Database Security Standard for Information Protection (DSSIP) Frequently Asked Questions (FAQ)

Contents

Office of the Chief Information Officer

General Questions

What is the DSSIP?

Databases play a critical role in protecting government information. The purpose of the Standard is to formalize database security best practices and standardize these practices across BC government databases. The DSSIP outlines steps and measures to ensure data are secured when new databases are created or existing ones are modified. The Standard also lays out key roles and responsibilities for Information Owners and Information Custodians.

Back…

Who is the intended audience for the DSSIP?

- Information Custodians - security professionals, database administrators, and those responsible for routine database operation on behalf of Information Owners.
- Information Owners - those who have the responsibility and decision making authority for information throughout its life cycle. Information Owners typically work with their delegates like architects or system/business analysts to address database security.
- Security Professionals in ministries planning to get database infrastructure in future. Ministries that are considering new database infrastructure must be aware of all standards and policies with which they will have to comply.

Back…

Why should I care about DSSIP?

The DSSIP comprehensively outlines the steps required to ensure that databases used in the BC government are secured from intrusion, fraud and fraud-related activities. This Standard allows for different security needs based on different sensitivity levels of stored information and legacy systems, and is consistent with other national and international laws and standards.

Back…

Office of the Chief Information Officer

Who developed the DSSIP?

The Information Security Branch of the Office of the Chief Information Officer developed the Standard, in collaboration with the ministries and other impacted organizations.

Back…

Where can I get more information about Information Security?

Please visit the Information Security Advisory Services website where there is information on many of our processes and standards. For specific questions, please contact Information Security Branch Advisory Services, at InfoSecAdvisoryServices@gov.bc.ca.

Back…

Technical Questions

What is meant by the term 'Database System'?

Database management system (DBMS) - the Standard only focuses on systems in which government data are stored and managed. This does not include applications, middleware, utilities, and other software that may contain "databases" of locally-used data.

Back…

What is meant by the term 'BC Government service'?

In the DSSIP 'BC Government service' includes both 'system' and 'service'. 'Service' indicates the end user perspective, meaning that they are being served in a certain way. Services could be web-based digital services, or in-house (delivered through agents).

In the DSSIP, this includes a procedure or process used to deliver services to users (system) as well as the end-product, or service, delivered.

Back…

What is an 'Information Owner' and 'Information Custodian'?

According to the Information Security Policy (s. 2.1.3):

- **Information Owners** have the responsibility and decision-making authority for information throughout its life-cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

- **Information Custodians** maintain or administer information assets on behalf of the Information Owners.

Back…

Where did the control statements come from?

The 36 control statements in the DSSIP are drawn from a variety of sources:

- Common database security best practices;
- Existing BC Government standards and policies adapted to apply to database security. Key documents include the Information Security Policy, the Critical Systems Standard, and the Privacy Management & Accountability Policy; and
- ISO/IEC 27002 - *Information technology – Security techniques – Code of practice for information security management*

Back…

What is meant by "suspicious or abnormal activities"?

As defined in the Standard, these are activities that are unusual and may indicate fraud or unauthorized access. It is up to the business unit to identify "suspicious or abnormal activities" based on the business and context. For example, copying a large amount of data or accessing the database after-hours may be a normal activity for one business unit, but a suspicious or abnormal activity for others.

Back…

If the current Information Security Classification Framework is updated or deprecated, will it affect the Standard?

No, changes to the Information Security Classification Framework will not substantially impact the Standard as the controls still apply regardless of the classification system or the way the data are classified. The critical point, and the intent of controls 3 and 6, is that production data are appropriately classified and encrypted.

Back…

Will there be a broad exemption for non-SQL Server Databases since Active Directory authentication is not possible?

Programmatic access to a database system (i.e. an application accessing a database) must use the enterprise authentication in order to provide proper password management.

Back…

What is the scope of the Disaster Recovery Plan (DRP) requirement?

This section reflects the requirements in the Critical Systems Standard to assist your organization to recover from disruption. It is up to the organization to decide on the scope (e.g. production only or critical production only) for the DRP based on the business needs.

Back…

What about Credentials Management? Isn't it critical to database security?

Additional standards are under development to address Credentials Management, and will be posted to the IM/IT Standards website as soon as they are available.

Back…