1. Purpose

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

This document provides detailed security specifications to support the IMIT 6.16 Database Security Standard. Both the standard requirements and these specifications MUST be followed.

2. Resources

Defensible Security Framework	Critical security controls (assessment and tools).
IMIT 5.10 Critical Systems Standard	Guidance on identifying and ensuring availability of critical government systems.
IMIT 6.10 Cryptographic Security Standard	Framework for the use of cryptography in government that helps organizations meet their goals to protect their information and technology assets.
IMIT 6.11 Security Threat Risk Assessment Standard	Requirements to assess (identify, analyze, and evaluate), define planned treatments, and report security threats and risks in information systems.
IMIT 6.14 Application and Web Security Standard	Minimum controls for secure software development and maintenance, and for the protection of B.C. government applications, including web and mobile applications.
IMIT 6.16 Database Security Standard	Corresponding standard for these specifications.
IMIT 6.18 Information Security Classification Standard	Four levels of security classification applied to government information based on expected harm that could result from unauthorized disclosure.
IMIT 6.23 Asset Management Security Standard	Minimum security controls for managing physical IT assets and information assets to protect B.C. government information and information systems.

IMIT 6.24 Access Control Security Standard	Blueprint to manage access, authorizations, and control requirements for computer networks, operating systems, applications, and information.
IMIT 6.27 Operations Security Standard	Security framework for secure IT operations management.
IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard	Requirements to incorporate security measures into the management of the lifecycle of an information system.
Information Security Glossary	List of information security terms and definitions.
NIST 800-32 Rev 1	Contingency planning guide for federal information systems.
OCIO Patch Guidelines	Current patching expectations for government assets and the Cybersecurity and Digital Trust Branch's expected patch mitigation plan for vulnerable systems based on risk rating.
OWASP Database Security Cheat Sheet	Guidance on securely configuring and using the SQL and NoSQL databases.
Payment Card Industry Data Security Standard (PCI DSS) Version 4.0	Security standards for organizations that accept, process, store or transmit credit card information.
Test Disaster Recovery Plans	List of disaster recovery testing types.

3. Specifications

3.1 Database system planning and acquisition

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

1. Define the information security requirements per the IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard by:
   a. Identifying and documenting[1] the highest[2] information security classification label (see IMIT 6.18 Information Security Classification Standard) for the information that will be stored in the new database system.
   b. Identifying the following to protect information from unauthorized access or tampering during transit and at rest, and documented[3] for a new database system or for enhancements to an existing database system:
      i. The minimum security controls required to comply with legislation and regulations, for example, FIPPA, PCI-DSS
      ii. Additional security controls required[4] to manage the risks to the confidentiality (based on the information security classification of the information), availability, integrity of the information and database system, and access requirements
      iii. Countermeasures to manage security risks related to the information that are associated with:
         - Data theft
         - Unauthorized access to sensitive data

[1] Record the information security classification in the system security plan for the database system. See the IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard for details.
[2] If more than one information security classification label applies to the datasets in the database system, apply the highest information security classification label to the database system. For example, if the information security classification Protected A label applies to dataset A, and the Public label applies to dataset B, apply the Protected A label to the database system.
[3] Per the IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard, the security controls and countermeasures for the database system MUST be documented in the system security plan.
[4] Identify the additional security requirements through a security threat and risk assessment (see the IMIT 6.11 Security Threat Risk Assessment Standard). If encryption is identified as one of the reasonable security controls to protect confidential or sensitive personal information in transit and at rest from unauthorized access or tampering, follow the requirements of IMIT 6.10 Cryptographic Standard for the encryption.

- Weak authentication and authorization
- Insufficient or weak audit logging
- Database system vulnerabilities
- Malware, including ransomware
- Denial-of-service attacks
- Database injection attacks; for example, SQL/NoSQL injection attacks
- Buffer overflow attacks
- Privilege escalation
- Privilege abuse
- Database backups exposure
- Poor sensitive data management
- Misconfiguration of databases
- Insufficient security expertise and education

2. Manage the security risks for a database system, including:
   a. Defining, documenting, and implementing policies and processes that are based on business requirements to authorize and revoke access to the database system and to the data in the database system.
   b. Establishing the database access management policies (according to the IMIT 6.24 Access Control Security Standard) for:
      i. Who is authorized to have access, when they have access, and what data they can access
      ii. Who is authorized to have elevated access, and when
      iii. Who is allowed unrestricted access, and when, if required
      iv. Who is authorized to access sensitive data
      v. If temporary access is to be granted, who is authorized to have access, when they have access, and what data they can access
      vi. Exceptions to the policies
   c. Assessing the risk level for exceptions to the database access policies, and the risks and exceptions documented.
   d. Removing unused accounts.

e. Implementing administrator restrictions on access as part of access management for the database system.
f. Including the requirement to comply with database access policies in the contract when the database system is managed by service providers or contractors.
g. Identifying critical production databases.
h. Defining and documenting a disaster recovery plan in the system security plan for the recovery of production databases from a disruptive event per the IMIT 5.10 Critical Systems Standard.
i. Ensuring the database system software version is vendor supported per the IMIT 6.27 Operations Security Standard.
j. Documenting a planned upgrade path for the database system in the system security plan.

3. Follow the IMIT 6.27 Operations Security Standard if production data must be stored or processed in non-production environments.
4. Include the security schedule in the contracts with service providers and contractors managing databases on behalf of the B.C. government.
5. Before granting access to a database with sensitive personal or confidential information, ensure at least the following are met:
   a. Government employees complete the IM117 Privacy and Information Management Training; contractors and service providers complete the FOIPPA Foundations course, and appropriate security training as defined in their contracts
   b. Applications that access the databases are built following the requirements of the IMIT 6.14 Application and Web Security Standard

3.2 Design, development, and testing

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

1. Assess the database system for vulnerabilities and harden the system as part of establishing reasonable security controls by:

a. Implementing recommended database hardening practices. See Appendix A: Database system hardening guides for details.
b. Applying the CIS benchmarks applicable to the database system. See Appendix B: Center for Internet Security (CIS) benchmarks for details.

2. Configure the logging system to capture at least the following database activities or events:
   a. When data manipulation occurs (such as record inserts, deletes, and updates)
   b. When records are viewed (only applies to databases that contain confidential, or sensitive personal information)
   c. When security activities occur (such as adding, updating, and deleting user accounts; changing access permissions)
   d. When high-risk database change activities occur (such as changing database or system level configurations, installing third-party plugins/library, and changing audit logging configurations)
   e. When suspicious or abnormal activities occur (that is, any observed activity that may indicate fraud, abuse, or a security breach attempt, such as multiple login attempts and unexpected changes to database configuration or schema)
3. Ensure no individual or single team is responsible for the entire operation, control, and management of production databases and security measures. The following table shows an example of how to separate the responsibilities.

Individual/Team A	Individual/Team B
• Authorizes, approves, and reviews database access and access permissions.	• Manages database access (such as granting access to database or making access permission changes).
• Manages database system (such as making changes to the database system configuration, architecture, schema, or the platform hosting the database system).	• Manages audit logging (such as making changes in settings for logging, logging deactivation, or disposition of log records or files).
• Manages database records (such as bulk transfer or copy of data from database).	• Manages database backups.

4. Follow the IMIT 6.27 Operations Security Standard to ensure:
   a. Production databases are separated from non-production databases.
   b. No database management system links are defined between the production and non-production databases.
5. Use an OCIO shared account management and authentication service (for example, IDIR or BCeID) to authenticate and manage database accounts. See Appendix C: Account management and authentication for details.
6. Follow the IMIT 6.27 Operations Security Standard and the IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard requirements to:
   a. Define and document security responsibilities for the database system in the system security plan.
   b. Develop and document supporting and operating procedures to secure production databases in the system security plan.
7. For critical database systems:
   a. Establish a disaster recovery plan and skilled resources (see IMIT 5.10 Critical Systems Standard for details).

b. Configure the database system for point-in-time recovery to meet the integrity requirements of the information in the database system. See Appendix D: Database backup and archiving for details.

8. Ensure the organization's change management process[5] includes authorization and testing before implementation.

3.3 Implementation, operations, and disposition

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

1. Maintain an inventory of its databases (production and non-production) per the IMIT 6.23 Asset Management Security Standard.
2. Implement and maintain documented security operating procedures per the IMIT 6.27 Operations Security Standard.
3. Ensure database audit logging and log is activated per the IMIT 6.27 Operations Security Standard for at least the following:
   a. Escalation of access privileges
   b. Configuration changes
   c. Database schema changes
   d. Security events and incidents related to:
      i. Database management controls
      ii. Access management controls
   e. When personal information is stored in database systems, the following is logged:
      i. Who (or what) accessed the database records
      ii. Time and date the database records were accessed
      iii. Details, including number, of the database records accessed
      iv. Type of access made (read, change, or delete)
      v. How the database record was accessed (automated or human)
      vi. Location access was made (geographic location or IP address)

[5] See the Defensible Security Framework security directive on change management and IMIT 6.27 Operations Security Standard, Appendix A.

4. Monitor and audit privileged user activity on production databases per the IMIT 6.27 Operations Security Standard to:
   a. Ensure segregation of duties is maintained.
   b. Detect and limit opportunities of privileged access abuse.
5. Update and test (verify) the disaster recovery plan at least annually. See Appendix E: Disaster recovery testing.
6. Assess regularly[6] and manage database systems vulnerabilities by prioritizing and applying database patches for vulnerabilities based on the vulnerabilities' risk severity and potential impact to the confidentiality, availability, and integrity of the information in the database.
7. Follow the patching schedule in the OCIO patch guidelines and document all patching activities in the system security plan for the database system per the IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard. For database systems subject to regulatory standards, follow the required patching schedule of the standards instead if the schedule exceeds the OCIO patch guidelines.
8. For all copy or transfer of bulk data from production databases to non-production environments or to third parties:
   a. Ensure the business operations procedures require documenting and obtaining approval[7] for any data copy or transfer.
   b. Use encrypted media for the copy or transfer of data.
   c. Desensitize sensitive data in production data before the copy or transfer of data to non-production environments or to third parties.

[6] Vulnerability assessments should be conducted at least annually. Vulnerability assessments MUST be conducted when:

- New security threats could pose a risk to the database system.
- A change is made to the database system.

[7] Depending on the sensitivity of the data, senior levels of approval may be required; for example, the Ministry Chief Information Officer approval.

d. Implement security controls that are equivalent to the production environment in non-production environments, or specify such requirements in agreements or contracts with third parties.
e. Document and apply conditions for when and how production data can be used in non-production environments.
f. Require third parties to adhere to confidentiality clauses or requirements in contracts when using production data.
g. Document the requirement to erase[8] production data held in the non-production environment or by third parties when it is no longer needed in operating procedures, or in agreements or contracts with third parties.

9. Review at least annually the list of users and accounts that have access to databases containing production data (that is, in production and non-production environments), and their access permissions to confirm that only authorized users and accounts have access, and their access permissions do not exceed what they need to perform their job (per the IMIT 6.24 Access Control Security Standard).

4. Revision history

These specifications are reviewed annually and updated as needed.

Version	Revision Date	Author	Description of Revisions
1.0	August 2024	S. Gopaldas Johnston	New.

5. Contact

For questions regarding these specifications, contact:

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

[8] See IMIT 6.29 Systems Acquisition, Development, and Maintenance Security Standard for details on erasure requirements.

Appendix A: Database system hardening guides

Ensure basic security controls are in place to protect confidential or sensitive personal information in the database system by:

1. Applying the security practices to harden the database management system as recommended by the database management system vendor (for example, Oracle, IBM, Microsoft, AWS, Google).
2. For vendor-agnostic NoSQL and SQL database systems hardening practices, also consider following the OWASP Database Security Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html

Appendix B: Center for Internet Security (CIS) benchmarks

1. Apply applicable CIS benchmarks for the database system first in the test environment.
2. Assess[9] and prioritize[10] reported vulnerabilities in your database system for fixing.
3. Test and approve fixes for the vulnerabilities before implementing them in the production environment.

Notes:

1. Hardening the database system using CIS benchmarks as guidelines is one step in securing the database system. The need for secure configurations is referenced throughout the CIS Critical Security Controls (CIS Controls). The CIS Controls are a general set of recommended practices for securing a wide range of systems and devices.
2. CIS Controls are mapped to most major security frameworks such as NIST Cybersecurity Framework (NIST 800-53), ISO 27000 series, CSA Cloud Controls Matrix (CCM), Azure Security Benchmark, ISACA COBIT 19, SOC2, and regulations such as PCI-DSS, HIPAA, NERC CIP, and FISMA. Applying the CIS Controls will also help achieve compliance with FIPPA[11].

[9] Audits performed on a database system MUST be conducted by an independent party with the same skills as the database system design team to ensure an objective assessment is performed.
[10] The audit reports are presented to the executive team for prioritization.
[11] Freedom of Information and Protection of Privacy Act (FIPPA) is the privacy legislation that applies to all public bodies in B.C. It is equivalent to the federal Personal Information Protection and Electronic Documents Act (PIPEDA) legislation that applies to private-sector organizations. PIPEDA is the Canadian version of the U.S. Health Insurance Portability and Accountability Act (HIPAA) legislation.

Appendix C: Account management and authentication

1. An OCIO shared account management and authentication service[12] MUST be used for account management and authentication per the Core Policy and Procedures Manual (CPPM) Chapter 12.
2. Request an exemption when an OCIO shared account management and authentication service cannot be used (as required in the IMIT 6.24 Access Control Security Standard) or when authentication for a production database is not possible.
3. If another account management and authentication service is to be used in place of an OCIO shared account management and authentication service, it MUST provide similar capabilities to:
   a. Manage and authenticate accounts, such as individual user or application/system accounts (see Notes).
   b. Manage and implement password controls.
   c. Manage privileged identities (privileged identity management).

Notes:

1. Per IMIT 6.24 Access Control Security Standard, sharing system account passwords with different individuals is prohibited. Shared passwords make it difficult to prove which individual is accountable for unauthorized or illegal activities conducted on the system. If shared accounts cannot be avoided, follow the guidance in the IDIR Account Lifecyle Management knowledge base article on MySC, specifically the section titled “Positional Account.”
2. If password sharing for privileged accounts cannot be avoided due to technical constraints, do the following:
   a. Apply for an exemption to the IMIT 6.24 Access Control Security Standard and implement mitigative measures to preserve the accountability for all privileged activities conducted on the database system.

[12] See IMIT 6.24 Access Control Security Standard for details.

b. Restrict the use of the shared privileged account to a single user at a time and maintain records on who used the shared privileged account and when.
c. Reset the password for the shared privileged account before assigning the account to a different individual.
d. Maintain accurate and secure records on who and when the shared privileged account was assigned.
e. Use multi-factor authentication for the shared privileged account.

Appendix D: Database backup and archiving

Backup

1. Configure a database as part of disaster recovery planning for point-in-time recovery to minimize data loss due to data corruption or a disaster.
2. Define the recovery point objective for the database to ensure any data loss does not exceed the data loss tolerance threshold. For instance, if the loss of an hour's worth of data can be tolerated, the recovery point objective is 1 hour.
3. Base the backup frequency for a database on the defined recovery point objective. The following table maps recovery point objectives to backup frequencies.

Recovery point objective	**Backup frequency**
Critical 0–1 hour	When any loss of data cannot be tolerated, the recovery point objective needs to be set for continuous backup. Data backups must be configured to occur **whenever a change occurs** to the data.
Semi-critical 1–4 hours	When some loss of data can be tolerated (up to 4 hours of data), the recovery point objective is up to 4 hours. Data backups must be configured to occur **every 4 hours or less**.
Less critical 4–12 hours	When the loss of data for up to 12 hours can be tolerated, the recovery point objective is up to 12 hours. Data backups must be configured to occur **every 12 hours or less**.
Infrequent 13–24 hours	When the loss of data for up to 24 hours can be tolerated, the recovery point objective is up to 24 hours. Data backups must be configured to occur **every 24 hours or less**.

Note: A data loss tolerance threshold is expressed by the recovery time objective. A recovery time objective is about having policies and technologies in place to enable

recovery from a system failure or disaster within a certain duration to minimize the data loss or the duration of unavailability.

Archiving

1. Define and adopt an archiving strategy for the data in the database that meets the business requirements for availability in terms of speed and access frequency to the archived data as well as retention policies. Archiving also helps to prevent or minimize data loss.
2. Configure the database system to meet the objectives of the archiving strategy.
3. Review and update the archiving strategy when there are updates to retention policies, business priorities, security concerns, government regulations, or technology. Update the archiving settings on the database system to meet the updated archiving strategy requirements.
4. Ensure the security protections for access to, transfer, and storage of the archived data are equivalent to the security protections for the data in active use.

Appendix E: Disaster recovery testing

Conduct disaster recovery testing when:

1. Significant changes are made to the database system.
2. Annually, if no changes were made during a 12-month period. Annually can be based on either a fiscal or calendar year.

The five types of disaster recovery testing are:

1. **Read through test.** Also known as plan review. Copies of disaster recovery plan are distributed to all interested parties for review to identify missing elements and eliminate inconsistencies.
2. **Structured walkthrough.** Referred to as a “table-top exercise” in which disaster recovery team members gather and role play a disaster scenario.
3. **Simulation test.** Disaster recovery team members are presented with a scenario and asked to develop a response while using the disaster recovery plan.
4. **Parallel test.** Relocate personnel to an alternate recovery site and implement site activation procedures.
5. **Full-interruption test.** Shut down the primary site and shift operations to the backup site.