BRITISH COLUMBIA
Office of the Chief Information Officer

IMIT 6.16 Database Security Standard

Document Version: 2.0
Effective Date: April 2018
Last Reviewed: August 2024

1. Purpose

To identify the minimum technical security requirements to secure B.C. government databases from intrusion, fraud, and fraud-related activities.

This standard describes the minimum controls to secure government database systems that contain information with the information security classification up to, and including, Protected B. A security threat and risk assessment MUST be conducted to identify security controls required for a database system that contain information with the information security classification Protected C.

The IMIT 6.16 Database Security Specifications document provides detailed specifications for this standard. Both this standard and the specifications MUST be followed. This standard supplements the IMIT 6.27 Operations Security Standard and the IMIT 6.29 System Acquisition, Development, and Maintenance Security Standard.

2. Application

This IMIT 6.16 Database Security Standard applies to:

- Ministries, agencies, boards, and commissions (referred to as ministries in this standard) who are subject to the Core Policy and Procedures Manual.
- Service providers and other entities conducting business or managing the B.C. government's information on its behalf.
- All B.C. government database systems used in applications that support a B.C. government service.

3. Requirements

3.1 Database system planning and acquisition

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.1.1 Identify the information security requirements for new database systems or enhancements to existing database systems to protect the confidentiality, integrity, and availability of information contained in the databases.

3.1.2 Manage the security risks related to the information in the databases and the database management system based on the confidentiality, integrity, and availability requirements of the information.

3.1.3 Prohibit use of production data in non-production environments without prior approval and production-like security controls in place.

3.1.4 Include confidentiality clauses in contracts with service providers and contractors who will have access to the information contained in the databases.

3.1.5 Before providing access to production databases, require:

1. Employees, contractors, and service providers to complete information security and privacy training before accessing production databases.
2. Applications that will access production databases to have built-in security and privacy controls.

3.2 Design, development, and testing

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.2.1 Conduct a vulnerability assessment and security tests to identify and remediate security risks in the database system before implementation in the production environment.

3.2.2 Configure logging systems to capture, record, and alert on activities that may violate the confidentiality, integrity, or availability of production databases that contain sensitive (Protected B and Protected C) or higher risk data (for example, critical data).

3.2.3 Separate the responsibilities for the database system to limit privileged access abuse and fraud opportunities based on the sensitivity of the information stored in the database system.

3.2.4 Separate production databases environments from non-production environments.

3.2.5 Use an OCIO authentication service to manage and authenticate access to databases.

3.2.6 Develop, document, maintain, and implement security operating procedures and responsibilities for production databases.

3.2.7 Develop and document a disaster recovery plan for the database system that meets business objectives and helps to recover from a disruptive event that will have an unacceptable impact to the availability and integrity of the information contained in the database system.

3.2.8 Follow the organization’s change management processes to implement changes to database systems in the production environment.

3.3 Implementation, operations, and disposition

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

3.3.1 Maintain an up-to-date inventory of all databases.

3.3.2 Maintain and implement documented security operating procedures that are necessary for ongoing support for, and operations of, production databases.

3.3.3 Activate audit logs for databases.

3.3.4 Monitor and audit privileged database user activities on production databases.

3.3.5 Test and maintain the disaster recovery plan for the database system, and ensure skilled resources are in place.

3.3.6 Conduct regular database vulnerability assessments to identify, analyze, and manage security risks related to critical and high-risk database vulnerabilities.

3.3.7 Apply database patches following the schedule outlined in the OCIO Patch Guidelines at minimum and in applicable regulatory standards.

3.3.8 Document and protect all copies or transfers of bulk production data to non-production environments or to third parties.

3.3.9 Conduct a formal review of users, accounts, and their access permissions to databases containing production data at least annually.

4. Supporting documents

IMIT 6.16 Database Security Specifications

IMIT 6.27 Operations Security Standard

IMIT 6.29 System Acquisition, Development, and Maintenance Security Standard

OCIO Patch Guidelines

5. Definitions

Information Security Glossary

6. Authority

Core Policy and Procedures Manual (CPPM)

Information Security Policy

Managing Government Information Policy

7. Revision history

This standard is reviewed annually and updated as needed.

Version	Revision Date	Author	Description of Revisions
2.0	August 2024	S. Gopaldas Johnston	Transfer to new template. Content updates and transfer of detailed/technical content to specification document IMIT 6.16 Database Security Specification.
1.0	April 2018	B. Dari; D. B. Johnson	First release.

8. Contact

For questions regarding this standard, contact:

Cybersecurity and Digital Trust Branch, Office of the Chief Information Officer
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca