BRITISH COLUMBIA
Office of the Chief Information Officer

DATABASE SECURITY STANDARD FOR INFORMATION PROTECTION

Information Security Branch
Office of the Chief Information Officer | Province of BC

Document Version 1.0
Published: April 4, 2018

Replaces: None

Introduction

This document contains standards for the protection of confidential, personal, and sensitive, information in databases (or "database management systems"). This Standard was developed in collaboration with ministries, endorsed by the Architecture and Standards Review Board, and approved by the Government Chief Information Officer.

Applicability

This Standard applies to database systems used for BC Government services, and will establish the baseline security controls for a secure database system.

This Standard identifies a minimum set of database system security controls. Privacy Impact Assessments (PIA) and Security Threat and Risk Assessments (STRA) may identify additional database security requirements.

Compliance Schedule

A compliance schedule will be developed in cooperation with the ministries, endorsed by the Architecture and Standards Review Board and approved by the Government Chief Information Officer.

For new database systems:
Controls in the standard are requirements for the procurement and/or implementation of new database systems. Where a new database system cannot reasonably be made compliant with this Standard but does not pose an unacceptable security risk and does not contravene Office of the Chief Information Officer (OCIO) strategic objectives, then an exemption may be requested through the OCIO.

For existing database systems:
Upon review, existing database systems may be found to pose unacceptable security risks. An existing database system must be brought into compliance with this Standard if it poses an unacceptable security risk. For existing database systems which do not pose an unacceptable security risk, ministries are encouraged to weigh resourcing of retroactive compliance efforts against resourcing other applicable, compensating, security controls.

.

Glossary

Critical (system) - Any IM/IT service, system, or infrastructure component that is deemed necessary by the SYSTEM OWNER to deliver a MISSION CRITICAL, or BUSINESS PRIORITY function, is a critical system for the purposes of this Standard.

Data Custodian – Person accountable for operational policy, definitions, rules, standards, structure, content, use and disposal for data under their responsibility.

Data Steward – Assumes some responsibilities of Data Custodian, but is not accountable for the data.

Database system(s) - A collection of organized information in a regular structure, in a machine-readable format accessible by a computer. Also: "Database Management System (DBMS)" or simply "database".

Environment - A term describing the setting where a part of the software lifecycle occurs, i.e. Development Environment, Testing Environment, Production Environment, etc.

Information - Data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision making.

Least privilege - A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

***MISO* -** Ministry Information Security Officer : The single point of contact for information security issues and related concerns in the ministry. For more information about the MISO role, refer to Link. For a list of all MISOs, refer to this Link.

***MPO* -** Ministry Privacy Officer: The single point of contact for privacy issues and related concerns in the Ministry. For more information about MPOs role, refer to this link. For a list of all MPOs, refer to MPO Directory.

***OCIO* -** Office of the Chief Information Officer (OCIO) leads strategy, policy and standards for telecommunications, information technology, and the management of the IM/IT investment portfolio for the Province.

***PIA* -** Privacy Impact Assessment, an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Production Database - Information that is persistently stored and used to conduct business processes. It must be accurate, documented and managed on an on-going basis to ensure its value to the organization.

Reasonable - Fair and moderate, not excessive, to a degree dictated by sensible evaluation of the factors impacting a decision.

Segregation of duties - The concept of sharing responsibilities for processes across more than one party. Segregation of duties reduces opportunity for fraud or malicious use by ensuring that there are checks in place for the conduct of critical operations. For example, segregation of duties can be applied to prevent fraud by making the party who reviews database use logs unable to modify those logs.

***Service Owner* -** the Single Point of Contact who is accountable for all aspects of a service throughout the service life cycle.

***Service Provider* -** a person or an organization retained under contract to perform services for the Government of British Columbia.

***STRA* -** Security Threat Risk Assessment, a tool for understanding the various threats to IT systems, determining the level of risk these systems are exposed to, and recommending the appropriate level of protection.

Suspicious or abnormal activities - Defined by the Information Owner and Information Custodians, and are activities that for one reason or another are unusual and may indicate fraud or unauthorized access.

Note to Readers

This Standard is ordered to follow a typical system development life cycle, from initiation to disposition of a database system.

Terminology

The term “MUST” is defined as an absolute requirement of the specification.
“SHOULD” means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications must be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the ADM of the information owner. For the purposes of this Standard “information owner” is defined in the Province’s Information Security Policy.

Standard/Controls:

Database System Planning, Acquisition & Requirements

1. Ministries and Service Owners must identify information security requirements for new database systems or enhancements to existing database systems. These information security requirements must include confidentiality, availability, integrity and access requirements.

2. Ministries and Service Owners must manage security risks related to production databases.

3. Ministries and Service Owners must ensure that data in production databases is classified from a security perspective and protected based on that security classification.

4. Ministries must identify critical production databases. Ministries must ensure that a tested Disaster Recovery Plan and skilled resources are in place to be able to recover from a disruptive event that has an unacceptable impact to critical production databases.

5. Ministries and Service Owners must work with Ministry Privacy Officer(s) to ensure that reasonable security controls are in place to protect personally identifiable information within databases.

6. Ministries and Service Owners must determine the use of encryption for data in transit and at rest based on the classification of the database information and the risk of unauthorized access.

7. Responsibilities must be separated so that no single person or team is entirely responsible for operations of production databases and security measures, controls, and management.

8. Formal user authorization process must be in place for granting and revoking access to production databases as defined by business requirements.

9. Ministries and Service Owners must ensure that employees accessing production databases have completed information security and privacy training.

10. Ministries and Service Owners must ensure that production databases' environments are isolated from non-production environments.

11. Use of production data in non-production environments is only permitted based on business needs with appropriate security controls in place.

12. Service Providers and Contractors accessing information within databases must comply with non-disclosure agreements (NDAs) and contracts governing their service provision.

Design, Development & Testing

13. Where reasonable, Ministries and Service Owners must ensure that production databases are configured to capture, record and alert on key data and database activities including, but not limited to:
    - view access to confidential or personal information;
    - data manipulation activities (e.g. insert, delete & change);
    - security activities (e.g. creation/deletion of users);
    - high-risk database activities (e.g. turn audit on/off); and
    - suspicious or abnormal activities.

14. Production databases requiring password authentication must utilize authentication lookup against approved BC Government authentication services (i.e. BCeID and IDIR) system. An exemption must be requested when this authentication is not possible.

15. Ministries and Service Owners must conduct regular database vulnerability assessments to identify, analyze and manage security risks related to critical and high risk database vulnerabilities.

16. Ministries and Service Owners must develop, document, maintain and implement security operating procedures and responsibilities for production databases.

17. Ministries and Service Owners must ensure changes to database systems follow the organization's Change Management processes, including changes being tested and authorized before implementation in production systems.

18. Ministries, Service Owners and Service Providers must ensure that a tested up to date Disaster Recovery Plan (DRP) and skilled resources are in place to meet business objectives.

Implementation, Operations & Disposition

19. Service Providers and Service Owners must develop and maintain documentation for production databases that is necessary for ongoing support/operations and future changes/upgrades.

20. Ministries and Service Providers must apply database patches on a regular and timely basis commensurate with the criticality of the database.

21. Copy or transfer of bulk data in production databases outside production databases and outside current operating procedures must be formally documented by the Ministry and restricted to specific business situations.

22. The Ministry and Service Owners must monitor and audit production databases to ensure privileged database users maintain appropriate database and access management controls including segregation of duties.

23. A formal review of users and their access permissions to databases containing production data must be performed by the Ministry or Service Owner on an annual basis.