BRITISH COLUMBIA | Ministry of Social Development and Social Innovation

ACKNOWLEDGEMENT OF MANAGEMENT RESPONSIBILITY FOR PROTECTION OF INFORMATION AND INFORMATION TECHNOLOGY AGREEMENT

The collection, use and disclosure of personal information collected on this form is subject to the provisions of the *Freedom of Information and Protection of Privacy Act.*

Management and personnel[1] have responsibility for the protection of information. This document sets out the core management responsibilities for acknowledgement by the Ministry Information Management Branch management team.

OBJECTIVE

To describe general and specific responsibilities for the IMB Management Team with respect to the securing of Ministry computer and information assets.

BACKGROUND

The Branch vision from the IMB Operating Plan, in part, is:

- To be modeling leading IM/IT best practices and leveraging solutions wherever possible
- To have information recognized and managed as a critical asset of the Ministry

Core Policy and Procedures Manual, Chapter 12:

Information management is a core component of government infrastructure; it is the intellectual capital of responsible governance. Information management policies and standards are disseminated across government to assist governance through the use of scarce resources as an integral part of efficient, accountable and cost-effective government business practice. Information technology is the full spectrum of technologies and services that support information management. … The principles underlying the effective management of information and technology are that:

1. *information is a vital government asset that must be managed, and, where appropriate shared to maximize investments;*
2. *information and technology are key components in delivering cost-effective government services to the public;*
3. *information and technology have the potential, when planned and managed properly, to improve productivity and reduce costs to government;*
4. *information and technology are strategic enablers of quality government service delivery;*
5. *the management and business principles applied to other government resources should be applied to information and technology resources;*
6. *the private sector is to play a major role in supplying services for the development and support of information technology.*

RESPONSIBILITIES

The general and specific responsibilities described here apply to program areas under the control of the management team. In addition, it is expected that the management team will support and participate in information protection and security programs as required for the Ministry.

The general responsibilities of management relative to information protection and Information security include:

- to **inform personnel** of their responsibilities, and to assist them to be responsible in their use of government resources;
- to **actively manage and monitor** government information usage, disposition and control;
- to actively manage and monitor government equipment usage and control;
- to **report on** suspected or actual **security breaches** or on conditions that are likely to result in a security breach;
- to **incorporate** security assessment and control activities **into operational processes.**

[1] The term “personnel” includes employees and other individuals (e.g., contractors, consultants, volunteers, third-party organizations).

ACKNOWLEDGEMENT OF MANAGEMENT RESPONSIBILITY FOR PROTECTION OF INFORMATION AND INFORMATION TECHNOLOGY AGREEMENT

Specific responsibilities of management for the protection of information include:

Things to do

- Be cognizant of the impacts of information breaches on public confidence and trust in government;
- Communicate information security responsibilities and practices to personnel:
  - appropriate and secure methods for media handling, storage, destruction and disposal of personal and sensitive government information;
  - reasonable security measures required to protect personal information under *The Freedom of Information and Protection of Privacy Act;*
- *Encourage and support personnel to adhere to and comply with information security policies;*
- *Ensure personnel receive information security information awareness, education, and training on an ongoing basis using mechanisms like the Employee Performance and Development Plans;*
- *Encourage security conscious work habits;*
- *Conduct or assist with periodic reviews and self assessments to ensure compliance with information security policies and procedures;*

Things to pay attention to

- Blatant disregard for legislation, policies, and procedures governing information protection;
- Environments where there is a high volume of personal and sensitive information available and accessible to staff;
  - ensure and verify that sufficient information protection measures are in place.

Things to establish procedures for

- Have controls in place to only assign authorized personnel with the appropriate level of access to government information and information systems.

Things to monitor

- Monitor for and examine irregularities surrounding the use and handling of government information.

Things to report

- Loss, theft or damage to any government device containing personal and sensitive information;
- Breaches of personal and sensitive government information.

Things to reinforce with staff

- Motivate and encourage personnel to adhere to information security policies;
- That whistleblowing is acceptable;
  - Policies are in place to protect those who report information breaches and violations;
- That personnel have a responsibility and duty to actively protect government information and information systems.

ACCOUNTABILITY AND GOVERNANCE

Specific targets and actions for improving, controlling or managing information protection should be documented in Employee Performance and Development Plans.

SIGNATURE OF ACCEPTANCE	
I have read, understand and accept my responsibilities to protect information under my care, control and authority.	
EMPLOYEE SIGNATURE	DATE (YYYY MMM DD)
PRINT NAME	POSITION TITLE