BRITISH
COLUMBIA
Ministry of
Citizens' Services

COMPLIANCE SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0

Published: September 2019

Table of Contents

I Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references “ sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.

1 Compliance

This chapter describes requirements for verifying that information systems comply with relevant statutory, regulatory, and information security contractual clauses. Compliance policies identify what to do to ensure that the Province is in compliance with applicable laws and policies. Processes to monitor the extent to which information systems follow policies include conducting security reviews, assessments and the systematic analysis of logged information.

1.1 Compliance with legal and contractual requirements

1.1.1	**The legislative, statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.** **a) Applicable legislation and contractual requirements**

Purpose: ***To ensure that the legal requirements of information systems are documented.***

1.1.1 a) Applicable legislation and contractual requirements

Information Owners are responsible for ensuring that legislative, statutory, regulatory, policy and contractual requirements of each information system are:

- Identified and documented when commencing a system development or enhancement initiative;
- Reviewed prior to, or concurrent with, changes to legislation, regulation or policy; and,
- Explicitly identified in contracts and service agreements, and included in:
  - Privacy Impact Assessments,
  - Security Threat and Risk Assessments,
  - System Security Plans,
  - Risk Management Plans, and,
  - Business Continuity Plans.

Privacy requirements for information systems containing or handling personal information are defined in the Freedom of Information and Protection of Privacy Act (FIPPA) - Policy and Procedures Manual (PPM) and the Core Policy and Procedures Manual (CPPM).

Recommended Tests:

Note: 1.1.1 is reported on as part of the annual information security review.

- Demonstrate that legislative, statutory, regulatory, policy and contractual requirements of each information system are identified and documented.

1.1.2 Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licencing.
a) Intellectual property rights of external creators and owners
b) Intellectual property rights for government assets

Purpose: To protect the intellectual property rights of information and software creators and owners.

1.1.2 a) Intellectual property rights of external creators and owners

Information Owners and Information Custodians must protect intellectual property by:

- Ensuring that information and software is only acquired from reputable vendors;
- Maintaining proof or evidence of ownership or right to use;
- Adhering to the terms and conditions of use associated with intellectual property;
- Ensuring the maximum number of users permitted is not exceeded;
- Implementing processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licences;
- Requiring the removal of unlicensed information and software from government information systems;
- Informing employees of government policies, including the Appropriate Use Policy;
- Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
- Complying with terms and conditions for information and software obtained from public networks (e.g., “free for personal use only”, open source).

1.1.2 b) Intellectual property rights for government assets

Policy for the intellectual property of government information assets is in the Core Policy and Procedures Manual 6.3.4 – Corporate Supply and Disposal Arrangements which is managed by the Intellectual Property Program of the Office of the Government Chief Information Officer.

Recommended Tests:

Note: 1.1.2 is reported on as part of the annual information security review.

- Demonstrate software is only acquired through reputable sources, and that copyright is not violated.
- Demonstrate asset registers, maintaining evidence of ownership of licences, maximum number of users permitted within the licence and carrying out review.
- Demonstrate licencing agreements for software provide evidence of adherence to terms and conditions.
- Demonstrate Ministry-developed intellectual property has the appropriate copyright notices.
- Demonstrate investigations or reviews are conducted to detect unlicensed software.

1.1.3 Government records must be protected from loss, destruction and falsification, unauthorized access, release, and disposal in accordance with legislative, regulatory, contractual and business requirements.
a) Protection of records

Purpose: To ensure compliance with legislative and policy requirements for government records.

1.1.3 a) Protection of records
When deciding upon protection of specific organizational records, Information Owners and Information Custodians must consider the information security classification.

Information Owners and Information Custodians must ensure the protection of records by:

- Using government guidelines on the retention, storage, handling and disposal of records and information;
- Following a retention schedule identifying records and the period of time for which they should be retained; and,
- Maintaining an inventory of sources of key information.

Disposal of government records must follow the records schedule as defines in the Information Management Act. Policy requirements for records management are in the Core Policy and Procedures Manual 12.3.3 – Information Management, and the Recorded Information Management Manual.

Recommended Tests:
Note: 1.1.3 is reported on as part of the annual information security review.

- Demonstrate that employees are made aware of and follow the document disposal requirements.

1.1.4 Privacy and protection of personal information must be ensured as required in legislation and regulation.
a) Privacy and protection of personal information

Purpose: ***To ensure the privacy and protection of personal information in compliance with legislation.***

1.1.4 a) Privacy and protection of personal information
Information Owners and Information Custodians must document and implement policies for privacy and the protection of personal information. The policy must be communicated to all employees involved in the processing of personal information. There must be Privacy Impact Assessment and Security Threat and Risk Assessment documents for all operations areas that are collecting, processing and storing personal information.

The Freedom of Information and Protection of Privacy Act requires personal information to be protected using ‘reasonable security measures’.

The Information Security Standard includes detailed controls which enable and support the protection of government information and information systems.

Recommended Tests:
Note: 1.1.4 is reported on as part of the annual information security review.

- Demonstrate user awareness is provided for dealing with personal information.

1.1.5 Controls must be in place to deter misuse of information systems.
a) Deterring unauthorized and inappropriate use of information systems

Purpose: ***To ensure employees do not create security exposures through unauthorized or inappropriate use of information systems.***

1.1.5 a) Deterring unauthorized and inappropriate use of information systems

Information Owners and Information Custodians must monitor information system usage to prevent, detect and respond to unauthorized or inappropriate use by:

- Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage;
- Implementing processes to analyze audit logs to identify potential misuse of information systems;
- Implementing system rules to prevent access to undesirable Internet sites;
- Implementing content inspection and filtering tools (e.g., for e-mail and web traffic);
- Immediately notifying employees of detected misuse (e.g., the 'Red Screen' for Internet blocking);
- Ensuring that security incidents are investigated in accordance with policy; and,
- Determining, in consultation with the BC Public Service Agency, if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for employees who have made unauthorized or inappropriate use of information system resources.

Prior to implementing information system monitoring processes, Information Owners and Information Custodians must ensure:

- Monitoring activities are compliant with legislative, legal, policy and contractual requirements and obligations;
- Employees are informed that specific activities may be monitored; and,
- Access to data gathered through monitoring processes is restricted on a 'need-to-know' and 'least privilege' basis to the fewest possible number of users.

Recommended Tests:

Note: 1.1.5 is not reported on as part of the annual information security review.

- Demonstrate audit logs are reviewed on a regular basis.

1.1.6 Cryptographic controls must be used in compliance with relevant agreements, legislation and regulations.
a) Regulation of cryptographic controls

Purpose: ***To prevent inappropriate use and unregulated importing or exporting of cryptographic controls.***

1.1.6 a) Regulation of cryptographic controls

When cryptographic controls are used, Information Owners and Information Custodians must:

- Ensure that the use of cryptographic control(s) is supported by an Information Security Threat and Risk Assessment;
- Consult with the Corporate Information and Records Management Office and Office of the Government Chief Information Officer regarding the records management, electronic commerce, information access, privacy and security issues prior to acquiring cryptographic controls;

- Ensure encrypted government information assets do not become unavailable due to unavailability or loss of cryptographic keys by implementing a process to manage cryptographic keys as defined by the Government Chief Information Officer; and,
- When acquiring cryptographic controls from outside Canada, the procurement must be from a reputable vendor who can provide reasonable assurance on the legality of import into Canada.

The Office of the Government Chief Information Officer will:

- Develop and document cryptographic key management processes;
- Provide guidance and assistance to Ministries and agencies in the selection and use of cryptographic controls; and,
- Establish and publish cryptographic standards.

Recommended Tests:
Note: 1.1.6 is reported on as part of the annual information security review.

- Demonstrate cryptographic controls are used as required.

1.2 Information security reviews

1.2.1	**Independent reviews of information security must be regularly conducted.** **a) Independent review of information security** **b) Remediation**

Purpose: ***To provide an assessment of the Information Security Program*.**

1.2.1 a) Independent review of information security
Independent reviews are necessary to ensure the continuing suitability, adequacy and effectiveness of the organization’s approach to managing information security. The review must include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

The Chief Information Security Officer must initiate an independent third party review of the Information Security Program every two years including:

- Assessing the operational effectiveness of the Information Security Program;
- Documenting the results; and,
- Reporting the results of the review to senior management.

1.2.1 b) Remediation
Information Owners and Information Custodians must address the identified weaknesses and non-compliant controls prior to the next review.

Recommended Tests:
Note: 1.2.1 is reported on as part of the annual information security review.

- Demonstrate a review of the information security program has been conducted by an independent third party.

1.2.2	**Information Owners must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.** **a) Compliance with security policies and standards** **b) Review of controls** **c) Review of implementation of information incident report recommendations**

Purpose: ***To ensure compliance of information systems with information security policy, requirements and standards.***

1.2.2 a) Compliance with security policies and standards

Information Owners must ensure security policies and processes are implemented and adhered to by:

- Conducting periodic self-assessments;
- Ensuring employees receive regular information security awareness updates; and,
- Initiating independent assessments, reviews or audits to assess compliance with policy.

When review processes indicate non-compliance with policies, Information Owners must:

- Determine cause(s);
- Assess the threats and risks of non-compliant processes;
- Document the marginal risks where required; and,
- Develop plans to implement corrective action.

1.2.2 b) Review of controls

Information Owners must develop an annual plan which identifies information systems scheduled for a security review in each fiscal year. The information systems to be reviewed in each year should be:

- Determined in conjunction with the Ministry Enterprise-wide Risk Management Plan;
- Endorsed by the Ministry Audit Committee, or equivalent; and,
- Reported as part of the annual information resource management plan.

Information Owners must ensure that critical information systems are reviewed at least every three years.

1.2.2 c) Review of implementation of information incident report recommendations

Information Owners and Information Custodians must ensure that recommendations from information incident reports are addressed.

The Chief Information Security Officer may perform compliance reviews or audits of the implementation of recommendations from information incident reports, when necessary. The Ministry Chief Information Officer must ensure that Information Owners and Information Custodians support the audit activities.

Guidelines:

When determining the review frequency for information systems consider:

- The value of the information system as determined by a Security Threat and Risk Assessment or a Risk and Controls Review;
- Frequency of changes or updates (as changes may introduce new risks, a system which has undergone frequent changes may have higher risks); and,
- Results of previous reviews.

Internal Audit and Advisory Services, Office of the Comptroller General, should be consulted prior to issuing Requests for Proposals or contracts for independent information security reviews or audits. Self-assessment tools are available from Information Security Branch, Office of the Government Chief Information Officer.

Recommended Tests:

Note: 1.2.2 is reported on as part of the annual information security review.

- Demonstrate issues identified in the annual Ministry information security compliance review are reviewed and addressed.

1.2.3	**Information systems must be regularly reviewed for compliance with security policies and standards.** **a) Technical compliance checking** **b) Authorization to conduct technical compliance checking** **c) Reporting results**

Purpose: ***To determine if technical controls meet established government standards.***

1.2.3 a) Technical compliance checking

Information Custodians must regularly test information system technical control compliance by using automated tools to:

- Detect network intrusion;
- Conduct penetration testing;
- Determine if information system patches have been applied;
- Confirm that system technical controls have been implemented and are functioning as designed; and,
- Perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or systems changes have not been made.

1.2.3 b) Authorization to conduct technical compliance checking

Supervisors responsible for technical compliance checking and Information Custodians must ensure that:

- Information Owners and operations employees are consulted prior to initiating tests;
- The Chief Information Security Officer is notified prior to testing to prevent triggering false security alarms from the infrastructure; and,
- Automated testing of operational systems is conducted by employees authorized by the Chief Information Security Officer.

Ministries must consult with the Chief Information Security Officer prior to issuing Requests for Proposal or contracts for technical compliance checking.

1.2.3 c) Reporting results

Supervisors responsible for technical compliance checking and Information Custodians must:

- Assess results of testing and promptly develop action plans to investigate and mitigate identified exposures in consultation with the Ministry Information Security Officer;

- Provide Information Owners and the Chief Information Security Officer with copies of test results and action plans;
- Provide the Chief Information Security Officer with the internal or external audit reports immediately upon receipt; and,
- Maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

Guidelines:
The Chief Information Security Officer should:

- Develop and maintain testing processes for authorizing/conducting tests, storing results and building on previous testing experience; and,
- Provide summarized quarterly reports to the Government Chief Information Officer on the status and results of testing.

Recommended Tests:
Note: 1.2.3 is reported on as part of the annual information security review.

- Demonstrates vulnerability testing on a regular basis, that controls are functioning, that patches are applied.
- Demonstrate authorization from the Information Owner is obtained prior to technical compliance testing.
- Demonstrate an action plan that documents control weaknesses and the verification of remediation.
- Demonstrate the Chief Information Security Officer is notified prior to technical testing.
- Demonstrate that Information Owners and Information Custodians provide copies of reviews and audit reports to the Chief Information Security Officer.