.	CIS Oracle Database Benchmark 3.10 Ensure No Users Are Assigned the 'DEFAULT' Profile
9.	Files created by the database instance owner account have secure permissions by default and are limited to approved systems administrators only.	DBMS applications often create numerous files and directories that may contain sensitive information. Failing to ensure that these data objects are created with secured permissions can allow unauthorized access to sensitive information.		
10.	Control which users can create objects within the schemas.	Without granular access controls, risk of unauthorized access increases.	The establishment of RBAC policies will provide standardized user roles that define access levels.	
Other				

	Requirement	Purpose	Implementation Notes	References
11.	The DBMS, data, operating system, log files, and backup files are segregated when configuring dedicated database servers.	Segregating these components reduces risk of unauthorized access to data, as an attacker would have easier access to the protected data if it were not segregated.	Logical or physical segregation of code, data, and logs helps to secure the overall DBMS. Credentials are not shared across the segments. It is understood that some databases are set up in a single tier environment, in which case this requirement does not apply.	NIST 800-53-controls; System and Communications Protection SC-2 Application Partitioning
12.	Database link protection is enabled.	This reduces the attack surface of a system and therefore the risk of unauthorised access to data.	Where database link required, written approval is obtained from the application owner.	CIS Oracle Database 5.9 Enable 'DATABASE LINK' Audit Option
13.	Views are implemented for data security.	Failure to use database views increases the risk that the data within those views will be accessed or modified by unauthorized users.		
14.	Sample data and users are removed prior to entering production	This reduces the attack surface of a system and therefore the risk of unauthorised access to data.		CIS Oracle Database 1.3 Ensure All Sample Data And Users Have Been Removed
15.	All backdoors are removed before moving databases to production.	This reduces the attack surface of a system and therefore the risk of unauthorised access to data.		
Post-Configuration Review				
16.	Ensure that front and back-end servers are only accessible from the proper location.	This reduces the attack surface of a system and therefore the risk of unauthorised access to data.		

Related Documents

- NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations
- Encryption TSB
- CIS Distribution Independent Linux Benchmark v2.0.0
- Microsoft Windows 10 Enterprise Release 21H1 Benchmark v1.11.0
- CIS Apple macOS 12.0 Monterey Benchmark v1.0.0

All deviations from this TSB are documented in line with the Global Information Security Policy.

Appendix A – Document management and version history

Version	Review Frequency	Approval Date	GSO Lead	Technical Lead	Revision
1	12 months	7/31/2017	Erica Drake	Sai Ragam, Brad Ritter	Regular document review/update.
2	12 months	9/13/2018	Erica Drake		Review/update
3	12 months	610/2019	Erica Drake	Sai Ragam	Deleted requirement 18 at request of owner
3	12 months	9/25/2019	Erica Drake	Patricia White, Saptarshi Banerjee, Jason Yau	Annual Review
4	12 months	10/15/2020	John Mickle	Patricia White, Saptarshi Banerjee, Jason Yau	Review/Update
5	12 Months	4/28/2022	Shaun Dyer	Patricia White, Saptarshi Banerjee, Jason Yau	Annual Review