July 30, 2010

Information Security Classification Framework

Supplemental to the Information Security Classification Standard

Security Classification: PUBLIC

BRITISH COLUMBIA
The Best Place on Earth

Office of the Chief Information Officer
Province of British Columbia

Information Security Classification Framework

Overview

Government Policy Requirements

The government Core Policy Manual (Chapter 12 IM/IT Management) requires that information assets be protected. Further, the Office of the Chief Information Officer - Information Security Policy (ISP) requires that business/information owners ensure that the systems and the information in those systems are protected commensurate with their information classification (ISP 2.1.3 and 3.2.1).

An information security classification system is one of the critical components of good information security. An information security classification system assists in determining the value and sensitivity of, and the protective measures to be applied to, the information. In the absence of a system, there is a risk that:

- All information may be regarded as highly classified and the cost of the measures to protect the information far exceeds the value and sensitivity of the information; or
- Highly sensitive information is not sufficiently protected.

As part of the government 2004-06 Security Enhancement Program, an information security classification system (or standard) was developed and approved. However, the standard was not fully implemented by the ministries due to the complexity of, and the lack of clarity as to the benefits of, the classification system. Further, at the time the classification system was approved, the available security controls were not well defined or communicated in relation to the standard.

Working Team

In 2009, the Office of the Chief Information Officer formed a working team, consisting of ministry and central agency representatives, to develop and recommend an Information Security Classification framework to support the implementation of the standard. In developing the framework, the working team were requested to achieve the following:

- An efficient and easy-to-use classification scheme to apply to the information assets
- A framework document to assist with the assessment and classification of information
- A framework that supports standards and policy and meets the business requirements

Framework

The working team developed a framework that will assist the Ministry Information Security Officers (MISO) or delegated officer(s) with the implementation of the information security classification.

A description of the framework is as follows:

- As defined in the standard, there are three information security classification levels: High, Medium and Low. These security levels are easy to understand and are consistent with risk classifications used in other methodologies (e.g., Security Threat and Risk Assessments and Financial Risk and Controls Reviews), deployed within government.

- For each information security classification level, a detailed description is provided to describe the potential level of risk or harm in the areas of financial, personal, and operational (business) areas.

- Illustrative examples are provided to show when business information/system is subject to a breach of confidentiality, integrity and/or availability, there is an associated financial, personal and/or operational harm. These examples are to provide a better understanding of each classification level.

- Examples of security controls (i.e. leading practices in tools, techniques, and processes to protect the information) are provided to show the protective measures that will need to be considered for each information security classification level. The list of control examples does not limit the choice of controls as technology changes and new controls will be introduced.

- Once information is classified, the information is to be labelled. The six labels, linked to an associated security level, are: Cabinet Confidential (High), High Sensitivity (High), Medium Sensitivity (Medium), Personal (Medium), Low Sensitivity (Low), and Public (Low).

Application of the Framework

The Ministry Information Security Officer is the single point of contact for advice, guidance and communication about the information security classification within the ministry. Further, the Ministry Information Security Officer works closely with the Ministry Records Officer and the Information Access Operations to implement the information security classification.

The framework is intended to assist the Ministry Information Security Officers or delegated officer(s) in communicating the application of the framework and/or labelling of the information. Since each ministry deals with different businesses, it is recommended that each ministry develops its own guidelines (based on this framework) and provide more ministry-specific examples. To facilitate the ministry internal communication, the working team will provide a ministry communication template and a policy summary on the information security classification.

As information security classification is closely related to records management and risk management, the application of the framework and labelling could be applied through the ministry processes and/or the following means:

- TRIM, the corporate records management system, which can facilitate the labelling of records
- iSMART, the corporate risk directory, which currently captures the risk assessments for government systems can facilitate the application of the information security classification
- The data custodianship provisions of data governance, which requires that data at all levels have an understood security review

However, as not all ministries have yet adopted these systems or tools, other means for communicating and implementing the framework will need to be considered.

Levels	Definition	Control Examples	Illustrated Examples	Labels
High	Could possibly be expected to cause **extremely serious personal or enterprise injury**, including any combination of: Financial harm, such as: a. Extremely significant loss of money or tangible assets b. Exteremly significant penalties or recovery costs incurred Operational harm, such as: a. Severely impaired decision making, resulting in severe loss of program control b. Program closure or serious sanctions as a result of breach of legislation, contract or regulatory standards c. Major political impact - complete and extended loss of public trust of or confidence in government Personal harm, such as: a. Loss of life b. Extreme hazard to public safety c. Wide-spread social hardship d. Major provincial ecenomic hardship	Security control examples include: • Access control to named individuals and positions • Physical storage of information server or file cabinet in a locked space • Tight accountability check and approval (e.g., electronic or physical access log management for sign in and out, access by approval/authentication) • Multifactor authentication (standard two-factor or plus biometric or nonce) • Data encryption • Network isolation for the servers from the corporate network • Backup mechanism for the isolated servers • High availability measures (e.g., duplication) • Integrity verification code for compromise check (e.g., hash, message digest)	**Confidentiality** examples include: a. Cabinet documents, b. Extremely confidential information and information that is intended for access by named individuals or positions only, c. Information relating to the case files of a major or serious crime (e.g., murder, burglary, rape, etc. - 'summary conviction offences' and 'indictable offences', defined by the severity of a crime), d. Identities or information about undercover police, police informant, or witness protection subject, and e. Provincial budget prior to public release. **Availability** examples include: a. Crisis communication during emergencies and provincial response plan and logs, b. Provincial base mapping and geomatics (Provincial Baseline Atlas: aerial photography, geo-spatial references, geomatics programs - see Base mapping and geomatics ORCS), c. Emergency health information services (e.g., pandemic), d. Law enforcement information (e.g., dangerous offenders files - see Corrections ORCS), e. Essential law enforcement communications information, f. Information of government activities and decision making on major projects (e.g., inability to provide legal evidence of government activities may lead to significant financial loss), and g. Mission critical systems that must be continuously available during regular **Integrity** examples include: a. Information systems used for testing food or water supplies that could result in loss of life or severe illness, b. Information systems related to emergency health care, c. Information systems on road conditions, avalanche warnings and other hazards, d. Extremely large financial transactions (e.g., over $1 million), and e. Corporate financial systems.	**Cabinet Confidential, High Sensitivity**

Levels	Definition	Control Examples	Illustrated Examples	Labels
Medium	Could possibly be expected to cause **serious personal or enterprise injury**, including any combination of: Financial harm, such as: a. Significant financial loss, penalty, or recovery expense Operational harm, such as: a. Significant impact on service levels b. Serious loss of confidence in a government program c. Damage to partnerships, relationships and reputation d. Staff forced to resign Personal harm, such as: a. Serious personal hardship or embarassment	Security control examples include: • Access control to specific groups of employees, external service providers • Accountability log (e.g., electronic or physical access log management for sign in and out) • Multifactor authentication (Standard two-factor) • Data encryption • Integrity check	**Confidentiality** examples include: a. Information that is intended for access by a specific group of employees only, b. Sensitive personal information (personal medical or health information, tax information, information describing personal finances, eligibility information for social benefits), c. Disclosure of trade secrets or intellectual property, d. Provincial standardized tests for schools, e. Industrial trade secrets, business or other third-party information, f. Information on archaeological and heritage sites (Provincial Heritage Register), g. Information relating to minors (e.g., adoption and foster records, medical and forensic psychiatric services - see Forensic Psychiatric Services ORCS), h. Information on young offenders (e.g., bail documents, diversion, sentencing or probation case files, etc. - see Corrections ORCS), and i. Calendar information (executive). **Availability** examples include: a. Payments of benefits to citizens (e.g., BC Benefits, Disability Benefits, Guaranteed Available Income for Need - see Social Services ORCS), b. Business continuity information for recovery of accommodation, telecommunications, etc.), c. Government payroll and payment systems, d. Financial management information systems, and e. Information systems that must not be unavailable beyond 1 business day. **Integrity** examples include: a. Information assets related to food or water supplies that would not meet expected standards of quality but not cause illness, b. Financial transactions (e.g., over $100,000), c. Identity information that could be used for criminal purposes (e.g., from Vital Stats, ICBC), d. Information on investigations and active incidents, e. Employee personnel files and work history data (e.g., CHIPS, signed copies of oath of employment and standards of conduct, OIC for executive appointments, emergency contact information, copies of verified documents confirming job qualifications, etc. - see Public Service Personnel Management Services ORCS), and f. Documentation of forfeiture of rural property (e.g., forfeiture absolute certificates - see Taxation Revenue Collections ORCS).	**Medium Sensitivity, Personal*** * Personal label is used for information that identifies a person and its disclosure may cause a serious harm to the person. When the "personal" information is combined with higher sensitive information, it should be classified as "High".

Levels	Definition	Control Examples	Illustrated Examples	Labels
Low	Could reasonably be expected to cause **limited or no injury** to individuals or enterprises, including any combination of: Financial harm, such as: a. Limited financial loss Operational harm, such as: a. Limited impact on service levels b. Reduced staff effectiveness due to loss of morale Personal harm, such as: a. Minor embarassment or inconvenience	Security control examples include: • Access control to employees and approved non-employees (contractors and citizens) • Accountability log (e.g., electronic or physical access log management for sign in and out) • Data encryption on desktops • Integrity check • Availability measures • Limited access control capability • Common system logging for system and service access	**Confidentiality** examples include: a. Information that is generally available to employees and approved non-employees (e.g., contractors, vendors, ASD providers, consultants, or interjurisdictional partners), b. Confidential and/or sensitive information, c. Basic personal information, d. Ordinary meeting agendas and minutes, e. Communications to claims clerks, f. Unauthorized release of the job applicants' names, and g. Calendar information (non-Executive). **Availability** examples include: a. Denial of service resulting in status of social assistance application not being available, b. Inability to renew a fishing licence, c. Temporailiy unavailable government-wide tools (e.g.,e-Performance, Time-On-Line, etc.), d. Information systems that can be down for up to 3 days, e. Certain delay to access the information is tolerable, and f. External press releases, media/public distribution. **Integrity** examples include: a. Information assets related to administrative information, b. Operational procedures related to non-critical activities, c. Financial transactions (e.g., under $100,000), d. Provincial budget after public release, e. Public accounts, f. Internal information of an organization with no legal effect, g. Public education materials, and h. Non-sensitive information, suitable to release.	**Low Sensitivity, Public**