

## INFORMATION SECURITY CLASSIFICATION GUIDELINES

Government owns and manages a wide range of information from public to personal and extremely sensitive information. In principle, information is protected commensurate with its value and sensitivity. The value and sensitivity of the information is the key to classify information. Information security classification is a fundamental step in protecting against the risks associated with the unauthorized disclosure, use or loss of government information assets. All security countermeasures to protect the information are determined by its security classification level.

If information is not classified, program areas may apply either overly expensive controls unnecessarily or inappropriately weak controls. It may result in the waste of resources or high risk of information misuse, loss or disclosure. Information security classification enables the selection and implementation of adequate security controls.

Ministry is required to identify and categorize information, based on the degree of damage that could reasonably be expected to result from compromise of the information.

Government uses the classification criteria defined in the Information Security Classification Framework. In the next page, the definition and examples of each classification level are presented in the context of the ministry businesses.

A brief description of the framework is as follows:

- As defined in the information security classification standard, there are three information security classification levels: High, Medium and Low. These security levels are consistent with risk classifications used in other areas of government.
- For each classification level, a detailed description is provided to describe the potential level of risk or harm in the financial, personal, and operational aspects.
- Illustrative examples are provided to show that there is an associated financial, personal and/or operational harm when business information or systems is subject to a breach. These examples are provided for a better understanding of each classification level.
- Once information is classified, the information needs to be labelled. Labels are linked to an associated classification level. Information in the same level can

be labelled differently since they need to be handled differently though they are protected with the same level of protection measures. For example, Cabinet Confidential information and High Sensitivity information will receive the same level of protection but they will be handled differently due to business processes and handling requirements.

- There are six labels: Cabinet Confidential (High), High Sensitivity (High), Personal (Medium), Medium Sensitivity (Medium), Low Sensitivity (Low), and Public (Low).

The government's Information Security Classification Framework is flexible enough to classify the security requirements of all government records as defined in the *Interpretation Act*:

*"record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.*

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.
- Citicus ONE, 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.

The **Ministry Information Security Officer (MISO)** is the single point of contact for advice, guidance and communication about information security classification. The Ministry single point of contact works closely with the Ministry Records Officer and the Information Access Operations of Shared Services BC to implement the information security classification in the aspect of records management and FOIPP (Freedom of Information and Protection of Privacy).

Sensitivity Classification	Definition	Illustrative Examples	Labels
<p><b>HIGH</b></p>	<p>Could possibly be expected to cause extremely serious personal or enterprise injury, including any combination of:</p> <p><u>Financial harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Extremely significant loss of money or tangible assets</li> <li>Extremely significant penalties or recovery costs incurred</li> </ol> <p><u>Operational harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Severely impaired decision making, resulting in severe loss of program control</li> <li>Program closure or serious sanctions as a result of breach of legislation, contract or regulatory standards</li> <li>Major political impact - complete and extended loss of public trust or of confidence in government</li> </ol> <p><u>Personal harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Loss of life</li> <li>Extreme hazard to public safety</li> <li>Wide-spread social hardship</li> <li>Major provincial economic hardship</li> </ol>	<ul style="list-style-type: none"> <li>Personal information combined with any highly sensitive information.</li> <li>Cabinet documents.</li> <li>Extremely confidential information and information that is intended for access by named individuals or positions only.</li> <li>Justice sector confidential information (e.g., law enforcement information, court information, witness protection programs).</li> <li>Provincial budget prior to public release.</li> <li>Crisis communication during emergencies and provincial response plan and logs.</li> <li>Emergency information (e.g., pandemic, natural disasters).</li> <li>Information systems used for testing food or water supplies that could result in loss of life or severe illness.</li> <li>Extremely large financial transactions (e.g., over \$1 million).</li> </ul>	<ul style="list-style-type: none"> <li><b>High Sensitivity</b></li> <li><b>Cabinet Confidential</b></li> </ul>
<p><b>MEDIUM</b></p>	<p>Could possibly be expected to cause serious personal or enterprise injury, including any combination of:</p> <p><u>Financial harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Significant financial loss, penalty, or recovery expense</li> </ol> <p><u>Operational harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Significant impact on service levels</li> <li>Serious loss of confidence in a government program</li> <li>Damage to partnerships, relationships and reputation</li> <li>Staff forced to resign</li> </ol> <p><u>Personal harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Serious personal hardship or embarrassment</li> </ol>	<ul style="list-style-type: none"> <li>Sensitive personal information (personal medical or health information, tax information, information describing personal finances, eligibility information for social benefits).</li> <li>Information intended for a specific group only.</li> <li>Trade secrets or intellectual property.</li> <li>Business or other third party information.</li> <li>Provincial standardized tests for schools.</li> <li>Information relating to minors (e.g., adoption and foster records, medical and forensic psychiatric services).</li> <li>Information on young offenders.</li> <li>Citizen payments of benefits (e.g., BC Benefits, Disability Benefits, Guaranteed Available Income for Need).</li> <li>Business Continuity Plan information.</li> <li>Identity information that could be used for criminal purposes (e.g., from Vital Stats, ICBC).</li> <li>Information on investigations and active incidents.</li> <li>Law enforcement records.</li> <li>Employee personnel files and work history data.</li> <li>Information systems that must not be unavailable beyond 1 business day.</li> <li>Financial management information systems (e.g., payroll, payments, accounts receivables, over \$100,000).</li> </ul>	<ul style="list-style-type: none"> <li><b>Medium Sensitivity</b></li> <li><b>Personal*</b></li> </ul> <p>* 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".</p>
<p><b>LOW</b></p>	<p>Could reasonably be expected to cause limited or no injury to individuals or enterprises, including any combination of:</p> <p><u>Financial harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Limited financial loss</li> </ol> <p><u>Operational harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Limited impact on service levels</li> <li>Reduced staff effectiveness due to loss of morale</li> </ol> <p><u>Personal harm</u>, such as:</p> <ol style="list-style-type: none"> <li>Minor embarrassment or inconvenience</li> </ol>	<ul style="list-style-type: none"> <li>Pre-approved personal information for release.</li> <li>Information that is generally available to employees and approved non-employees (e.g., contractors, vendors, service providers, or consultants).</li> <li>Non-sensitive information, suitable to release.</li> <li>Ordinary meeting agendas and minutes.</li> <li>Communications to claims clerks.</li> <li>Job applicants' names.</li> <li>External press releases, media/public distribution.</li> <li>Operational procedures related to non-critical activities.</li> <li>Provincial budget after public release.</li> <li>Public accounts after publication.</li> <li>Public education materials.</li> <li>Information systems that can be down for up to 3 days.</li> <li>Financial transactions (e.g., under \$100,000).</li> <li>Information published by government, which requires integrity protection</li> </ul>	<ul style="list-style-type: none"> <li><b>Low Sensitivity</b></li> <li><b>Public</b></li> </ul>