

 California DEPARTMENT OF TECHNOLOGY		3132	
MIDRANGE DATABASE SERVER SECURITY STANDARD			
OWNER:	Security Management Branch	ISSUE DATE:	4/10/2009
DISTRIBUTION:	Office of Technology Services Employees	REVISED DATE:	12/31/2015

This document was last reviewed/updated in December, 2015.

SECTION 1 – INTRODUCTION

This Standard addresses the security requirements surrounding data access and administrator roles and responsibilities of the Office of Technology Services (OTech) midrange database administration. This Standard is applicable to OTech staff supporting midrange Relational Database Management Systems (RDBMSs) and OTech customers implementing midrange RDBMSs in managed solutions.

Security is a major concern for modern-age systems, network, and database administrators. While it is natural for an administrator to be concerned about hackers and external attacks while implementing security, it is essential to first implement security within an organization by creating a security plan. Primarily, a security plan must identify which individuals of an organization will have access to data, the type of access that will be granted, and which database activities will be performed and by whom.

To access data within a database, a user must pass through two stages of authentication. One is at the operating system level, the other at the database level.

SECTION 2 – STANDARD REQUIREMENTS

Part I – Database Security Requirements

The requirements listed below must be implemented to consolidate database security across managed services. They are necessary for OTech database system administrators to properly support, administer, and audit the database systems.

- A. RDBMS installations shall retain current security rights unless they conflict with a California Department of Technology (CDT) Security Policy and/or Standard. If any configuration is in conflict with a current CDT Security Policy or Standard, a remediation of non-compliance will need to be coordinated.
- B. RDBMSs which support report generating/rendering services (e.g. Crystal Reports, Structured Query Language [SQL] Server Report Services, etc.) that provide a hypertext transfer protocol (HTTP) based interface with outbound traffic must not be designated over port 80 from the database tier of the standard n-tier network architecture. Refer to [3117 - Network Architecture Standard](#) for details regarding acceptable network architectures in the hosting environment.
- C. Access to database server settings will be restricted to OTech database system administrators. If specific changes are needed, customers must submit a Service Request requesting the change.

- D. OTech database system administrators:
- Maintain operating system and security patch levels and health of the servers.
 - Maintain system hardening configuration documentation in accordance with security standards. Refer to [3126 - Server Security Standard](#) and [3302 - Security Update Management Standard](#).
 - Are responsible for server access accounts. Only OTech database system administrators are authorized to change access levels.
 - Are responsible for scheduling database job scripts.
 - Are responsible for service accounts and their respective access rights for the database management system.
- E. Customers shall have permissions as listed below to their databases:
- Database owner (DBO) access or equivalent is provided for database maintenance purposes.
 - Applications must have specific roles and/or user permissions as needed to perform application functions.
- F. Customers are not provided Server Administration (SA) Authority (except in exceptional cases, see “Section 3.1 – Security” of the applicable Database Server Guideline (found on the OTech Service Catalog website) and 3502 – Information Security Exception Request Procedure).

Part II – Customer System Administrator Directives

OTech database system administrators are responsible for the proper support, administration, and auditing of the database systems in the managed services. The requirements listed below must be implemented to consolidate database security and integrity of those systems. Additionally, OTech’s business model requires that environments be standardized in order to achieve cost efficiencies.

In exceptional cases, in which an OTech customer (internal or external) is granted Server Administration (SA) Authority, the following actions (or similar) are not permitted without the prior approval and coordination from the appropriate OTech service area.

- Changes to the operating system or RDBMS configuration parameters.
- Changes to OTech scheduled jobs.
- Creation of RDBMS agent jobs.
- Creation or modification of user accounts.
- Changes to the RDBMS service accounts and system administrator accounts (these accounts are owned by OTech staff).
- Installation of RDBMS server and components (e.g., SQL Reporting Services).

Please see the online detailed matrix located in the [OTech Service Catalog](#) for an outline of respective functional responsibilities.

SECTION 3 – APPLICABILITY AND EXCLUSIONS

- A. This Standard applies to systems hosted in the managed services environment. Direct any questions regarding the applicability of this Standard to the Security Management Branch for clarification.

- B. This Standard does **not** apply to customer-managed applications in Tenant Managed Services.
- C. Exceptions to this Standard must be documented and will be considered on a case-by-case basis. Requests for an exception to this Standard must be submitted via the process described in [3502 - Information Security Exception Request Procedure](#).

SECTION 4 – AUDITING AND REPORTING

- A. Auditing may be performed on a periodic or random basis by the Security Management Branch or its designees. In the event an audit determines this Standard is not being applied, notification will be sent to the appropriate person(s) for remediation, and system administrator access may be revoked.
- B. Any known violations of this Standard must be reported to the CDT Chief Information Security Officer and the reporting employee's immediate supervisor. Noncompliance with the requirements outlined above may result in remediation or the revocation of system administrator access.

SECTION 5 – AUTHORITY/REFERENCES

[3117 - Network Architecture Standard](#)
[3502 - Information Security Exception Request Procedure](#)
[OTech Service Catalog](#)

Please contact your OTech Customer Representative for the below documents:

3400 - Acceptable Use Policy
3126 - Server Security Standard
3302 - Security Update Management Standard