Ministry of Finance

Core Policy and Procedures Manual - Amendment Summary May 2011

Policy	
15.0 Security	15.2 Roles and Responsibilities - Revised to clarify the role of the Executive Director, Risk Management Branch as government's Chief Risk Officer. The amendment also identifies the roles and responsibilities of the new position of the Chief Security Officer, Government Security Office.

Thank you for visiting our web site.
If you have any comments or questions, please email us.

Ministry of Finance

Security

Table of Contents

15.1 Objectives

- develop and ensure an enterprise-wide security framework for all government operations
- establish an integrated and proactive security program within each ministry to identify security risks associated with any activity, function or process
- identify security measures for ministries to prevent loss or harm to people, information, information technology systems and physical assets
- provide program direction to evaluate, mitigate and monitor security risks that are a ministry threat
- establish security standards and guidelines based on an integrated assessment of potential loss, impacts, threats and vulnerabilities
- continuously promote government-wide security processes, best practices, training and awareness for employees

15.2 General

Security is a proactive process required to manage the Province's exposure to accidental losses, malicious threats or criminal acts. It is an integral part of the enterprise-wide risk management process to maintain continuous security of all government operations. Enterprise-wide security encompasses managers and staff co-operating to ensure:

- the safety and security of employees;
- the confidentiality, integrity, availability and value of information, information technology and physical assets; and
- the continued delivery of critical services by identifying, analyzing, evaluating, treating and monitoring significant security risks.

Good risk management practices provide the foundation for effective and efficient security in business operations and contracted services. The success of a security framework depends upon the integration, co-ordination, implementation and performance of each element of security outlined in government policy, and related Risk Management Branch (RMB) security standards and guidelines.

Roles and Responsibilities

Ministries, under the direction of deputy ministers, are responsible for initiating, developing and implementing ministry-wide security management programs.

Other agencies and organizations have direct responsibility for security within their respective corporate assignments.

Ministries and agencies, in conjunction with Risk Management Branch, are also responsible for identifying and implementing

appropriate security measures and controls to conditions that could cause a security risk to government operations and critical infrastructure.

The government Security Office is resident in the Risk Management Branch.

The Executive Director, Risk Management Branch (RMB), is the government's Chief Risk Officer responsible for the formulation and implementation of comprehensive risk management programs including security for the provincial public sector.

The Chief Security Officer, Government Security Office, is responsible for:

- overall management and coordination of the BC Government's Security Program;
- advising and assisting ministries in developing security strategies, security awareness, asset protection and technical assistance with investigations related to breaches of security;
- developing, maintaining and co-ordinating the government security policy, operational standards, guidelines and procedures;
- establishing and maintaining an inventory of security expertise and resources; and
- chairing the Government Security Advisory Committee.

The British Columbia Public Service Agency is responsible for providing policy direction, advice and assistance on matters that impact personnel, including personnel safety.

The Chief Information Officer (CIO) is responsible for providing strategic directions for information management/information technology (IM/IT) and electronic government service delivery and also for the development and maintenance of related corporate IM/IT policies, standards and architectures.

The Deputy Minister of Citizen's Services is responsible for protecting the confidentiality, integrity, availability and privacy of government's electronic information. The Deputy Minister works with all ministries to monitor, report and manage the risks to the security of government's IT infrastructure.

The Comptroller General is responsible for financial management policy, advice and guidance; internal audits that address major risk areas, including security; and determining compliance with the government security policy.

The Accommodation and Real Estate Services division is responsible for providing advice and assistance on security of physical facilities, design services, and the plant and equipment necessary to meet the security needs as identified by government policy, security threat and risk assessments, and from other approved sources.

15.3 Policy

1. Deputy ministers, senior managers and ministry security officers in each ministry collectively must manage security programs in their ministry, in accordance with RMB security standards and guidelines.
2. Each ministry must manage personnel security in conjunction with the Personnel Management Policy and occupational safety and health programs to provide a safe and secure workplace.
3. Each ministry must protect information holdings in all physical, electronic and digital formats commensurate with its value and sensitivity at all stages in the life cycle of the activity to preserve the confidentiality, integrity, availability, intended use and value of all records. Security categories approved by Risk Management Branch must be used.
4. Each ministry must implement this policy when receiving or sharing information and other assets with other governments (including federal, provincial, aboriginal, municipal or regional governments and foreign governments) and educational and private sector organizations.
5. Each ministry must ensure all components of electronic services, information systems and critical assets and infrastructures are protected commensurate with their value and sensitivity at all locations where government information is stored, processed and transmitted.
6. Ministries must identify and categorize information and other assets based on the degree of injury (low, medium, high) that could reasonably be expected to result from compromise to their availability or integrity, with reference to the provisions of the *Freedom of Information and Protection of Privacy Act* or other legislation.
7. Each ministry must establish the appropriate type and number of restricted zones to achieve the necessary conditions

for personnel safety, and for the protection of sensitive or valuable information and assets by implementing appropriate access controls for public, reception, operations and security zones.

8. For interministry activities and co-located ministries, one ministry must assume primary responsibility for security planning and management including negotiating security requirements, safeguards, terms and conditions with co-operating ministries and agencies.
9. Ministries are responsible for ensuring that security policy applies equally to contracted services when sensitive information and assets of the Province require safeguarding.
10. Each ministry must review security each time a real or imminent threat occurs or circumstances indicate a changed or new exposure and apply corrective measures to reduce the risk of future occurrence.
11. A General Incident or Loss Report for security incidents including the loss of public monies and assets must be submitted to Risk Management Branch within 24 hours (refer to Loss Reporting for requirements).
12. Each ministry must complete an annual security exposures review for personnel security, information security, information technology security and physical security.

15.4 Information and References

Risk Management Branch (RMB) supports the development and implementation of comprehensive risk management programs for the provincial public sector (including ministries, Crown corporations, government agencies and contracted service agencies).

RMB, through the Security Management Program (SMP), provides essential reference information for ministries that are developing a security management program. Operational standards, Security Guidelines, Security Definitions and supplemental materials are available at the RMB intranet address: http://gww.fin.gov.bc.ca/gws/pt/rmb/. This site is limited to users that have Government of British Columbia intranet access only.

All readers can obtain additional information through the RMB internet site: Risk Management Branch or by contacting RMB by telephone: 250 356-1794.

RMB addresses are:

Mailing Address:
PO BOX 9405 STN PROV GOVT
Victoria BC V8W9V1

Physical Address:
595 Pandora Street 3rd Floor
Victoria BC V8W 1N5