Ministry of Finance

Core Policy and Procedures Manual - Amendment Summary March 2011

Policy	
6.0 Procurement	6.0 Procurement - organization names updated throughout chapter for greater clarity 6.3.3 Contract Award – all procurement - new section added under Selection and Award - b. (1) Vendor Reference Check Review Policy (see TB Directive 4/11).The Directive provides policy for ministries to conduct internal reference checks on all core government service contracts with an estimated value of $10 Million or more (including the provision of an internal administrative review system enabling vendors to appeal a disqualification decision). To support ministries in the application of the Directive, CPPM Chapter 6 will also include Reference Check Review Guidelines that have been developed to provide clarity on the implementation of the government's vendor reference check requirements for government service contracts.
7.0 Revenue Management - Part I Revenue	7.2 General – increases ministry responsibilities for the control of public money to also ensure ongoing compliance with payment card industry (PCI) standards adopted by the provincial government. Expands Provincial Treasury functional authority and responsibilities to ensure government electronic payment systems comply with PCI standards. Detailed roles and responsibilities are provided in a PCI guide: Acceptance of Credit Card Payments: PCI Compliance Standards Roles & Responsibilities 7.3.8 Acceptance of Electronic Payments – new policy requirement for implementation of PCI standards for government electronic payment systems, and clarification of the Banking/Cash Management Branch's functional authority for the approval of systems and standards.
12.0 Information and Technology Management	12.3.5 Information Technology Standards – policy a) item 7 and 8 have been re-ordered, and item 9 added in order to provide the logical principles to ensure ministries and agencies leverage existing systems and processes, and that new systems with a payment application component will be compliant with PCI standards, government's processes and policies.
13.0 Financial Systems and Controls	13.3 Policy - 1. recognizes the need for consistency with PCI standards along with government information technology standards in methodologies for the development of new financial systems, or changes to financial systems, that have a customer facing payment service. Also, policy 10 expanded to recognize the roles and responsibilities of ministries and central agencies for public facing payment systems, and specifically electronic commerce systems. Policy 11 now requires ministries to ensure financial systems documentation is in sufficient detail to enable effective systems maintenance as well as compliance requirements.

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

Ministry of Finance

Procurement

Table of Contents

6.0 Procurement
Part I: Procurement
6.1 Objectives
6.2 General
6.3 Policy
6.3.1 Procurement Planning
6.3.2 Pre-Award and Solicitation
All Procurement
Goods
Services and Construction
Continuing Service Agreements
6.3.3 Contract Award – all procurement
Selection and Award
Responses
Pricing
Administration
6.3.4 Corporate Supply and Disposal Arrangements
Rentals and Leasing
Photocopying Equipment and Supplies
Repairs and Maintenance
Disposal of Surplus Assets
Crown Copyright
Disposal of Intellectual Property
6.3.5 Information Management and Information Technology Procurement
General
Unsolicited Proposals
6.3.6 Contract Administration and Monitoring
Receipt of Goods
Payment
Monitoring, Evaluation and Reporting
Deficient Performance Breach
Asset Management
Disputes
Part II: Vendor Complaint Review Process For Government Procurement
6.1 Objectives
6.2 General
6.2.1 Definitions
6.2.2 Scope of VCRP
6.2.3 Roles and Responsibilities
6.3 Policy

6.4 Information and References
6.4.1 Shared Services BC
6.4.2 BC Bid
6.4.3 Request for Proposals
6.4.4 Trade Agreements
6.4.5 Disclosure of Contract Information
6.4.6 Risk Management Branch

PART I: Procurement

6.1 Objectives

The following objectives for government procurement activity for goods, services and construction are based on the principles of fair and open public sector procurement: competition, demand aggregation, value for money, transparency and accountability.

- acquisitions are managed consistent with government policy and requirements of trade agreements
- government receives the best value for money spent on contracts
- vendors have fair access to information on procurement opportunities, processes and results
- acquisition and disposal opportunities are competed, wherever practical
- ministries and Shared Services BC (SSBC) only engage in a competitive process with the full intent to award a contract at the end of that process
- ministries and SSBC are accountable for the results of their procurement decisions and the appropriateness of the processes followed
- government buying power is leveraged through corporate supply arrangements (CSAs) and demand aggregation, wherever practical
- the cost of the procurement process, to both vendors and ministries, is appropriate in relation to the value and complexity of each procurement
- assets surplus to the needs of government are disposed of in a coordinated way to maximize the dollar return to government, and to minimize the risk to the environment

6.2 General

This policy applies to government contracts (i.e. agreements to procure goods, services and construction) and to contract expenditures chargeable to the Consolidated Revenue Fund (including special funds) and trust funds. This policy does not apply to statutory and formulae-driven contributions, such as government transfers (entitlements) to school boards, hospitals, universities and colleges that do not normally require a contract.

The Province is a party to the national Agreement on Internal Trade (AIT) and the British Columbia - Alberta Trade, Investment, and Labour Mobility Agreement (TILMA). Ministries must abide by the terms and conditions of the agreements when undertaking contracts.

Roles and Responsibilities

Ministries are responsible for:

- planning, managing and fully documenting the process to acquire goods, services and construction;
- using all existing CSAs for goods and services to meet program requirements;
- managing solicitation and contract award processes in a prudent and unbiased manner that fairly treats all potential vendors and bidders;
- ensuring that contracts for goods, services and construction are designed to provide the best value to government;

- ensuring that all ministry acquisitions and disposals are consistent with policy, applicable legislation and trade agreements;
- declaring goods surplus when their use to the ministry has ended; and
- ensuring compliance with this policy.

Shared Services (SSBC) is responsible for:

- identifying, planning, negotiating, establishing, managing and fully documenting corporate supply arrangements that will provide best value to the Province;
- managing and fully documenting the processes used to acquire goods, services and construction when requested to do so on behalf of a ministry;
- managing solicitation and contract award processes in a prudent and unbiased manner that fairly treats all potential vendors and bidders;
- ensuring that contracts for goods, services and construction are designed to provide the best value to government;
- ensuring that all SSBC acquisitions and disposals are consistent with policy, applicable legislation and trade agreements;
- disposing of all tangible and intangible assets that are surplus to government except as provided by ministry legislation, or Treasury Board directive(s);
- providing operational advice to ministries for procurement services within the scope of SSBC's activities;
- providing advice on all transactions involving Crown Copyright and Intellectual Property; and
- ensuring compliance with this policy.

The *Procurement Governance Office* is responsible for:

- developing and revising corporate procurement policy and providing official communications and interpretations of this procurement policy;
- monitoring and reporting for compliance with this procurement policy;
- establishing and managing policy for a formal government vendor complaints resolution process, including an internal escalating complaint resolution procedure in ministries and SSBC, and a last resort procedure in PGO;
- providing support and advice on corporate procurement policy, including development and management of a procurement training curriculum; and
- being the contact point for the negotiation, compliance and reporting requirements for the national Agreement on Internal Trade chapter 5 – Procurement and for procurement related matters in the British Columbia - Alberta Trade, Investment, and Labour Mobility Agreement.

The *Financial Management Branch* is responsible for developing and revising corporate contract administration and monitoring policy and providing official communications and interpretations of this policy.

The *Procurement Council* supports an effective and productive relationship between procurement governance, procurement service and clients for shared service procurement delivery, including promotion of best practices for government procurement and corporate resolution of procurement policy and service issues.

6.3 Policy

6.3.1 Procurement Planning

1. Procurement planning must be undertaken as part of the program/service planning process.
2. SSBC must identify opportunities for demand aggregation that provide overall savings to the Province. Ministries and the agencies within their authority must participate in CSAs established by SSBC, and advise SSBC of their procurement plans and requirements for common goods, services and construction in advance of program needs.

3. Ministries must review alternatives to acquiring new goods, services and construction such as considering repairs to existing assets and transfer of used assets.
4. Ministries must have the appropriate authority and funding to complete a procurement project prior to soliciting proposals, awarding a contract, or contracting for any goods, services, or construction.
5. For service contracts greater than $100,000, before taking any steps to find a contractor, a ministry must ensure that a cost / benefit justification exists for the contract, including, where appropriate, comparing the cost of contracting out with the cost of providing the service in-house if the resources were available. Contract outcomes must be defined; and the contract must be consistent with policy, applicable legislation, and trade and collective agreements.
6. Where a contract for the continuation of a service is to be awarded (that is not the result of exercising an option to renew) and the requirements have not changed from those provided under the initial contract, the ministry may rely upon the original cost / benefit justification if it is still relevant. If not, the ministry must update the original justification or provide a new justification.
7. A contract must not result in the contractor occupying an ongoing organizational position, or take the place of work normally conducted or acquired by a central agency. In addition, a contract must not result in the establishment of an employer/employee relationship. Every contractor engaged by the government must be independent and operating at arm's length from government.
8. Ministries and staff must not divulge any information that could impair the negotiating position of the government or that could benefit the competitive position of one contractor at the expense of another.
9. Where funding is provided to the contractor to acquire assets the contract must identify the assets and the funding provided for the purpose of acquiring the assets. The contract must also state who owns the assets that are provided to a contractor by a ministry; the assets created as a result of the contracted services; or the assets that are purchased by the contractor with funds provided by the ministry. The contract must also state who is responsible for the maintenance of the asset during the period of the contract and the disposition of the assets at the termination of the contract.
10. Ministries must not provide government assets to contractors, or fund a contractor's asset acquisition, where doing so could be viewed as a business subsidy or would create an employer/employee relationship.
11. Ministries and SSBC must not bestow a favour on, or grant preferential treatment to, any prospective contractor.
12. An employee who has received benefits under a voluntary exit program must repay all or a portion of the lump sum payment if remuneration is received from a contract with the government within the period beginning with the date of termination of employment and for the number of months equivalent to the amount of the benefits.
13. An employee who has received a severance payment on termination of employment must repay all or a portion of the lump sum payment if remuneration is received from a contract with the government within the severance settlement period.
14. Ministries and SSBC are encouraged to follow the Guidelines for Procurement of Environmentally Responsible Products and Services. These guidelines are available under the Procurement Procedures available on the SSBC website.

6.3.2 Pre-award and Solicitation

a. All Procurement
    1. Ministries must not use any procurement or solicitation instrument (e.g., RFP) to acquire goods or services that are currently available through a CSA. CSAs must be used where available. The following is an illustrative list of CSAs in government and the responsible organizations through which these commodities must be obtained.

Goods and Services	Responsible Office
Goods and services CSAs which are identified at the following website: http://www.pss.gov.bc.ca/csa/csa.html	Purchasing Services Branch, Shared Services BC, Ministry of Citizens' Services
Advertising and publications (excluding recruitment advertising) – all informational communications for the Province including Agencies of Record	Public Affairs Bureau, Ministry of Citizens' Services
Common IT Services	Purchasing Services Branch, Shared Services BC, Ministry of Citizens' Services
Employee household relocation services	BC Mail Plus, Shared Services BC, Ministry of Citizens'

	Services
Insurance and insurance related services	Risk Management Branch, Provincial Treasury, Ministry of Finance
Legal services	Legal Services Branch, Ministry of Attorney General
Mail processing and distribution services, which are identified at the following website: http://www.pss.gov.bc.ca/bcmp/	BC Mail Plus, Shared Services BC, Ministry of Citizens' Services
Mail Processing Equipment	BC Mail Plus,Shared Services BC, Ministry of Citizens' Services
Paper, office products, protocol giftware, and stationery products which are identified at the following website: http://www.pss.gov.bc.ca/dcv	Distribution Centre Victoria, Shared Services BC, Ministry of Citizens' Services
Uniforms, protective clothing and emergency preparedness products which are identified at the following website: http://www.pss.gov.bc.ca/pdc	Product Distribution Centre, Shared Services BC, Ministry of Citizens' Services
Polling services	Public Affairs Bureau, Ministry of Citizens' Services
Printing equipment and servicing	Queen's Printer, Shared Services BC, Ministry of Citizens' Services
Printing services which are identified at the following website: http://www.pss.gov.bc.ca/qp/	Queens' Printer, Shared Services BC, Ministry of Citizens' Services
Recruitment advertising – the BC Public Service Agency has assigned an Agency of Record for this service.	BC Public Service Agency
Real property and accommodation infrastructure services	Shared Services BC, Ministry of Citizens' Services
Records storage services	Corporate Records Management ,Information Access Operations, Shared Services BC, Ministry of Citizens' Services
Risk assessment and consulting	Risk Management Branch, Provincial Treasury, Ministry of Finance
Statistical services	BCStats, Ministry of Citizens' Services
Vehicle acquisitions, repair and maintenance	Purchasing Services Branch, Shared Services BC, Ministry of Citizens' Services

2. An employee must not participate in a contracting decision if the contract involves a direct relative, a person married to a direct relative, or a person sharing the same household as the employee. A direct relative means a spouse, parent, grandparent, grandchild, brother, sister, son, or daughter.
3. An employee who is exposed to an actual, perceived or potential conflict of interest in relation to an actual or proposed solicitation must disclose the matter to his or her supervisor and/or the contract manager. If, after review, it is determined that there is a conflict, the supervisor or contract manager must remove the employee from this particular contract situation. An employee who fails to disclose a conflict of interest can be subject to disciplinary action up to and including dismissal. Any suspected conflicts of interest must be investigated and resolved (09. Policy Statement - Standards of Conduct (Human Resources Policies).
4. Ministries may directly acquire goods and services when an unforeseen emergency exists. Emergency Purchase Orders (EPOs) must only be used to meet extraordinary deadlines that have pre-empted the ability to access the normal acquisition processes for goods and services (e.g., CSAs, SSBC's distribution centres, requisitioning). Ministries must limit the authority to issue EPOs to designated positions with appropriate signing authority. Where the appropriate ministry authority determines that it is essential to proceed, a written explanation of the need for an EPO must be kept on record.
5. Ministries must use the standard government formats for solicitation documents (e.g., ITT, RFP, RFQ, ITQ, RFSO) available from SSBC. Ministries must obtain the approval of SSBC and legal counsel for any changes to the standard formats. Only current versions of the solicitation documents may be used.
6. When subdivision of a major project into two or more component parts occurs, the Terms of Reference, Business Case and solicitation document for each component part must clearly disclose the potential combined scope of the project. Approval, by the expense authority, must be sought on the combined value of all contracts issued for a sub-divided project.
7. All standard competitive processes (i.e., ITT, RFP, ITQ, RFSO, RCSA) must provide identical information for potential bidders or proponents to the solicitation, to fairly and equally base their response. For Joint Solution Procurements, the amount of information and how it is provided to potential contractors differs depending on the phase of the process. See policy 6.3.2 c(3).

8. The permitted response time to a solicitation must be sufficient to allow all potential proponents to have a reasonable opportunity to compete, taking into account the time required to disseminate information, the complexity of the procurement, and the time required to prepare an appropriate response.
9. Objective selection criteria for the awarding of a contract must be established prior to inviting bids and proposals and must be consistent with those specified in the solicitation documents. Selection procedures and timelines must not limit anyone from competing.
10. Ministries and SSBC must be alert to the potential for bid rigging, and report any suspicious bidding patterns.
11. An expired contract must not be retroactively extended. When a contract expires and the original deliverables have not been fully met, a subsequent new contract may be considered in order to complete the work. The approval of the new contract should include consideration of the evaluation of the first contract (6.3.6 Contract Administration and Monitoring c.3).
12. Projects cannot be subdivided to avoid requirements of policy or trade agreements.
13. To establish a pre-qualified supplier list, a process must be undertaken which uses the standard Request for Qualification template, unless an alternate form is approved by SSBC and Legal Services. The process is to include an evaluation of the responses to the identified pre-qualification requirements to determine which respondents will be placed on the list of pre-qualified suppliers.
14. The method for selection of a contractor from the pre-qualification list must be specified in the RFQ document and this selection method must be followed.
15. As required in accordance with the provisions of the AIT and the BC - Alberta Trade, Investment, and Labour Mobility Agreement (TILMA), if the expected contract value is over the goods, services or construction threshold (see section 6.4.4), the contractor is to be selected through a competitive process between all suppliers on the pre-qualification list that meet the criteria for a specific project (e.g., specialization). The competitive process will evaluate each supplier's proposed approach, or pricing, or other elements required for the project.
16. Opportunities to be registered on a pre-qualification list must be provided either continuously or at regular intervals. The period for which a pre-qualification list will be valid must be specified in the RFQ document.
17. If the requirement for goods, services or construction falls within the provisions of the AIT or TILMA, the process to identify pre-qualified suppliers of goods, services and construction opportunities which may be over the associated threshold (see section 6.4.4) must be advertised annually on BC Bid.

b. Goods

1. Requests for goods valued over $5,000 that cannot be met through a pre-existing CSA must be directed to SSBC, except where SSBC and the ministry have negotiated a different arrangement which is included in the Service Level Agreement, or other agreements as required, between the Parties.

   The criteria used in the negotiation to determine the nature and degree of procurement services provided by SSBC for the ministry will include:

   - availability and level of procurement skills of ministry procurement specialists
   - uniqueness of ministry procurement and degree of specialized product and supplier knowledge of ministry procurement specialists
   - historical ministry compliance with the Core Policy and Procedures Manual
   - the degree of adverse impact on other SSBC clients
   - degree of risk of ministry vs SSBC undertaking procurement in relation to precedence and application of best practices
   - procurement process value-add by SSBC particularly on high risk or complex procurements
   - cost reduction generated from aggregation of demand and centralized procurement by SSBC
2. Where ministry requirements can be met by an existing CSA, goods must be purchased through that arrangement.
3. Unless a specific exemption is available under TILMA, or unless the conditions for direct awarding apply (see section 6.3.3. a), all acquisitions, supply arrangements, and processes to select pre-qualified bidders with an estimated value of $10,000 or more must be competed by advertising on BC Bid (see section 6.4.2). In addition,

opportunities may also be distributed to all vendors on a source list maintained for the specific goods, or they may be advertised in a national newspaper (Vancouver Sun).

4. Goods acquisitions with an estimated value less than $10,000 must be awarded using a competitive process that is appropriate to the value, complexity and profile of the business opportunity, unless the conditions for direct awarding apply (see section 6.3.3a). Opportunities can be posted on BC Bid, and/or an RFQ process can be followed, or at least three quotes must be obtained.
5. When a contract for goods valued at $10,000 or more is intended to be awarded on the basis that there is only one vendor that can provide the goods required, but this cannot be strictly proven as required in policy 6.3.3 a (1), a Notice of Intent must be posted on BC Bid.

   All objections received by the indicated response date must be reviewed and if any are substantiated a competitive process must be undertaken. If no objections are received, or the objections received are not substantiated, a direct award may be made.

   A Notice of Intent is not required if it is determined that the direct award meets one or more of the allowable exceptions specified in policy 6.3.3 a (1).

c. Services and Construction

1. Ministries are to determine, in negotiation with SSBC, the service and construction solicitations in which SSBC will be involved. These negotiated arrangements will be included in the Service Level Agreement, or other agreements as required, between the Parties.

   The criteria used in the negotiation to determine the nature and degree of procurement services provided by SSBC for the ministry will include:

   - availability and level of procurement skills of ministry procurement specialists
   - uniqueness of ministry procurement and degree of specialized product and supplier knowledge of ministry procurement specialists
   - historical ministry compliance with the Core Policy and Procedures Manual
   - the degree of adverse impact on other SSBC clients
   - degree of risk of ministry vs SSBC undertaking procurement in relation to precedence and application of best practices
   - procurement process value-add by SSBC particularly on high risk or complex procurements
   - cost reduction generated from aggregation of demand and centralized procurement by SSBC.
2. Ministries must utilize CSAs for services where they exist.
3. All services procurements using the Joint Solutions Procurement (JSP) acquisition method must be planned in conjunction with SSBC and the procurement process managed by SSBC.
4. Unless a specific exemption is available under TILMA, or unless the conditions for direct awarding apply (see section 6.3.3. a) any service opportunity, process to select pre-qualified bidders, or supply arrangement for the supply of services with an estimated value of $75,000 or more must be competed by advertising on BC Bid (see section 6.4.2). In addition, opportunities may also be distributed to all vendors on a source list maintained for the specific service, or they may be advertised in a national newspaper (Vancouver Sun).

   Unless a specific exemption is available under TILMA, or unless the conditions for direct awarding apply (see section 6.3.3.a), any opportunity or supply arrangement for construction with an estimated value of $100,000 or more must be competed by advertising on BC Bid (see section 6.4.2). In addition, opportunities may also be distributed to all vendors on a source list maintained for the specific type of construction, or they may be advertised in a national newspaper (Vancouver Sun).
5. Any service opportunity with an estimated value from $25,000 up to $75,000, or the establishment of a supply arrangement for the supply of services with an estimated value from $25,000 up to $75,000 must be awarded using a competitive process that is appropriate to the value, complexity and profile of the business opportunity unless the conditions for direct awarding apply (see section 6.3.3a). Opportunities can be posted on BC Bid or at least three quotes must be obtained.

Any construction opportunity with an estimated value from $25,000 up to $100,000, or the establishment of a supply arrangement for construction with an estimated value from $25,000 up to $100,000 must be awarded using a competitive process that is appropriate to the value, complexity and profile of the business opportunity unless the conditions for direct awarding apply (see section 6.3.3a). Opportunities can be posted on BC Bid or at least three quotes must be obtained.

6. Any service or construction opportunity, or supply arrangement for the supply of service or construction, with an estimated value of less than $25,000 should be competed to the extent reasonable and cost-effective.

7. When a contract for services or construction valued at $50,000 or more is intended to be awarded on the basis that there is only one vendor that can provide the services required, but this cannot be strictly proven as required in policy 6.3.3 a (1), a Notice of Intent must be posted on BC Bid.

   All objections received by the indicated response date must be reviewed and if any are substantiated a competitive process must be undertaken. If no objections are received, or the objections are not substantiated, a direct award may be made.

   A Notice of Intent is not required if it is determined that the direct award meets one or more of the allowable exceptions specified in policy 6.3.3 a (1).

d. Continuing Service Agreements

1. A contract in the form of a Continuing Agreement for a period of not less than three years may be made between a ministry(ies) and a contractor for the delivery of one or more of the following community health and social services:
   - Child, Family and Community Services
   - Child Care Services
   - Stopping the Violence Services
   - Community Support Services
   - Income Support Services
   - Community Justice Services
   - Correctional Services
   - Employability, Skills and Training Services
   - Mental Health Services
   - Continuing Care Services
   - Community Health Services
   - Alcohol and Drug Services
   - Multicultural/Immigration Services.
2. A contract in the form of a continuing agreement must be used where the ministry has determined that the following criteria have been met:
   - the services are to be rendered to a third party of behalf of the government;
   - service provider continuity is desirable and the services are to extend for three years or more; and
   - the services are applicable community health and social services.
3. To be eligible, contractors must meet government organizational standards for continuing agreements, must meet documented ministry performance and program standards, and must have an established relationship with the provincial government, i.e. the contractor has provided continuous community health and/or social service under a service contract for a minimum of three consecutive years immediately preceding the start date of the continuing agreement, and there are no unresolved compliance issues or concerns with any of the services provided by the contractor.
4. Contractors who are entering a continuing agreement for the first time must immediately meet the performance and program standards, but may negotiate a time period not to exceed one year from the commencement of the continuing agreement, in which they commit to a work plan with progress reports to demonstrate to the contract

manager that the contractor meets the organizational standards for continuing agreements.

5. Any new services, and all services not included in a component schedule of an existing continuing agreement, must be subject to a competitive selection process. Ministries may direct award where at least one of the following applies:
    - standard service contract direct award policy conditions apply (see section 6.3.3a);
    - service is developed jointly with a service provider in response to an identified need.
6. The competitive selection process must take into account: continuity of service; service provider availability; degree of community participation and investment; efficiency of operations; and effectiveness demonstrated by past performance.
7. Where the services to be obtained may be eligible for a continuing agreement, that information must be disclosed in the solicitation documents.
8. Once a contractor has been chosen to deliver a new service, ministries must determine the appropriate contract mechanism to define the relationship, (i.e., service contract or continuing agreement). Ministries must determine if the services to be delivered meet the criteria for a continuing agreement. If the services do not meet these criteria, ministries must follow the policies and guidelines for service contracts until such time as the criteria for a continuing agreement are met.
9. Where component services currently provided under existing continuing agreements are modified and/or expanded, ministries must first consult with current qualified contractor(s) to determine whether these existing continuing agreements can accommodate the modification and/or expansion. The scope of consultation may be limited where service requirements specify geographic location.
10. Where modification and/or expansion of component services cannot be accommodated under existing continuing agreements, the services must be subject to the competitive selection process. Where more than one existing continuing agreement holder can accommodate the expanded or modified services, ministries must conduct a solicitation process.
11. The conditions for negotiation and direct award for modified and/or expanded services without a competitive process are the same as the conditions for direct award of new continuing services agreements listed in #5 above.
12. Except as described above for modifications or expansions, services provided under a continuing agreement are not subject to a competitive selection process for the duration of that continuing agreement.
13. Where the services are to be delivered on behalf of more than one ministry, a representative of each ministry must sign the contract.
14. A ministry must agree in an annual funding letter to make payments of a negotiated amount to the contractor. The letter must also specify the outputs, and where feasible, the outcomes. Where more than one service is to be delivered by a contractor, the funding letter must specify the annual funding amounts and outputs and/or outcomes for each service. The funding letter may be amended during the year to modify the outputs/outcomes, or to change payments for new or emerging services, by mutual agreement of the ministry and the contractor.
15. Appropriate measures for success and evaluation methods (best practices) must be established jointly by the contract manager and the contractor. Contractors' performance relating to outcomes of contracted services must be evaluated at least once every three years.
16. Every continuing agreement must contain a provision that allows the agreement and/or a component schedule of the agreement, to be terminated by the minister(s) with cause at any time without notice. Every continuing agreement must contain a provision that the agreement or a component schedule of the agreement may be terminated by either party without cause on notice not exceeding one year.
17. Ministries must establish their own guidelines and procedures to set appropriate time periods, by program, for notice of termination consistent with this continuing agreements policy, and the guidelines and procedures established by other ministries receiving similar services in the community health and social services sector.

6.3.3 Contract Award – all procurement

a. Direct Awards

1. Contracts for acquisitions (of goods, services, and construction) and disposals may be negotiated and directly

awarded without competitive process where one of the following exceptional conditions applies:

- the contract is with another government organization;
- the ministry can strictly prove that only one contractor is qualified, or is available, to provide the goods, services or construction or is capable of engaging in a disposal opportunity;
- an unforeseeable emergency exists and the goods, services or construction could not be obtained in time by means of a competitive process;
- a competitive process would interfere with a ministry's ability to maintain security or order or to protect human, animal or plant life or health; or
- the acquisition is of a confidential or privileged nature and disclosure through an open bidding process could reasonably be expected to compromise government confidentiality, cause economic disruption or be contrary to the public interest.

The contract manager is responsible for documenting, in the contract file, the rationale, or the circumstances, that supports the use of one or more of the above exceptions. This documentation must be appended to the contract file and be available when requested.

2. The direct award of a Transfer Under Agreement must meet a direct award condition of 6.3.3 a (1), or be:

- financial assistance provided to a specified target group or population (e.g., a First Nation, or a direct beneficiary- individual or family or legal guardian of that individual under a community/social service program); or
- a shared cost agreement or a public private partnership where a competitive selection is not appropriate.

b. Selection and Award

1. Ministries must award contracts on the basis of the criteria set forth in the solicitation documents.

2. The rationale for the ranking of all proponents must be documented.

3. Ministry staff must participate in the evaluation process to select the successful contractor(s).

4. Before considering a bid or proposal, ministries must ensure that it meets all mandatory requirements specified in the solicitation documents.

5. In the case of ITTs and ITQs, contracts must be awarded to the lowest-priced qualified bidder meeting the terms and conditions of the solicitation document.

6. In the case of an RFP, the contract must be awarded to the proponent whose proposal meets all mandatory proposal requirements, and achieves the highest overall rating of all evaluation criteria specified in the solicitation documents.

7. In all situations where an alternate evaluation methodology is required (e.g., dual track negotiation, best and final offer), a full description of the methodology must be provided in the solicitation document and the process as stated must be followed to determine the successful proponent.

8. Ministry staff must not do or say anything to create a verbal contract on behalf of the government.

9. Multi-year contracts are permitted when the stability of the longer time frame supports better value to government. However, they must not be established through ongoing amendments and extensions of standard term contracts, unless the extensions were planned and included as part of a competitive process.

10. Ministries and SSBC, where practical and depending on the size of the contract, must undertake measures to conduct appropriate due diligence on prospective contractors such as, but not limited to: credit and background

checks; business reference checks; and identification of shareholders, directors and officers of the company.

b. (1) Vendor Reference Check Review Policy (see TB Directive 4/11)

1. For a procurement of services under a contract with an estimated value of $10 million or greater, ministries must include a pre-qualification process with an internal performance reference check component. The internal performance reference check must review a vendor's performance on all contracts with a value of $1 million or greater that the vendor currently has or has had with the Province in the three years prior to the closing date of the pre-qualification process.
2. The Qualifications Review Committee that assesses vendors under the pre-qualification process may disqualify a vendor from proceeding to the next stage in the procurement process for failing the internal performance reference check; vendors disqualified for failing the internal performance reference check may request in writing to the Qualifications Review Committee a review by the Office of the Comptroller General of their disqualification.
3. It is the responsibility of the Executive Financial Officer (EFO) (or delegate) for each ministry to:
    a. oversee the performance management process for the ministry, for all contracts with a value of $1 million or greater,
    b. oversee the design and use of a standardized internal performance reference check template to be used in ministry pre-qualification processes and a post-contract evaluation template to be used to provide a record of performance by ministry contractors as part of the ministry performance management process, and
    c. ensure sufficient document retention to support internal performance reference checks by other ministries engaged in pre-qualification processes.

See Reference Check Review Guidelines for implementation of the Vendor Reference Check Review Policy.

c. Responses

1. A written confirmation must be sent to the contractor who was successful on a solicitation. Unsuccessful respondents to a RFP must be notified and offered the opportunity for a debriefing on their proposal. Unsuccessful bidders on an ITQ must be notified of the winning bidder through a listing on BC Bid or other means.

d. Pricing

1. Every contract must have a firm contract ceiling price (exclusive of HST). Where a firm contract ceiling price is not possible, a unit price must be predetermined, and the ministry must have control over the number of units of service that are delivered within each phase of the contract.
2. Fixed price contracts are permitted for service contracts, if the scope of the work can be clearly defined in advance.

e. Administration

1. Ministries must maintain adequate contract documentation for all phases of the procurement process, including planning, solicitation, award, management, amendments, schedules of payment, progress reports and contract evaluations.
2. Contracts must be in writing and signed and delivered by all parties prior to the commencement of the work or service (or, in the case of an emergency, as soon as possible thereafter).
3. Contracts must be made in the contractor's legal name. Each contract must be approved and signed by the appropriate authority. In no circumstances should an unauthorized employee or agent legally bind the Province with apparent authority.
4. Subject to policies 5 and 7 below, one of the three approved Service Agreement templates should be used for service contracts in all instances *except* the following:

    - any contract with a value greater than $250,000, unless use of the template for the contract has been approved by the ministry's legal counsel;
    - contracts for office assistance services or with employment agencies where a CSA exists;
    - vehicle and equipment rentals;

- contracts for third party service delivery (e.g., Transfers under Agreement);
- capital construction projects;
- goods acquisitions unless ancillary to services under the contract and advice has been obtained from the ministry's legal counsel about additional provisions that may be appropriate; or
- software licensing.

No changes should be made to these approved Service Agreement templates that have not been prepared, or advised on, by the ministry's legal counsel.

5. If none of the approved Service Agreement templates is appropriate for a particular transaction or type of transaction, a ministry may develop an alternative contract template provided the template is prepared by, or with advice from, the ministry's legal counsel. If an alternative contract template contains an indemnity of the contractor by the Province, the indemnity must be approved by an authorized official in the Risk Management Branch, Ministry of Finance or otherwise in accordance with the Guarantees and Indemnities Regulation prior to the template being used.
6. Ministries must not use letters of agreement to enter into a contract without seeking advice from legal counsel.
7. Some contractors prefer to use their own standard contract forms. If not precluded by the terms of any applicable competitive process documents, ministries may accept the use of such forms, but the forms must meet government requirements and must first be reviewed by their legal counsel. Where a contractor's form contains an indemnity of the contractor, the indemnity must be approved by an authorized official in the Risk Management Branch, Ministry of Finance or otherwise in accordance with the Guarantees and Indemnities Regulation prior to a ministry entering into a contract using that form.
8. Supply arrangements are competed in the same manner as an individual contract. Where a supply arrangement may give rise to a contract that would require central agency approval because of its amount or nature, the ministry must request approval of the supply arrangement.
9. Whenever a contract is to be modified, the standard form of modification agreement must be used unless legal counsel has approved an alternative modification process or form.

   The justification for all modification agreements must be documented on the contract file.

   Modifications to a contract must be in writing, and signed by both parties.

   A modification agreement to extend the term of the agreement for a reasonable period of time is allowable when an unforeseen event has delayed the delivery of specific contract outputs.

   A modification agreement must not be used to substantially change the nature and intent of the original contract.

   Expense authority approval, when applied, must reflect the total dollar value of the contract and not just the dollar value of the modification agreement.

10. Annual or multi-year contract renewals are only allowed when the potential for renewal has been explicitly included in the solicitation documents, including the establishment of a limit on the number of renewals.
11. Ministries must ensure that the contractor's agent or broker completes and signs the Province of British Columbia Certificate of Insurance (FIN 173 MS Word), in compliance with the insurance requirements of the contract.
12. A Privacy Protection Schedule (PPS) must be completed and attached as a schedule to any contract between the government and a contractor that involves "personal information" as defined in the *Freedom of Information and Protection of Privacy Act* unless it is not intended that the public body will own or control the personal information.

    A PPS must be in the form set out at http://www.cio.gov.bc.ca/cio/priv_leg/foippa/contracting/ppsindex.page unless an alternative version has been authorized by Knowledge and Information Services, Office of the Chief Information Officer, Ministry of Citizens' Services.

Ministries and staff must not divulge information regarding a contract unless it is available to the general public or the disclosure has been authorized by the Ministry Executive based on prior consultation with their Manager, Access and Records Service Delivery and/or Legal Services.

6.3.4 Corporate Supply and Disposal Arrangements

a. Rentals and Leasing

1. Ministries may use Purchasing Cards to rent or lease goods where the total cost does not exceed $5,000. Renewals are not permitted and ministries must obtain a receipt from the lessor for the return of a leased item when the lease expires. Exceptions include vehicle rentals for operational purposes exceeding 30 days and vehicle rentals while an employee is on travel status.
2. Ministries must requisition leases, including potential capital leases, through SSBC and provide justification for leasing in lieu of purchase.

b. Photocopying Equipment and Supplies

1. Ministries must access the SSBC photocopier equipment and supplies CSA for requirements up to the limits specified therein.
2. Photocopier paper must be ordered from SSBC.
3. Government photocopy equipment is to be used for government business only. Personal use of government photocopier equipment is prohibited.

c. Repairs and Maintenance

1. Service contract requests for repairable assets must be submitted to SSBC.

d. Disposal of Surplus Assets

1. Where an opportunity exists to replace an outdated asset with a similar asset, details of the potential trade-in must be forwarded to SSBC, which will conduct an analysis of the potential trade-in to determine the best overall value to government. Ministries must only negotiate trade-in arrangements after consultation with SSBC.
2. Assets that are surplus to the needs of the government are to be disposed of at fair market value by SSBC who will determine the appropriate method for disposal of such assets.
3. Where assets are to be disposed of by a ministry under specific legislative authority or under a Treasury Board Order or Directive, SSBC must be notified prior to initiating the disposal in order to ensure there are no issues that may arise from the disposal in relation to other pre-existing disposal agreements.
4. The disposal of a medium with information capacity must be done in a manner to protect the privacy and security of the stored information in accordance with information and records disposal policy (see 8.3.2 policy 6).

e. Crown Copyright

1. All government employees must perform their duties in compliance with the *Copyright Act*. It is the responsibility of deputy ministers to ensure that their employees are aware of the provisions of the *Copyright Act*, which pertain to making copies of Works (whether in paper or electronic format). A notice provided by the Intellectual Property Program must be prominently affixed on or near all government-operated photocopiers. The Intellectual Property Program is responsible for providing information to ministries regarding the Crown copyright policies, including the provisions of the *Copyright Act*.
2. Crown Copyright of any Work means it belongs to the Province and not to individual ministries or any other government agencies. Unless there is a written agreement to the contrary, including terms of a collective agreement, the copyright for any Work that has been prepared or published by the Province's employees in the course of their employment belongs to the Province.
3. The right to reproduce Work may only be granted to a third party under the authority of:

   - the Intellectual Property Program operating under the *Procurement Services Act*, section 2(1)(f);
   - specific legislation granting such authority; or
   - Treasury Board directive under authority of the *Financial Administration Act*, section 46, Public Property.

4. If a Third party wishes to reproduce a Work or a portion of a Work for non-commercial purposes, the Third Party must send a completed Copyright Permission Request Form to the Intellectual Property Program. Subject to policy 7 below, the Intellectual Property Program will administer the request.
5. If a Third Party wishes to reproduce a Work or a portion of a Work for commercial purposes, the Third Party must contact the Intellectual Property Program to obtain a license agreement. Subject to policy 7 below, the Intellectual Property Program is responsible for license negotiations on behalf of the Province. A fee and/or royalty will be charged unless waived at the Province's discretion.
6. The Province will refuse permission to reproduce a Work or a portion of a Work if that reproduction:

    - is not in the financial or public interest of the Province;
    - does not comply with the policies of the Intellectual Property Program;
    - is not consistent with the *Freedom of Information and Protection of Privacy Act* or any other applicable legislation; or
    - is not approved by the Intellectual Property Program Committee.

7. The Province will require a Third Party to withdraw or cease reproducing a Work if that reproduction:

    - purports to be the official version and is not;
    - is inaccurate;
    - is considered to be misleading for any other reason, (e.g., out of date material presented as current); or
    - is for commercial purposes and is being done without a license agreement with the Province.

8. If a ministry obtains authority from Treasury Board, under the authority of section 46 of the *Financial Administration Act*, to grant a license to a Third Party to reproduce a Work or a portion of a work, or to assign the copyright in a Work to a Third Party, the ministry must comply with the policies of the Intellectual Property Program.
9. If a ministry does not have the authority outlined in policy 7, any request from a Third Party to reproduce a Work for Commercial Purposes or for the sale of the Province's copyright in a Work must be forwarded to the Intellectual Property Program with details outlining the Work affected, intended use, method of distribution, target date for release, and contact person.
10. Unless a ministry's legal counsel approves an exception, a ministry must ensure that each Standard Service Contract includes specific wording ensuring that copyright in any material produced under contract belongs exclusively to the Province. The wording must also require the contractor to deliver, upon request of the ministry, documents waiving any moral rights of the contractor, contractor's employees and subcontractors over the material, and confirming the vesting of the copyright in the Province.

f. Disposal of Intellectual Property

1. Disposals of intellectual property involve the sale, transfer or licensing of these rights to third parties. Such disposals can only take place under the following authorities:

    - the Intellectual Property Program operating under the *Procurement Services Act*, section 2(1)(f);
    - legislation applicable to a specific ministry; or
    - Treasury Board directive(s) under the *Financial Administration Act*, section 46.

2. Where intellectual property is to be disposed of by a ministry under specific legislative authority or under a Treasury Board Order or Directive, SSBC must be notified prior to initiating the disposal in order to ensure there are no issues that may arise from the disposal in relation to other pre-existing intellectual property licensing agreements.
3. The Province's intellectual property must be protected during its development and life span, and when providing access to or releasing the intellectual property to third parties.
4. Ministries must not allow materials to be copied or used for commercial purposes by third parties, except under a license agreement executed by SSBC, or by a ministry with the specific legal authority to dispose of the intellectual property at hand.

5. Materials must be developed solely to meet the program needs of government, rather than to create marketable products.
6. Providing access to information under the *Freedom of Information and Protection of Privacy Act* does not include the transfer of intellectual property, such as the rights to copy and redistribute for commercial purposes.
7. Where a disposal of intellectual property includes information or data, the licensee must be obligated to comply with the *Freedom of Information and Protection of Privacy Act*.
8. If a ministry is contacted by a Third Party that is interested in acquiring any intellectual property, or a ministry becomes aware it has intellectual property that has commercial value, it must notify the Intellectual Property Program to evaluate the potential disposal opportunity.
9. Where the disposal of intellectual property is a sale, transfer or a license that provides exclusive rights, the disposal must be done through a competitive bidding process.
10. Revenue from disposal of intellectual property will be paid into the SSBC $1000 Vote. Annually, Treasury Board Staff will add, as approved by Treasury Board in the Estimates, the ministry share of revenue received in the given fiscal year to that ministry's base budget for the following fiscal year.

6.3.5 Information Management and Information Technology (IM/IT) Procurement

For detailed information on the Chief Information Office's IM/IT policies and standards, refer to the Office of the Chief Information Officer.

a. General

1. Previous approval requirements are superseded by Treasury Board Directive 5/04 (February 4, 2004).
2. All IM/IT goods and services must be procured in accordance with the business requirements of the ministry as identified in the Ministry Service Plan.
3. Prior to initiating procurement of all IM/IT-related products or services, ministries must discuss their IT requirements with SSBC and their IM requirements with the Chief Information Office (CIO), which will determine whether a corporate solution will be implemented for the requirement.
4. Large projects frequently include smaller IM/IT-related component projects. These component projects must be considered at the same time as the larger project.
5. All IM/IT goods and services must be procured in accordance with government financial and procurement policies, including the Core Policy and Procedures Manual, and must be consistent with the ministry Information Resource Management Plan, the Agreement on Internal Trade, and the Chief Information Office (CIO) policies, strategies and standards, and all legislative requirements.
6. All ministry IM/IT hardware and software requirements, including shared devices (e.g., desktop, laptop, server, and printer devices) must be ordered through SSBC. Where available, CSAs, pre-established by SSBC, will be utilized for the supply of these items. Any exceptions to this policy must be approved by CIO, or SSBC, as appropriate. This policy applies to purchases of any volume or dollar value.
7. If 51% or greater of the estimated value of a contract is for hardware and/or software and the value of this contract is $10,000 or more, the opportunity must be advertised on BC Bid (see section 6.4.2).
8. If the estimated value of a service contract is $75,000 or more, the purchase must be advertised on BC Bid unless a specific exemption is available under TILMA, or unless the conditions for direct awarding apply (see section 6.3.3.a) any service opportunity, process to select pre-qualified bidders, or standing offer for the supply of services with an estimated value of $75,000 or more must be advertised on BC Bid.
9. Except where SSBC and the ministry have negotiated different threshold values which are included in the Service Level Agreement, or other agreements as required, between the parties, all solicitations for IM/IT projects valued between $100,000 and $500,000 must be reviewed by SSBC prior to proceeding with the acquisition and all IM/IT projects valued over $500,000, and all procurements utilizing the Joint Solutions Procurement (JSP) acquisition method, must be planned in conjunction with SSBC and the procurement process managed by SSBC.
10. Government Purchasing Card: standard regulations for the use of this card apply to all IM/IT-related purchases.
11. BC Business Opportunities: Ministries must identify opportunities for regional-based IM/IT service providers, and

ensure that alliances with large firms provide opportunities for smaller BC companies, subject to the provisions of the Agreement on Internal Trade and the British Columbia - Alberta Trade, Investment, and Labour Mobility Agreement.

b. Unsolicited Proposals

1. In this section, an "unsolicited proposal" is defined as a supplier-initiated offering of Information Management or Information Technology (IM/IT) goods, services, or solutions to government. The aim of such a proposal is to enable an IM/IT supplier to establish a sales contract or business alliance partnership with government that is neither the result of a competitive solicitation nor the result of a ministry-initiated direct award.
2. Ministries can receive unsolicited proposals from the private sector. If the ministry determines that the proposal warrants consideration, then the proposal must be submitted to the Unsolicited Proposals Review Panel.
3. The proposal must demonstrate that:
    - it is unique; and
    - it addresses the current or future needs of government; and
    - the goods or services are not otherwise available in the marketplace.
4. Unsolicited proposals, received in the proper format, must be reviewed by the Unsolicited Proposals Review Panel. The Panel will be chaired by the Procurement Governance Office (PGO) and comprised of members drawn from:
    - Shared Services BC (SSBC);
    - the interested ministry(ies);
    - Treasury Board Staff;
    - the Chief Information Office (CIO);
    - the Procurement Governance Office (PGO); and
    - optionally at the discretion of the PGO, disinterested third-party(ies).
5. Panel members will be selected by the Chair based on the nature of the proposals requiring review.
6. The Panel must ensure that the unsolicited proposal meets the criteria as stated in policy 3 above before contract negotiations commence.
7. Ministries must not enter into contract negotiations before the Panel review is complete. If there is any doubt that an otherwise acceptable proposal is unique, SSBC shall issue a Notice of Intent prior to the ministry entering contract negotiations.
8. Any proposal not meeting the criteria under policy 3 above will be rejected. If the proposal is accepted and approved by the Panel, the ministry may enter into contract negotiations, subject to funding availability and any required Treasury Board approvals.
9. Notwithstanding the reference to Notices of Intent under policy 7 above in this section, all contracts resulting from unsolicited proposals must be subject to the Procurement chapter of the Core Policy and Procedures Manual, including policies related to direct awards.
10. Funding for contracts resulting from unsolicited proposals must be drawn from within the existing appropriation of the contracting ministry.
11. Ministries must not use the unsolicited proposals process to bypass the competitive tendering process for goods or services requirements that are initially identified by the ministry.
12. In the event that the Panel approves an unsolicited proposal, ministries must ensure that all contracts resulting from unsolicited proposals with a value of $10,000 or over for goods and $75,000 or over for services comply with the British Columbia - Alberta Trade, Investment, and Labour Mobility Agreement, Part V, Government Procurement, paragraph 2, and that they comply with the requirements of the Agreement on Internal Trade Article 511.3, annual reporting on procurement excluded under Article 506(12).

6.3.6 Contract Administration and Monitoring

a. Receipt of Goods

1. Ministries must ensure that adequate receiving processes are in place to confirm that goods are received as ordered (i.e., correct quantity and suitable quality).
2. Ministry employees, before signing for the receipt of goods, must inspect the shipment for damage and/or missing or incorrect items. Goods received must match the shipment's documentation.
3. Discrepancies between goods received and goods ordered must be reported immediately to the supplier. If the supplier does not take appropriate corrective action, SSBC should be contacted for assistance.
4. Ministries must not accept product substitutions by suppliers without prior SSBC approval. Purchase Order Amendments are required to cover any substantial changes to the original purchase order.
5. Ministries must maintain adequate receipt records or other documentation to support account verification and payment.

b. Payment

1. A contract summary record must be maintained for all service contracts, either by using a contract summary sheet, or equivalent electronic record.
2. A contract cannot include a cost overrun clause. If a cost overrun is unavoidable, ensure the costs are justified. Any overrun is to be authorized in advance using a modification agreement form. There may be additional approval requirements triggered by cost overruns.
3. Fees, Expenses, Maximum Amount, Statements of Account, and Payments Due, must be contained in Schedule B to contracts. This applies whether the contract is established on the basis of Daily Rate, Hourly Rate, Rate per Unit/Deliverable or Flat Rate. (For contractor travel, refer to Travel, Contractors.)
4. All contract quotations must exclude the HST. Statements of accounts must include a calculation of fees (plus applicable taxes, such as HST) and expenses.
5. Ministries must ensure that payments made to contractors who are non-residents of Canada comply with the withholding tax provisions of the federal *Income Tax Act*.
6. Payments made in advance must be specifically provided for in the contract or in accordance with a formal modification agreement. The contract or modification agreement must specify how the advances are:
    - to be deemed to be earned; or
    - if the services are not subsequently rendered, to be repaid; and
    - what interest rate, if any, must apply.

    Procedure Requirements - D.3

c. Monitoring, Evaluation and Reporting

1. For every contract, ministries must clearly establish the outputs and outcomes required, together with their quality and quantity, against which the performance of the contractor can be monitored throughout the duration of the contract. These output and outcome requirements must be included in the contract.
2. Ministries must ensure timely and consistent monitoring of the contractor's performance as the assignment progresses in accordance with the terms and conditions of the contract.
3. A post-completion evaluation is required on every contract over $50,000 to provide a record of the contractor's performance and to assist in future contracting activity.
4. Under the Agreement on Internal Trade, provinces are required to calculate the number and aggregate value of procurements over and under the applicable thresholds, and report on them annually. In addition, the Provinces must report on any contracts established by utilizing the allowable exemptions or exclusions from the AIT. Therefore, ministries must ensure that methods are in place for collecting this information. Ministries should report the information for the previous fiscal year to the Procurement Governance Office by the date specified in the report call letter issued each year. AIT Article 511 contains further details on these information and reporting requirements.

d. Deficient Performance and Breach

1. Where a contractor deviates from the terms and conditions of a contract, the contract manager must immediately take one or more of the following steps:

i. Step 1 – Notify the contractor in writing of the deficiency and arrange to discuss the problem. A record should be kept of such discussions. The discussions could result in an agreement to amend the terms of the contract.

ii. Step 2 – Issue a notice to comply if the contractor persists in deviating from the terms and conditions of the contract.

iii. Step 3 – Issue a stop work order if the contractor ignores the notice to comply.

iv. Step 4 – Terminate the contract, subject to the advice of the ministry's contract specialist and/or legal counsel.

2. Where the breach or deficiency puts public safety at risk, the ministry must proceed immediately to Step 2 and issue a notice to comply, or to Step 4 and terminate the contract.

3. If fraud is suspected, refer to Loss Management, CPPM 20.2.2.

e. Asset Management

1. Ministries must identify and manage any asset maintenance, risk and liability issues arising from their contracting activities.

2. Where assets are determined to be owned by the Province, they must be appropriately safeguarded, controlled and accounted for. Assets being replaced due to being damaged, lost or stolen must be reported on the General Incident or Loss Report (government access only). See CPPM M, Loss Reporting.

3. Ministries must not fund a contractor's amortization as part of a contractor's administration costs for the contractor's assets acquired with government funding.

f. Disputes

1. Any dispute arising out of a government contract must be dealt with in a just, prompt and cost-effective manner. All contracts must contain a clause that identifies how a dispute will be resolved. Any dispute arising out of a government contract must ultimately be resolved according to the terms of the contract.

2. For contracts that are subject to the AIT, ministries must settle any AIT-related disputes in accordance with the dispute resolution process provided in AIT Article 513. Ministries will be responsible for the Province's share of the cost of any dispute panel that is established to investigate the dispute.

PART II: Vendor Complaint Review Process for Government Procurement

6.1 Objectives

The objectives of this policy are to define a vendor complaint review process (VCRP) that is accessible, consistent, fair, impartial and timely, and to identify ways to make improvements in the manner in which procurement is undertaken by government.

6.2 General

The VCRP is designed to ensure that there is a process for the review of vendor complaints about a government procurement process. The intent of the VCRP is to assist government in identifying and responding to problems in the establishment and application of government procurement policy and procedures.

This VCRP requires that ministries, SSBC and vendors provide full access to all information pertinent to complaints. All information under this VCRP is subject to the *Document Disposal Act* and the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*.

6.2.1 Definitions

PGO means the Procurement Governance Office, Office of the Comptroller General, Ministry of Finance.

SSBC means Shared Services BC, Solutions BC, Ministry of Citizen's Services (see section 6.4.1).

Procurement means those processes, including direct awards, related to the purchase of goods, services and construction.

Complaint means a written objection submitted by a complainant regarding a competition, direct award, contract award, or proposed contract award for goods, services, or construction.

A complaint may be made with respect to the process used to evaluate proposals and how the evaluation criteria were applied, but may not include issues pertaining to individual point ratings given by an evaluation committee to specific evaluation criteria.

Complainant

1. For the purpose of a vendor complaint relating to a competition or direct award, means an actual or prospective bidder or proponent whose business interest would be affected by the award of a contract, or by the failure to award a contract.

2. For the purpose of submitting a vendor complaint relating to a contract award, means a proponent who actually submitted a proposal in response to the competition for the contract.

6.2.2 Scope of VCRP

- The application of this VCRP is limited to ministries and direct government entities (i.e. excludes municipalities, academic institutions, school boards, health and social service authorities, and Crown corporations) whose procurement is subject to government procurement policy as described in Chapter 6 of this Core Policy and Procedures Manual. It does not apply to procurement undertaken by SSBC for a public sector entity that is outside of direct government.
- This VCRP is limited to issues of procurement policy and procedures. This VCRP is not available for issues related to vendor or ministry/SSBC performance or conduct during a contract. These issues are to be dealt with through the dispute resolution processes identified in the contract document.
- This VCRP does not limit or impair the rights of any vendor to seek a review through the Ombudsperson's Office, or to seek remedies of law through the judicial or other process.

6.2.3 Roles and Responsibilities

Ministries/SSBC Responsibilities:

- Establishing and managing an accessible and fair process for responding to vendor complaints related to procurement activities undertaken by ministries or SSBC.
- In the case of those complaints submitted to the PGO, providing all pertinent and required information.
- Recording information on all vendor complaints managed under their vendor complaint review process, and providing reports to the PGO as required.
- Implementing changes required to ministry/SSBC procurement processes identified through their complaint review process.
- Implementing any outcomes recommended by the PGO, and any subsequent remedial action.
- Making all reasonable efforts to review complaints.

PGO Responsibilities:

- Ensuring that ministries and SSBC have a vendor complaint review process as described in these policies and procedures.
- Managing a last resort process for complaints not satisfactorily concluded through the ministry/SSBC vendor complaint review process.
- Providing guidelines regarding the information and reporting requirements for ministries and SSBC.
- Monitoring and reporting on government-wide VCRP activity and outcomes of complaint reviews.

- Implementing changes required to government procurement policies and procedures, and to procurement training methods and tools identified through the complaint review process.

Vendor Responsibilities:

- Making reasonable efforts to review the complaint with the ministry or SSBC by contacting the entity and following their complaint review process.
- Providing all pertinent and required information related to a complaint.

6.3 Policy

1. The ministries and SSBC have primary responsibility for reviewing vendor complaints regarding their procurement processes. They must establish and administer a process for reviewing, recording, managing and reporting vendor complaints, and must make the process known to vendors by posting it on a readily accessible ministry/SSBC web site which is linked to the PGO web site.
2. The PGO must establish and administer a process that deals with complaints that have not been satisfactorily concluded by the ministry or SSBC.
3. Where a serious flaw in the procurement process has been detected, legal counsel will be requested to review any correspondence to be sent to a complainant. Where appropriate, such correspondence will be issued by Legal Services.
4. If a vendor submits an FOI request related to the procurement, the timeframes for the VCRP may be extended, due to resource limitations, until after the FOI request is completed.
5. The VCRP is not intended to detract from a vendor's access to legal recourse or to the Ombudsperson's Office. However, VCRP complaints will not generally be considered concurrently with one of these other processes.
6. No compensation will be awarded to a complainant under the VCRP.
7. A decision of the PGO shall be the final determination on a complaint registered with the VCRP process.

6.4 Information and References

6.4.1 Shared Services BC (SSBC) in Solutions BC provides a wide range of purchasing-related services to ministries, agencies and their employees, including but not limited to:

- procuring goods and services through fair and open tendering, and providing advice and consultation on purchasing matters;
- posting solicitations on BC Bid for electronic procurement;
- providing information to suppliers about how to do business with government;
- managing lists of qualified suppliers;
- analyzing spend data across government and participating public sector agencies in order to identify opportunities for demand aggregation and volume procurement, establishing standards and specifications, and establishing and managing CSAs for common use goods and services;
- managing the government's vehicle management outsourcing contract, purchase card, and travel card programs and any other cross government supply contracts;
- managing the catalogue within the iProcurement module that is used by all ministries;
- determining how to choose the right procurement method;
- providing a reference library, including common use formats such as solicitation templates and sample contract forms; and
- managing disposals of tangible and intangible property through fair and open disposal processes, and providing advice and consultation on disposal matters.

6.4.2 BC Bid is the Province's online tendering system. Ministries, Crown corporations and public bodies use the system to

distribute Opportunity Notices, complete bid documents and bid results for suppliers. BC Bid offers suppliers unrestricted access to government procurement. The disclosure of bid results supports monitoring of the fairness and value of government purchases.

6.4.3 Request for Proposals – SSBC has developed an RFP template and guide to the Request for Proposal process. Refer to: http://www.pss.gov.bc.ca/psb/procurement/procurement-templates.html

6.4.4 Trade Agreements

a. Agreement on Internal Trade (AIT) – the Agreement came into effect on July 1, 1995. The AIT applies to:

- all ministries, agencies, boards and commissions;
- all acquisitions of goods of $25,000 or more; and to
- all acquisitions of services and construction of $100,000 or more.
- Entities excluded from the AIT are listed in AIT Annex 502.2A.

b. The British Columbia - Alberta Trade, Investment, and Labour Mobility Agreement (TILMA) - Effective April 1, 2007 TILMA applies to:

- ministries, agencies, boards, councils, committees and commissions;
- procurement of goods: $10,000 or more;
- procurement of services: $75,000 or more; and to
- procurement of construction $100,000 or more.

Exceptions to TILMA are listed in Part V of the agreement.

6.4.5 Disclosure of Contract information – *Freedom of Information and Protection of Privacy Act* governs policy related to the disclosure of any contract information. The Freedom of Information and Protection of Privacy Policy and Procedures Manual contains policy and guidance. In addition, each ministry has a Director/Manager of Information and Privacy who can provide direction and advice.

6.4.6 Risk Management Branch – The Risk Management Branch is accountable for the effective management of the risks of loss to which the government is exposed by virtue of its assets, programs and operations. In delivering its mandate, the branch has assumed four different roles: central risk management agency within government, risk management advisor/consultant, risk management program development and delivery, and claims and litigation management.

Ministry of Finance

Revenue Management

Table of Contents

7.0 Revenue Management

Part I Revenue

- 7.1 Objectives
- 7.2 General
- 7.3 Policy
  - 7.3.1 Revenue Recognition
  - 7.3.2 Fees and Licences
  - 7.3.3 Cost Sharing Arrangements
  - 7.3.4 Internal Control of Public Money
  - 7.3.5 Delegation of Authority
  - 7.3.6 Credit Management
  - 7.3.7 Billing and Payment
  - 7.3.8 Acceptance of Electronic Payments
  - 7.3.9 Receipts and Deposits
  - 7.3.10 Accelerated Transfer Accounts
  - 7.3.11 Refunds
  - 7.3.12 Dishonoured Banking Instruments
  - 7.3.13 Exchange Rates
  - 7.3.14 Suspense Accounts
  - 7.3.15 Insurance Proceeds
- 7.4 Links

Part II Accounts Receivable

- 7.1 Objectives
- 7.2 General
- 7.3 Policy
  - 7.3.1 Recording of Accounts Receivable
  - 7.3.2 Control and Subsidiary Accounts
  - 7.3.3 Statements to Debtors
  - 7.3.4 Reporting Requirements
  - 7.3.5 Interest on Accounts Receivable
  - 7.3.6 Ministry Collection Action
  - 7.3.7 Employee Collection Action
  - 7.3.8 Set-offs
  - 7.3.9 Third Party Demands and Garnishments
  - 7.3.10 Collection and Loan Management Branch
  - 7.3.11 Private Collection Agencies
  - 7.3.12 Write-offs
  - 7.3.13 Extinguishments
  - 7.3.14 Remissions

PART I Revenue

7.1 Objectives

- ensure that revenue from all sources is identified, claimed, recorded, collected, safeguarded and reported in a timely and effective manner
- receipts of money are accurately and completely accounted for and adequately controlled to prevent or detect error, fraud or omission
- proper administrative and control processes are established for accelerated transfer accounts, including authorization, review and reconciliation
- minimize, wherever practicable, the creation of accounts receivable

7.2 General

Ministries are responsible for ensuring that public money is adequately controlled, collected and reported.

Government Caucus Committee on Government Operations and the Economics Branch, Ministry of Competition, Science and Enterprise, reviews ministry proposals for new or modified fees, licenses and other charges.

Banking/Cash Management Branch, Provincial Treasury, is responsible for approval of corporate payment solutions that consider client and government needs, and approves accelerated transfer accounts with financial institutions.

Risk Management Branch, Provincial Treasury, receives and reviews reports on losses of public money.

Intergovernmental Fiscal Relations Branch, Treasury Board Staff, Ministry of Finance, is responsible for reviewing cost sharing arrangements.

Financial Management Branch, Office of the Comptroller General, develops and maintains revenue management policy.

Ministries and central agencies are responsible to ensure that public facing payment services are managed in compliance with Payment Card Industry Data Security Standards.

7.3 Policy

7.3.1 Revenue Recognition

1. Revenue must be recorded at the earliest point at which goods or services or rights under an agreement are provided or performed, or when fines or penalties are imposed and taxes come due.
2. Revenue from the sale of goods must be recorded when government has transferred the significant risks and rewards of ownership to the buyer.
3. While not recognized as revenue, the Harmonized Sales Tax (HST) applies to sales of taxable goods and services. Ministries must charge, collect and record this HST as a Balance Sheet Item in the "HST Collected" STOB 1576.

   Procedure Requirements - M.1, M.3 & M.19

7.3.2 Fees and Licences

1. Ministries (and certain taxpayer-supported Crown entities and agencies) must submit proposals for changes to fees, licences and fines to the Treasury Board Fee Sub-Committee, Treasury Board Staff, as part of the budget process. Full instructions on the fee review process are available on the Treasury Board Staff Budget Information website (government access only).
2. Ministries must maintain a complete and up-to-date inventory of fees, licenses and other non-tax charges, and services that are provided at no charge.

7.3.3 Cost Sharing Arrangements

1. Ministries must maintain an inventory of intergovernmental or public/private cost sharing arrangements and make claims under these agreements promptly. At each fiscal year-end, ministries must report cost sharing arrangements to the Intergovernmental Fiscal Relations and Income Security Branch, Ministry of Finance.
2. Chief financial officers must participate in the negotiation and monitoring of cost sharing arrangements to ensure that there are appropriate financial systems and internal controls in place.

7.3.4 Internal Control of Public Money

1. Ministries must establish effective systems and controls for the identification, receipt, collection and safeguarding of public money. Accounting records must be supported by a complete audit trail.

7.3.5 Delegation of Authority

1. Deputy Ministers must approve their ministry revenue authorities matrix that lists those officers who are authorized to:

    a. receive public money;
    b. extend credit;
    c. issue invoices;
    d. write off debts;
    e. approve credit notes;
    f. approve refunds;
    g. approve journal vouchers;
    h. initiate set-offs; and
    i. waive dishonoured cheque service fees.
2. Specimen signature cards approved by the signing authorities officer must be maintained in respect of the authorities granted under policy 1.
3. Officers authorized to *receive public money* (policy 1(a)) must not be given any other authority described in policy 1.
4. Officers authorized to *issue invoices* (policy 1(c)) must not be given authority to receive public money, write off debts, approve credit notes, refunds or journal vouchers, or initiate set-offs.
5. Any exception to policy 3 or 4 to accommodate an extraordinary ministry operational requirement (e.g., limited office staff) must be checked by appropriate compensating controls and balanced against the risks in the circumstances. Ministry chief financial officers must approve any such exception to policy.

7.3.6 Credit Management

1. Ministries must grant credit only where:

    - the terms and conditions of a loan agreement or other program provide for payment; or
    - services, goods or rights under an agreement are provided on specific credit terms.

2. Ministries providing loans, or goods, services or rights under an agreement on credit must assign an officer with responsibility for credit management functions.

7.3.7 Billing and Payment

1. When payment is not received at the time that goods and services are provided, an invoice or other type of debit note must be issued as soon as possible (e.g., within 30 days). Where goods and services are provided on a continuing basis or over a long period of time, invoices must be issued at regular intervals.

7.3.8 Acceptance of Electronic Payments

Ministry programs will provide for electronic payment instruments for consumer convenience and consistency when accepting public money.

1. The Province, through Banking/Cash Management, Provincial Treasury, has adopted the payment card industry standards (PCI) for its electronic payment systems for government.
2. The Banking/Cash Management Branch, Provincial Treasury, will approve and coordinate ministry acceptance of electronic payments. This ensures that adequate security and process standards are maintained including safeguarding the integrity and non-repudiation of transactions and data storage, retention and use.
3. Ministries are responsible for any costs associated with electronic payment transactions incurred by program areas operating within their mandate, including disputed sales.
4. Banking/Cash Management Branch, Provincial Treasury, will determine and approve a standard suite of electronic payment options based on program type and delivery models and payment card industry requirements. Consideration will be given to corporate solutions and government agreements with banks and card processors in addition to ministry and program objectives.

7.3.9 Receipts and Deposits

1. Public money must be deposited promptly to the credit of the Minister of Finance:
    - to an accelerated transfer account at a financial institution;
    - with a government agent;
    - or other person appointed by the Minister of Finance to receive deposits of public money on behalf of the government.
2. Post-dated cheques must be listed and secured until their payment date and deposited promptly at that time.
3. Ministries must issue a receipt to payers of public money that is paid in cash at the time the exchange takes place. Ministries must discourage the remittance of cash through the mail. Ministries must record the collection of all public money.
4. Payment may be made by cash, cheque, or electronically. Ministries can refuse to accept cheques in certain circumstances, which must be approved by the ministry chief financial officer.
5. Cheques and other negotiable instruments must be endorsed "*For Deposit Only to the Credit of the Minister of Finance*" immediately upon receipt, except for remittances where conditions for payment have not been met (e.g., security deposits). Payments that do not meet payment conditions (e.g., conditional payment) must be returned immediately to the remitter.
6. Whenever payment is made by a cheque by a member of the public in person, ministries must make reasonable checks before accepting the payment. For example, compare the cheque details to the person's separate identification to match the name and address.
7. Ministries must provide adequate facilities for the safekeeping of public money at all times (e.g., from the time received until it is banked).
8. Deposits must be made *daily* except where circumstances dictate this is not practicable or cost effective. The ministry's chief financial officer must approve any exceptions.

Procedure Requirements - G.1

7.3.10 Accelerated Transfer Accounts

1. Ministries must keep the number of accelerated transfer accounts to a minimum. Ministry applications for accounts must be consistent with operating requirements.
2. The Banking/Cash Management Branch must only set up accelerated transfer accounts with financial institutions.
3. Ministries must keep an adequate record of deposits to accelerated transfer accounts, and provide this record to the Office of the Comptroller General, upon request, for bank reconciliation purposes.
4. Ministries must keep an adequate record of their accelerated transfer accounts. This ministry record must be reconciled at least annually to the central record maintained by Banking/Cash Management Branch.

5. Ministries must review accelerated transfer accounts at least annually to ensure each account is still required. Any account not required must be closed.

   Procedure Requirements - G.2

7.3.11 Refunds

1. Ministries must define "*money received for any purpose that is not fulfilled*", and must determine whether refunds are permitted, and the minimum amount to be refunded. In making these determinations, ministries must take into account enabling legislation and regulations under which revenues are collected.
2. Ministry policies regarding refunds must be documented and communicated as part of the schedule of fees and licences, and must be consistently applied.
3. Refunds must be identified and recorded in the ministry's accounting records.
4. Where a partial refund is made, the reason for refunding a reduced amount must be documented.

7.3.12 Dishonoured Banking Instruments

1. Where a banking instrument (e.g., a cheque, pre-authorized debit or electronic funds transfer) has been deposited by the Province in settlement of a claim and it has been subsequently dishonoured, an accounts receivable must be set up by the responsible ministry. The amount must include a dishonoured banking instrument fee shown separately on any billing. A fee of $30 will be levied against each banking instrument that is dishonoured.
2. Ministries must immediately advise debtors of their dishonoured banking instrument and the fee charged.
3. Payments received for dishonoured banking instrument fees must be paid into the Consolidated Revenue Fund and identified from other public money by use of a separate STOB.

7.3.13 Exchange Rates

1. The Office of the Comptroller General (OCG) establishes a Canadian/U.S. dollar exchange rate at the start of each fiscal quarter, or more frequently where fluctuations are significant. OCG must advise ministries and government agents of the prevailing quarterly rate two working days preceding each fiscal quarter.
2. The difference between the actual premium received from or discount paid by the financial institution and the established exchange rate must be recorded in the U.S. Fund Exchange STOB established by OCG.
3. Overpayments resulting from payments received by mail in U.S. funds must be credited initially to a miscellaneous STOB of the ministry. Underpayments resulting from payments received by mail in U.S. funds must be accepted or returned according to the amount of the underpayment and the status of the debtor.
4. All payments received in U.S. funds exceeding $10,000 must be deposited according to procedures established by the Banking/Cash Management Branch, Provincial Treasury. Ministries must consult with Provincial Treasury in respect of these deposits.

   Procedure Requirements - G.4

7.3.14 Suspense Accounts

1. Where public money has been received and cannot be immediately identified, it must be paid into the Consolidated Revenue Fund and credited to a suspense account established for that purpose.
2. Entries in suspense accounts must be cleared to appropriate accounts as soon as sufficient information is received. In no case should this time exceed one month.
3. Monthly, each ministry must analyze its suspense accounts and reconcile them with the balance reported in the central accounting system.

7.3.15 Insurance Proceeds

1. Ministries must ensure that insurance claims are submitted to the Risk Management Branch, Provincial Treasury, for presentation to the insurer. Ministries must maintain a record of claims submitted and insurance proceeds received.

2. Ministries, in consultation with the Risk Management Branch, must identify the value of and likelihood of receiving proceeds from an insurance claim. A ministry must record the claim as an account receivable when the value is determinable and expected to be received.
3. When insurance proceeds are received before incurring an expenditure, they must be paid into the Consolidated Revenue Fund and credited to a suspense account.
4. When insurance proceeds are received in the same fiscal year to replace an insurable loss not involving tangible capital assets, ministries must credit the proceeds to the expenditure service line. Unless an account receivable for the claim has been recorded (as in policy 2), proceeds received in a subsequent fiscal year must be credited to a miscellaneous revenue STOB, "Insurance Proceeds."
5. Insurance proceeds from loss or damage to tangible capital assets, regardless of the fiscal year, must be recorded as proceeds of disposition/disposal and form part of the gain/loss calculation on disposal of tangible capital assets.
6. Where no expenditure has resulted from a loss, damage or other event, insurance proceeds must be paid into the Consolidated Revenue Fund and credited to a miscellaneous revenue STOB, "Insurance Proceeds". Proceeds from loss or damage to tangible capital assets must be recorded as proceeds of disposition/disposal and form part of the gain/loss calculation on disposal (as in policy 5 above) and the write down of the asset not replaced.
7. Where the amount of insurance proceeds is greater than any expenditure resulting from a loss, the surplus must be paid into the Consolidated Revenue Fund and credited to miscellaneous revenue STOB, "Insurance Proceeds". Surplus proceeds from loss or damage to tangible capital assets must be recorded as required in Policies 5 and 6.

7.4 Links

Acceptance of Credit Card Payments: PCI Compliance Standards Roles & Responsibilities

PART II Accounts Receivable

7.1 Objectives

- manage accounts receivable effectively, including prompt and vigorous collection to minimize amounts owing to government
- provide consistent and equitable treatment to debtors, and regular communication on amounts owing
- charge interest on overdue accounts receivable
- ensure uncollectible accounts receivable are written off under the proper authority, and only after all reasonable and appropriate collection action has been taken
- ensure that debts extinguished by legislation are adjusted in a timely manner

7.2 General

Ministries are responsible for effective communication with debtors, third parties and the Collection and Loan Management Branch (CLMB); and ensuring that accounts receivable are adequately reported, collected, extinguished or written off as appropriate.

CLMB, Ministry of Small Business and Revenue, is authorized to collect delinquent non-tax debts on behalf of ministries that do not specialize in the collection function or have specific authority under legislation other than the *Financial Administration Act*. CLMB also has the authority to sign third party demands on behalf of the Minister of Finance and to set off taxes owed to the debtor by Canada Customs and Revenue Agency.

The Office of the Comptroller General maintains policy for the administration of accounts receivable and provides quarterly and annual government-wide receivables performance reports.

7.3 Policy

7.3.1 Recording of Accounts Receivable

1. All amounts determined to be due to the government must be promptly recorded as an accounts receivable by the ministry. Each account receivable must be recorded and maintained until payment is received or the recorded amount is written off or extinguished.
2. An adequate provision for doubtful accounts must be established. When all reasonable efforts fail to collect an account receivable and it has been approved for write off, the related provision for doubtful accounts should be reduced.

7.3.2 Control and Subsidiary Accounts

1. Ministry accounting systems must incorporate control accounts, where applicable, to ensure the completeness and accuracy of individual accounts.
2. A ministry's accounts receivable control STOB must include all receivables except loans, mortgages and accountable advances. Separate control STOBs must be maintained for loans, mortgages and accountable advances. Each control STOB must consist of total amounts due, less total amounts received, and any authorized adjustments.
3. Ministries must maintain subsidiary accounts for individual debtors in a manner that discloses, at a given point in time, the aggregate amount owed by each debtor as well as individual amounts making up the aggregate amount. Ministries must also produce aged trial balances for review by senior officers.
4. Monthly, ministries must reconcile subsidiary accounts with the control STOB for each accounts receivable, loans receivable, mortgages receivable and accountable advances.

7.3.3 Statements to Debtors

1. Ministries must issue periodic statements to debtors providing meaningful and concise information on the status of their debts (e.g., identifying principal and interest components). Ministries must determine the frequency of issuing statements based upon the nature of the accounts receivable.
2. Where an amount is due under a loan or other agreement, the debtor must be notified at least 30 days before the due date. If interest is to be assessed for late payment, it must be specified on the invoice and statement.

7.3.4 Reporting Requirements

1. By July 20, October 20, January 20 and April 30 of each year, the ministry chief financial officer must report to the Financial Management Branch, OCG, accounts receivable on an aged basis, and by each major revenue source or program as at the quarterly period ended. Explanations of significant variances from the report for the previous quarter must be included with each quarterly report. The aging categories must be as follows:

    - accrued/not accrued;
    - current;
    - 31 - 60 days;
    - 61 - 90 days;
    - 91 days - 1 year;
    - 1 - 2 years;
    - 2 - 3 years;
    - over 3 years.

2. By April 30 of each year, the chief financial officer must report to the Financial Management Branch, OCG, a summary of accounts receivable activity by source or program for significant revenue and accounts receivable at fiscal year-end (revenue normally exceeding $25 million, or accounts receivable balances normally exceeding $5 million).

7.3.5 Interest on Accounts Receivable

1. Ministries must charge interest on amounts owing to the government in accordance with the *Interest on Overdue Accounts Receivable Regulation*.
2. Ministries must calculate interest on overdue accounts receivable on a prorated basis (compounded monthly as in

policy 9) commencing on the first day after the money becomes due. Money is due when:

- an invoice or a written request to the debtor for payment had been issued and not paid within 30 days; or
- the goods have been delivered in good condition or the services have been performed in accordance with the contract and not paid within 30 days.

3. Where the amount of interest calculated is $5.00 or more it must be added to the accounts receivable. Where the amount is less than $5.00 it is deemed not due to the government.
4. When a debtor pays an account in full within 30 days, the ministry must accept payment of that amount as full settlement of the account.
5. Ministries must record interest charges owing separately in their accounts receivable records and identify individual amounts owing for each debtor.
6. Ministries must advise each debtor of all interest charges to the debtor's account either by separate invoice or through periodic statements of account.
7. Ministries must deposit payments for interest charges to the Consolidated Revenue Fund.
8. Where interest arises from a loan agreement or similar contractual arrangement, interest on the past due principal and interest must be calculated according to the terms and conditions of the contract.
9. When a debt has been written off, ministries must stop recording interest as revenue and an amount owing. If a debt that was written off is reactivated, the ministry must record interest from the date the debt was written off until the debt is paid.
10. The interest calculated must be compounded monthly. Monthly compounding occurs on the same day, as the due date in any subsequent calendar month (i.e., if the due date is May 11, then the first compounding date is June 11). Compounding is based on the number of days from, but excluding the last compounding date (or if no compounding date has yet occurred, the due date) to and including the current compounding date.

Procedure Requirements - G.7

7.3.6 Ministry Collection Action

1. Each ministry must establish a collection strategy that takes advantage of the full range of available collection methods, tools and specialists. The collection strategy needs to complement program needs and statutory requirements.
2. Ministries must establish an accurate and timely reporting system to notify collections staff when an accounts receivable becomes overdue.
3. Ministries must take prompt and vigorous action to collect overdue accounts receivable. Ministries must establish fair but determined processes to recover these accounts.
4. Ministries must document all actions taken to collect overdue accounts.
5. Each ministry is accountable for its own accounts receivable collection results. This accountability for collection results does not end on the transfer of a ministry's accounts receivable to a central government collection branch, a private collection agency or by any other alternative method of collection.
6. Accounts receivable are considered overdue when a debtor does not pay or resolve the debt within 30 days after the government issues an invoice or a written request for payment to the debtor.
7. Accounts receivable, in most cases, should be at least 30 days overdue (i.e., 60 days after invoice notification), before ministries advise debtors that their accounts are overdue and that the accounts may be:

    - turned over to a central government collection or private collection agency; or
    - subject to legal action.

8. In circumstances where the government owes money to a person, and that same person owes money to the government, recovery must be initiated by the creditor ministry by way of:

    - adjustment to payment, if within the ministry; or
    - set-off through Legal Encumbrance Section, OCG if between ministries

9. When a payment has been received and two or more ministries have claims against a debtor, they must be addressed in the following order:
    - first, by the expressed statements or implied actions of the debtor;
    - second, to the government's advantage; and
    - third, to the earliest debt in time, and to interest before principal.
10. Ministries must enter into information sharing agreements when sharing personal information with another ministry or public body for the purpose of collecting government debt, as indicated by section 33 (i) (i) of the *Freedom of Information and Protection of Privacy Act*.

7.3.7 Employee Collection Action

1. Ministries must immediately inform employees of any salary or other overpayments and establish a mutually agreeable schedule for full repayment. The repayment schedule must be signed off by the ministry and the employee, and placed on the employee's payroll file. The amount owing must be recorded as an account receivable until the overpayment has been recovered. Where the employee will not agree to a reasonable repayment schedule, deductions from pay can be made without the employee's written authorization. The deduction may be considered repayment of an advance.
2. Ministries must consult with Strategic Human Resources in any situation where the collection action being considered is beyond the scope of this policy.

7.3.8 Set-offs

1. Before set-off action is initiated, ministries must ensure that all regular means of collecting the debt have been considered and attempted.
2. Ministries must forward interministry set-off requests submitted under section 38 of the *Financial Administration Act* to the Comptroller General for approval.
3. After approval by the Comptroller General, the account receivable of the debtor may be reduced once processing of the cheque or payroll requisition is completed.
4. Where the amount due to the government is less than or equal to the amount owing by the government, the payment requisition must include the amount to be set-off against the gross amount to be paid. This policy does not apply to contractual arrangements containing a specific provision not to set-off.
5. The ministry must initiate set-off action to protect the government's interest for any goods or services provided prior to the date of appointment of a receiver or of an assignment in bankruptcy. Any residual amount payable is to be paid to the receiver or trustee in bankruptcy, as appropriate. The ministry must consult with its legal counsel if there is any doubt as to the legality of the payment.
6. When the ministry wishes to take set-off action against a Crown corporation or a public body of the Province, it must first consult with the ministry responsible for the debtor entity. The result of this consultation must be included with the request to the Comptroller General for set-off action. A copy of the request must be sent to the chief financial officer of the ministry responsible for the debtor.
7. Before initiating a trust account set-off, ministries must obtain a legal opinion that this action is acceptable, either under statutes governing the trust or under the trust instrument itself. Ministries must include a copy of the opinion with the set-off request.
8. When a set-off is made, the debtor must be informed in writing of the gross payment, the set-off amount and the net payment.
9. Where two or more ministries are pursuing set-off action with a debtor and the government receives a payment for less than the total of all claims, the funds must be allocated to the ministries in the order outlined in Ministry Collection Action, section 7.3.6, policy 9. Where ministries do not agree on the priority of their respective claims, the Comptroller General must allocate the funds.
10. With the exception of salary overpayments, ministries must provide employees who owe money to the Province with written notice of the intent to set-off. Notice must be presented to the employee directly.
11. Where third party demands are initiated at the same time as set-off action, the ministry must inform the Assistant Manager, Legal Encumbrance Branch, OCG, immediately when payment is received. When a debt is recovered in full, all set-offs and third party demands relating to the debt must be cancelled and any surplus funds must be returned

promptly.

7.3.9 Third Party Demands and Garnishments

1. The ministry chief financial officer must ensure that the following information is retained on file prior to approving a request for a third party demand:
    - how and when the debt arose;
    - evidence that the debt can be collected legally;
    - collection action taken to date;
    - the reason for initiating the third party demand;
    - third parties known to do business with, or who employ, the debtor;
    - set-off action instituted or recommended; and
    - a completed (but unsigned) Third Party Demand Notice.
2. Prior to issuing a request for a third party demand, ministries must ensure:
    - accounts receivable collection has been pursued consistent with policy;
    - the debt can be collected legally. Where doubt exists, the ministry must request that legal counsel obtains a judgment against the debtor; and
    - consider set-off action; or
    - consider a defined payment schedule.
3. Ministries must forward unsigned Third Party Demand Notices together with documentation indicating the chief financial officer's approval to the Collection and Loan Management Branch (CLMB) for sign-off.
4. The debt must include interest in accordance with policy. The third party demand must stipulate that interest is accruing.
5. Normally, ministries should not initiate a demand on a third party until at least 90 days after the debt was incurred.In certain instances, however immediate collection may be warranted. A third party demand must be requested promptly and normal means of collection can be bypassed or shortened.
6. A third party demand on an employer must not exceed 30 per cent of the net wages or salary per pay period of the employee (debtor) except where the ministry considers it is unlikely that the remainder of the debt will be collected, or the debtor will remain employed with that employer.
7. The debtor must be notified by the ministry at the same time and in the same manner as a demand is made on a third party.
8. Ministries must not execute against joint bank accounts unless all parties to the account are debtors of the Province.
9. If set-off relating to the same debt has been initiated, the ministry must also inform the Assistant Manager, Legal Encumbrances Branch, OCG, upon receipt of payments.
10. When a debt to the government is paid in full, all demands and set-offs for that debt must be cancelled. Surplus funds received from the third party or from the debtor must be returned promptly.
11. Verbal instructions to the third party by a ministry officer are sufficient to cancel a demand notice. Verbal cancellation of a demand notice must be confirmed in writing by the ministry.
12. A third party demand expires when the debt is paid in full, or if applicable, at the end of the term set out in the demand notice.
13. Where there is any doubt about government proceedings, ministry legal counsel must be consulted to ensure that garnishment orders are obtained in an appropriate manner.

7.3.10 Collection and Loan Management Branch

1. Ministries must obtain approval from Treasury Board Staff to transfer the collection of delinquent debts to the Collection and Loan Management Branch (CLMB).
2. Either the ministry or CLMB can seek to establish a memorandum of understanding for the transfer of delinquent

debts. The parties must submit a joint proposal to Treasury Board Staff providing the general framework for the transfer of debts from the ministry to CLMB.

3. The ministry and CLMB must complete a memorandum of understanding, based on a netting model, for the recovery of administrative costs. The memorandum of understanding should set out any direct reimbursement by the ministry to CLMB for services or costs not covered by the netting model.
4. Prior to a ministry referring debts to CLMB, the ministry must validate all accounts and ensure that the debts are clear of any appeals and/or adjustments.
5. The ministry and CLMB must sign an information sharing agreement that provides direction on the reasons for collection and for the use and disclosure of that personal information.

7.3.11 Private Collection Agencies

1. Ministries must only consider the services of private collection agencies to recover debts owed to the government after the ministry's normal collection activities have been exhausted, or when a business case supports this collection option.
2. Commission costs for private collection agencies to collect ministry delinquent accounts receivable must only cover fees payable for the successful collection of debt. The cost of additional services that are not directly related to the successful collection of debt (e.g., skip tracing, credit checks, credit bureau reporting) cannot be netted from collection proceeds and must be funded by the ministry.
3. Ministries must not use private collection agencies for debts due from the following:
    - other ministries or agencies, trusts, boards or commissions and government organizations;
    - provincial government employees from whom the ministry can recover by set-off action;
    - other governments; and
    - participants in a current appeal or a court proceeding.
4. The ministry and the private collection agency must complete a contract specifying the transfer of delinquent debts and the details of collection. The contract must include the commission rate for accounts collected, the cost of additional services and the rights and obligations of each party.
5. The amount of a fee or the rate of commission must be reviewed by the ministry and approved by Treasury Board as part of the annual review of fees and licenses.

7.3.12 Write-offs

1. Only those debts for which all reasonable and appropriate collection action has been taken can be submitted for write-off.
2. Ministries must ensure that uncollectible debts are reviewed at least once a year and identify those debts that should be submitted for write-off.
3. All write-off submissions must include the relevant debt information. Submissions for the write-off of debts exceeding $5,000 must be appropriately categorized, and must include details of the collection action taken, the debtor's financial status (if relevant), and why further collection action is not possible.
4. The categories for submission are:
    - debtors who have died leaving no estate;
    - debtors who cannot be located;
    - debtors who are indigent;
    - debtors residing outside of Canada in locations where there are no apparent means of collection and there is no indication that the debtor has family or business ties that might encourage return to Canada;
    - debts where, in the view of the creditor ministry, further expenses to collect are not justified in relation to the amount of the debt and the possibility of collection;
    - debts where legal counsel has indicated that the amount involved does not warrant the prospective costs of action to collect;
    - debts where liability has not been admitted by the debtor and where the success of proceedings to collect is

unlikely;

- debts where the existence of an enforceable debt due the Crown cannot be readily established (e.g., where records have been lost or destroyed and the ministry is unable to prove receipt of services by the debtor); and
- debts where a corporation is inoperative and without assets.

5. The chief financial officer must authorize the write-off of receivables of $5,000 or less. This authority may be delegated to officers within the ministry to write off individual debts of $500 or less. Officers must maintain adequate records of any amounts that they have written off and report quarterly to the chief financial officer on any write-off action taken during the quarter.
6. The executive financial officer must recommend the write-off of debts greater than $5,000 and less than or equal to $100,000. Submissions for approval must be made to the Comptroller General through the Financial Management Branch, OCG.
7. The respective minister must sign on the recommendation of the executive financial officer all submissions for the write-off of debts greater than $100,000. Submissions for approval must be made to Treasury Board through the Financial Management Branch, OCG.
8. Ministries must not submit the following debts to the Comptroller General or to Treasury Board for write-off:
   - bankrupt individuals – when an order of discharge has been granted, the ministry must remove the account on the basis of the order;
   - judgment or other court orders – when it is determined that the Province can collect a lesser amount than the recorded debt, the ministry must adjust the account on the basis of the court's order;
   - restrictions imposed by statute – where a statute restricts the amount of a debt (e.g., the *Court Order Enforcement Act,* the *Limitation Act*), the ministry must adjust the account on the basis of the recoverable amount.
9. Debts of a bankrupt corporation must be written off through the normal procedures since, according to the *Federal Bankruptcy and Insolvency Act*, a corporation may not apply for a discharge unless it has fully satisfied the claims of its creditors.
10. After consulting with its legal counsel, a ministry may accept a compromise settlement of a debt. A portion of the original debt must be written off as identified under the terms of an agreement.
11. When authority has been received to write off a debt, the debt must be transferred from the ministry accounts to a reference file of "debts written off", where it must remain until paid, or forgiven (pursuant to section 18 or 19 of the *Financial Administration Act*), or extinguished pursuant to other legislation.
12. Annually, ministries must submit statements of debts written off during the fiscal year, together with supporting authorizations, to Financial Reporting and Advisory Services, OCG, for Public Accounts reporting purposes.

7.3.13 Extinguishments

1. The responsible minister must authorize all submissions for extinguishment. Proposals must be forwarded for review to the Minister of Finance, through the Financial Management Branch, OCG, prior to submission to the Lieutenant Governor in Council.
2. The Minister or the Deputy Minister of Finance, or the Assistant Deputy Minister, Provincial Treasury, pursuant to BC Regulation 269/92, can conclude a settlement agreement or compromise settlement to forgive some or all of a debt or obligation not exceeding $100,000. In addition, the following CLMB officers have authority to conclude a settlement agreement to forgive some or all of a debt or obligation (principal plus interest) to the following limits:
   - the director – $40,000;
   - a manager – $20,000;
   - a collection officer – $10,000.
3. A ministry may accept a compromise settlement of a debt only after approval by Legal Services, Ministry of Attorney General. A portion of the original debt can be extinguished under the terms of an agreement.
4. Annually, ministries must submit statements of debts extinguished during the fiscal year, together with supporting documentation, to Financial Reporting and Advisory Services, OCG, for Public Accounts reporting purposes.

7.3.14 Remissions

1. Submissions for remission orders must be:
    - prepared by the ministry officials responsible for revenue management;
    - recommended by the senior and executive financial officers;
    - recommended by the Minister of Finance; and then
    - submitted to the Executive Council (i.e., Cabinet).
2. Recommendations submitted pursuant to policy 1 must be to:
    - approve;
    - approve with conditions;
    - not approve; or
    - provide no opinion because of conflict of interest or some other circumstance that makes an opinion inappropriate or impossible.
3. All submissions for individual ministry remission orders must, at a minimum, contain the following information:
    - the name and address of the person whose obligation is to be forgiven;
    - the amount to be remitted;
    - justification for remission;
    - sufficient background information to enable Cabinet to form an opinion on the question of whether "great public inconvenience", "great injustice" or "great hardship" will result if the remission is not granted; and
    - other information, including ministry comment for or against the remission.
4. Annually, ministries must submit statements of remissions granted during the fiscal year, together with supporting documentation, to Financial Reporting and Advisory Services, OCG, for Public Accounts reporting purposes.

Ministry of Finance

Information Management and Information Technology Management

Table of Contents

12.0 Information and Technology Management
- 12.1 Objectives
- 12.2 General
  - 12.2.1 Principles
  - 12.2.2 IM/IT Governance
- 12.3 Policy
  - 12.3.1 Appropriate Use of Government Resources
  - Appropriate Use of Information Technology
  - 12.3.2 Information and Technology Planning
  - Information Resource Management Plans
  - Vital Records and Information Technology Business Continuity Plans
  - 12.3.3 Information Management
  - Data Management and Architecture
  - Personal Information Protection
  - Managing Information
  - Sharing of Government Information
  - 12.3.4 Electronic Identity Management
  - 12.3.5 Information Technology Management
  - 12.3.6 Information Technology Security
- 12.4 Information and References
  - 12.4.1 Definitions
  - 12.4.2 Links

12.1 Objectives

The objectives of this chapter are to:

- Provide guidance for key legislation, including
  - *Document Disposal Act;*
  - *Electronic Transactions Act;*
  - *Freedom of Information and Protection of Privacy Act; and*
  - *Personal Information Protection Act.*
- Define authorities, responsibilities and accountabilities for information and technology management.
- Provide a policy framework within which government can derive the maximum benefits from the use of information and technology.
- Establish policies for the management of information and technology activities.

12.2 General

12.2.1 Principles

Information management is a core component of government infrastructure; it is the intellectual capital of responsible governance. Best practice policies and standards result in efficient, accountable and cost-effective use of resources. Information technology constitutes the full spectrum of technologies and services that support information management. The

Government Chief Information Officer (CIO) is responsible for the corporate management of information and information technology. The principles underlying effective management are:

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

12.2.2 IM/IT Governance

As Chief Information Officer and technology strategist for major government information and technology initiatives (see CPPM chapter 2 section 2.4.1, Central Agency Policy Responsibility Areas) the Office of the Government CIO is the central authority for the government of British Columbia responsible for Chapter 12. The policies contained in this section should be considered in conjunction with other core policy areas on planning (chapter 3), procurement (chapter 6), fees and licensing (chapter 7), asset management (chapter 8), financial systems and controls (chapter 13), risk management (chapter 14), general security (chapter 15), business continuity (chapter 16) and loss management (chapter 20).

The Office of the Government CIO also maintains four major manuals that support the Core Policy and Procedure Manual (CPPM) Chapter 12. They are the:

- Information and Technology Manual (Supplement to CPPM Chapter 12);
- Freedom of Information and Protection of Privacy Policy and Procedures Manual;
- Recorded Information Management Manual; and
- Information Security Policy.

Additionally there are a variety of standards, directives and memoranda that support core policy located on the Government CIO's website.

In May 2006 Cabinet "Mandate[d] the Chief Information Officer with governance authority for standards setting, oversight and approvals for the Province's information and communications technology." The following authorities, responsibilities and accountabilities reflect past ones that have been ascribed to the Government CIO and new ones that have been developed as part of the Government CIO's Governance Working Group's work. They also include authorities, responsibilities and accountabilities ascribed to Ministries and/or Ministry CIOs in the past version of this chapter as well as those recommended through the work of the Government CIO's Governance Working Group.

Government Chief Information Officer

The Government CIO develops, proposes, and maintains corporate-wide IM/IT policy, procedures and standards, and evaluates compliance. Areas associated with this authority include data access, electronic identity management, records management, information management, information technology, privacy, security applications, and systems of government.

Governance and Policy:

a) Legislation

- Recommends legislation in the areas of information and technology management, including access rights in the public and private sector, privacy, security, records management and electronic service delivery.
- Ensures the legislated Personal Information Directory summaries in the Personal Information Directory are maintained.

b) Policies, Procedures, and Standards

- Proposes corporate IM/IT architecture and related policy, procedures and standards to protect and manage information as a government asset.
- Ensures the privacy and security of citizens through the policies, procedures and standards governing citizens' information held by the Province.
- Ensures government's information systems are designed to be interoperable, secure, and able to authenticate and authorize appropriate access.
- Ensures ministries procure information and technology management goods and services compatible with the government infrastructure.
- Clarifies the interpretation of corporate IM/IT policies, procedures and standards.

c) Compliance Monitoring

- Develops mechanisms and processes to ensure compliance with corporate IM/IT policies, procedures and standards.
- Proposes corporate IM/IT performance metrics that enable ministry compliance.
- Informs ministry CIOs of their responsibilities in complying with corporate IM/IT policies, procedures and standards.
- Recommends and reviews audits in coordination with other central authorities to ensure compliance with corporate IM/IT policies, procedures and standards.
- Accesses audit report data to identify information management practices, and information system infrastructure and applications.
- Identifies information necessary for the performance of the Government CIO's duties from any public officer.

d) Advising Government

- Advises senior ministry decision makers, committees and councils, Treasury Board and Cabinet regarding telecommunications, access rights in the public and private sector, privacy, information and technology management, records management, security and electronic service delivery.
- Provides analysis and recommendations to Treasury Board Staff on initiatives, submissions and/or proposals related to information and technology management.

Strategic IM/IT Planning:

a) IM/IT Planning Framework

- Leads the strategic planning process for corporate IM/IT governance.
- Develops, maintains and facilitates the implementation of an integrated government-wide IM/IT planning framework.
- Facilitates the corporate strategic IM/IT planning process and ensures the alignment of IM/IT plans with government's strategic direction.
- Develops and maintains working relationships with Broader Public Sector (BPS) CIOs to communicate government's IM/IT strategic direction and promote the alignment of BPS IM/IT with core government.
- Ensures that the Province is aware of and keeping pace with legislation, policy trends and issues in other jurisdictions.
- Defines corporate vendor engagement strategies to deliver government's IM/IT priorities.

b) Information Resource Planning

- Provides leadership and strategic direction to ministries for the development of the annual Information Resource Management Planning (IRMP) process.
- Coordinates ministry IRMPs with government's IM/IT strategic directions and priorities.

c) IM/IT Human Resource Capital Planning

- Recommends the strategic direction for human resource capital needed to focus on IM/IT functions across government.
- Identifies human, financial and technical resources required to deliver corporate IM/IT strategic plan.
- Advises Public Service Agency on IM/IT human resource capacity required to achieve government's IM/IT strategic directions and priorities.
- Ensures that awareness and training activities inform staff and contractors of their rights, roles and accountabilities for the security, privacy and management of government's IM/IT assets.

Strategic Infrastructure Development:

- Defines the technological direction and framework for IM/IT across government.
- Provides the strategic direction for cross-ministry IM/IT projects.
- Evaluates new information technologies to determine applicability to government business processes.
- Ensures that structures and reporting relationships for IM/IT sub-committees support strategic infrastructure development. Reviews the IM/IT implications of agreements involving compatibility with government's IM/IT infrastructure and strategic directions.
- Designs strategic infrastructure and coordinates activities to enable stakeholder participation in development of the next generation government network.
- Closes the Digital Divide for First Nations communities, and establishes the basis for implementing the next generation government network.
- Provides leadership and obtains resources for key IM/IT projects to facilitate the ongoing development of government's strategic infrastructure.

Transformational Opportunity Analysis:

- Chairs the CIO Council.
- Advises ministries on the hiring of the ministry CIO.
- Researches and reports on transformational activities and leading IM/IT practices in other jurisdictions.
- Identifies and assesses transformational or integrating IM/IT opportunities in government and, where requested, in the Broader Public Sector.
- Promotes the development of cross-government business processes and an enterprise architecture.
- Ensures alignment to the government's strategic direction for major IM/IT projects and projects with service integration implications through project milestone sign-offs and final project approvals.
- Proposes efficiency and effectiveness measures for improvements in the application of information and technology.

Security:

- Provides the overall strategic direction and policy for securing government's information technology infrastructure and government records including electronic information.
- Ensures that measures are established to assess compliance with IM/IT security policies, procedures and standards.

Ministry Chief Information Officer

Governance and Policy:

a) Governance Authority

- Reports to their respective ministry ADM accountable for IM/IT, with a functional reporting relationship between the Government CIO and the ministry CIO.
- Maintains accountability for all business and operational IM/IT initiatives that have no cross-government implications.

Maintains accountability for IM, budgets, records management, forms management, privacy, security, e-services, business architecture, ministry applications, information management, IM/IT strategic planning and IT (including ministry infrastructure).

- Manages information and technology, and all related support activities.
- Ensures that the delegated responsibility for information and technology is carried out fully.
- Develops an IM/IT workforce strategy to support business transformation, information protection, business continuity and succession planning in consultation with the ministry Strategic HR Director.

b) Legislation

- Provides legislated Personal Information Directory summaries for the Personal Information Directory.

c) Policies and Standards

- Reinforces IM/IT core policies and standards from a risk management perspective.

d) Compliance Monitoring

- Ensures compliance with the IM/IT core policies and standards.

e) Advice to Government

- Ensures that information technology plans address human resource requirements in terms of job design, training and working environment.

Strategic IM/IT Planning:

a) IM/IT Planning Framework

- Establishes strategic direction, consistent with overall government IM/IT direction.
- Participates in ministry service plans and corporate IM/IT planning.
- Accesses the Executive table of each ministry, with stronger emphasis on strategic discussions, rather than just operational issues.

b) Information Resource Planning

- Plans the three year Information Resource Management Plan.
- Works together with other ministry CIOs on horizontal initiatives, both within and across sectors, and adapting to changing priorities.

c) IM/IT Human Capital Planning

- Develops staff to make safe, effective and efficient use of information and technology.
- Manages ministry information resources, ensuring that sound information management practices are followed.

Transformational Opportunity Analysis:

- Provides business analysis and project management expertise.

Strategic Infrastructure Development:

- Functions with a greater role in Information Management within their ministry.
- Supports ministry line of businesses applications.
- Supports ministry-unique applications.

- Develops ministry specific applications if and when required.

Security:

- Protects 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.
- Uses security categories approved by Risk Management Branch.
- Identifies and categorizes information and other assets based on the degree of injury (low, medium, high).

12.3 Policy

12.3.1 Appropriate Use of Government Resources

Objectives

- Meet the requirements mandated by the Standards of Conduct.
- Maximize productivity and prevent risks to network security and performance.
- Protect the privacy, confidentiality and security of government's information.
- Increase adherence to government information and technology-related legislation, policies and standards.
- Promote public trust in government's use of information and technology assets.

General

All users of government's information and technology resources must take responsibility for, and accept the duty to, actively protect information and technology assets. This includes taking responsibility to be aware of, and adhere to, all relevant legislation, policies and standards. Government uses information technologies to support employees and other authorized users to work efficiently in delivering services to citizens. Proper use of these technologies assists in the daily management of information, saves time and money, reduces administrative overhead and improves service delivery. The technologies include, but are not limited to, information systems, services (e.g., web services; messaging services); computers (e.g., hardware, software); and telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants). Improper use may jeopardize the confidentiality, integrity and availability of government's information and technology assets, and may put personal information protection, security or service levels at risk.

Policy

a) Appropriate Use of Information Technology

1. Users must use government-provided information technology resources as the business tools required to do their work and provide efficient service delivery. This use is subject to the same restrictions and management review process as any other government resource.
2. Users must use information and technology resources in accordance with the Standards of Conduct, and applicable terms and conditions. The following conditions, and others that may be established by the Government CIO from time to time, apply to all users:

Users must not:

- attempt to circumvent or subvert system or network security measures;
- propagate viruses knowingly or maliciously;
- detrimentally affect the productivity, integrity or security of government systems;
- obtain files from unauthorized or questionable non-government sources (e.g., racist material, pornography, file swapping sites);
- access Internet sites that might bring the public service into disrepute or harm government's reputation, such as those that carry offensive material;

- access radio stations or video clips (typically referred to as "streaming" audio or video) over the Internet, unless the access is work-related and authorized;
- download non-work related files, such as Freeware, Shareware, movie or music files;
- divulge, share or compromise their own or another's government authentication credentials;
- transmit or otherwise expose sensitive or personal information to the internet;
- use information and technology resources for commercial solicitation or for conducting or pursuing their own business interests or those of another organization;
- distribute hoaxes, chain letters, or advertisements;
- send rude, obscene or harassing messages;
- send, forward and/or reply to large distribution lists concerning non-government business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists; and
- attempt to obscure the origin of any message or download material under an assumed internet address.

Users must:

- comply with all applicable legislation, regulations, policies and standards;
- use all appropriate anti-virus precautions when accessing non-government data and systems from the government network;
- adhere to licensing agreements for all software used;
- respect copyright and other intellectual property rights in relation to both programs and data;
- only use the email account provided by government from the government network when exchanging email with outside systems;
- use approved security measures when accessing the government network from home or a non-government computer;
- only use messaging forums (e.g., Internet Relay Chat, internet newsgroups) when conducting work-related business or exchanging technical or analytical information; and
- use the rules for complex passwords to create password.

3. Employees must have their manager's permission for the personal use of government information technology resources. Personal use of government information technology resources must not occur during peak hours (i.e., 8 a.m. to 5 p.m.) and must be consistent with professional conduct and the Standards of Conduct.
4. Any content created or transmitted using government equipment or retained within the government network will be managed as a government record. There is no expectation of personal privacy related to the use of government information technology resources except for specific privileged communications (i.e., Cabinet, solicitor/client, and union representative communications).
5. Inappropriate use of government information technology resources will be investigated on a case-by-case basis. Individuals misusing government information technology resources are subject to disciplinary action, including dismissal, cancellation of contract, and/or other legal remedies.

12.3.2 Information and Technology Planning

Objectives

- Establish planning tools to integrate government's strategic information and technology directions, ministry service plans, and information management and information technology plans.
- Help ministries align information and technology investments with program objectives, and improve services to the public.
- Improve accountability on information and technology initiatives.
- Evolve an enterprise architecture plan that supports the information and technology needs of government.
- Provide strategies for managing information and technology during daily operations, including critical incidents

management.

- Facilitate the re-establishment of operations during, and immediately following, a critical incident or other serious disruption.

General

The Office of the CIO oversees the information and technology planning cycle to locate, foster and monitor key issues, opportunities and investments in e-government infrastructure and services. The Government CIO has overall responsibility for the Information Resource Management Planning (IRMP) process. This annual planning cycle is driven by the broader business planning cycle of the government (see CPPM chapter 3, Part 1, Objectives). The development of an IRMP helps ministries align information and technology investments with government strategic plans, ministry service plans, information management and technology plans and program objectives to provide improved services to the businesses and citizens of British Columbia. The IRMP provides an opportunity to assess and strategize for optimization of shared services and consider or implement alternate service delivery approaches.

Vital records and business continuity planning is another key planning area that ensures government's business will continue by keeping information safe and accessible and timely recovery of operations following a service disruption. Plans must include how to re-establish the systems and records that enable government to operate effective and efficiently. Service disruptions can range from a short term inability to access records or services to more significant longer term critical incidents where entire networks may be affected.

Policy

a) Information Resource Management Plans

1. An update of a three to five year Information Resource Management Plan must be submitted annually to the Government Chief Information Officer and Treasury Board Staff.

b) Vital Records and Information Technology Business Continuity Plans

1. Government must create and maintain a business continuity plan that includes identification and management of its vital records.
2. Vital records must be maintained so that re-establishing the legal, financial and functional responsibilities of government is achieved quickly after a catastrophic event or crisis.
3. Vital records must be maintained in a manner that meets current environmental and security standards.
4. Ministries must develop, or work with their supporting infrastructure technology service providers to develop, Business Continuity and Disaster Recovery Plans on all information systems and the associated technology infrastructure and test them regularly.

   See CPPM chapter 16 Business Continuity Management, chapter 14 Risk Management and the Government CIO website Information Resource Management Planning.

12.3.3 Information Management

Part I: Data Management and Architecture

Objectives

- Derive maximum business benefit from information and technology.
- Facilitate and enhance government's ability to make informed decisions.
- Improve the accuracy and timeliness of data.
- Increase system effectiveness and efficient access to data.
- Share data within legislative authority to improve service delivery to citizens of British Columbia.

General

To demonstrate that services are delivered efficiently and effectively, government must have access to the data in various computer systems, files and reports. Consistent data management practices allow a common structure for data access, integrated programs/services, data sharing and interoperability with government information systems. The use of data within government is governed by legislation that applies to all public bodies. More specific legislation also authorizes ministry program management and information collection including, in some cases, personal information.

Policy

a) Data Management

1. The Government CIO must define, maintain and publish government data definitions and structures to maximize the business value of shared data.
2. Data and corresponding information systems must be identified, classified, inventoried, documented and maintained throughout their lifecycle.
3. Ministries must establish and maintain a data administration/architecture program to manage the design, integrity, availability, and efficient use of data and information systems.
4. Data and corresponding information systems must have an identified Data Custodian.

See Data Administration Standards.

Part II: Personal Information Protection

Objectives

- Ensure the lawful collection, use, retention, disclosure, disposition and security of personal information by public bodies within British Columbia.
- Assure citizens that privacy principles are being taken into account during the design, implementation and evolution of programs, systems and services.
- Ensure that Privacy Impact Assessments are completed and that privacy issues that arise through these assessments are dealt with prior to implementation.
- Ensure that Information Sharing Agreements are completed when a ministry shares personal information with a party external to the ministry.
- Record summaries of Information Sharing Agreements, Privacy Impact Assessments and Personal Information Banks in the Personal Information Directory.

General

To promote government accountability and protect personal information privacy as described in the *Freedom of Information and Protection of Privacy Act* (the Act) all public bodies must comply with the provisions of the Act and its regulation. The FOIPPA Policy and Procedures Manual is a supplemental manual (publicly available) that interprets the Act by describing the operational policies and procedures that ministries and other government offices must use in carrying out their legislated responsibilities. In some cases public bodies may have other legislation specific to their business that adds privacy, confidentiality or security provisions regarding personal information management, (e.g., *Medicare Protection Act*).

Two standard tools that assist ministries in the management of personal information are Privacy Impact Assessments (PIA) and Information Sharing Agreements. Ministries are required to conduct a PIA for new or revised projects, programs, applications, systems or new enactments. The PIA process determines if the privacy protection requirements of the Act are met. In all cases part 1 (basic information) of the PIA should be completed to assess whether personal information is being collected. Where it is determined that personal information is collected the complete PIA is required, whereas if it not being collected then only part 1 is required. The PIA supports government business objectives by ensuring the collection, use, retention, disclosure and security of information is conducted consistent with the Act and government policies, procedures and protocols. Information Sharing Agreements establish relationships, responsibilities, security requirements, access rights, and authentication requirements between ministries and the data consumers to whom they supply government information. Information Sharing Agreements may also be used in conjunction with alternate service delivery data management contracts and privacy protection schedules or with research agreements to clarify responsibilities of all of the involved parties.

The Act requires that the Minister Responsible for this Act must maintain and publish a Personal Information Directory (PID)

to provide summary information about records in the custody or under the control of ministries of the government of British Columbia and about the use and disclosure of those records. The IM/IT Privacy and Legislation Branch of the Government CIO's office (see Information and Privacy) maintains the central directory of Personal Information Banks, Privacy Impact Assessments and Information Sharing Agreements created by and/or operating on behalf of provincial ministries. Ministries as custodians of the data have the knowledge of the personal information holdings and the responsibility to supply the summaries for inclusion into the PID in a timely manner.

To ensure a proactive privacy framework, sound principles of privacy, security and confidentiality must be understood by all users of personal data and incorporated into daily practice within public bodies. This involves developing a culture where privacy is seen as design objective for information and technology not an obstacle to be overcome. Personal privacy is a right protected through legislation, policies and best practices by the Government of British Columbia.

Policy

a) Privacy Impact Assessments

1. A Privacy Impact Assessment (PIA) must be conducted to determine if a project, program, application, system or new enactment collects, uses, retains or discloses or secures personal information.
2. A preliminary PIA must be completed during the feasibility or initiation stage of any project, program, application, system or enactment. A formal PIA must be finalized, including the sections on security and retention of personal information, before implementation of any project, program, application, system or enactment.
3. Ministries must review existing summaries in the government Personal Information Directory, PIA section, at least once a year, and submit new summaries as needed within 30 days of the final signing off of a PIA.

b) Information Sharing Agreements

1. Ministries must develop Information Sharing Agreements to cover personal information exchanges outside of the immediate program area, as required. These agreements must include a compliance review requirement and schedule of planned reviews.
2. Ministries must review existing sharing agreement summaries in the government Personal Information Directory, Information Sharing Agreement section, at least annually, and submit new summaries as needed within 30 days after approval of an Information Sharing Agreement.

c) Personal Information Banks

1. Ministries must maintain a directory of Personal Information Banks and review the existing Personal Information Banks summaries in the government Personal Information Directory at least annually.
2. New Personal Information Bank summaries must be submitted to the government Personal Information Directory within 30 days of implementation.

d) Personal Information Management

1. People who manage access or use government information must receive privacy and information management training on initial employment and as required thereafter.
2. Personal information in the custody or control of public bodies must be stored, managed and accessed solely within Canada throughout its lifecycle, except in specified circumstances.
3. Remote access from a foreign country to personal data, including viewing, is prohibited except in specified circumstances.
4. Ministries must use the principles of "need-to-know" and "least privilege" when authorizing access to personal information.

Part III: Managing Information

Objectives

- Assign responsibility and accountability for the management of information within the custody, or under the control of,

government.

- Assure compliance with legislation, policies and standards.
- Create and retain a full and accurate record documenting decisions and actions.
- Provide relevant information in a timely, useable, cost-effective, and accurate manner.
- Preserve government information in a manner that retains the information's authenticity, reliability, accessibility and integrity for as long as required.
- Support transparent and effective access to government information within legally established privacy and confidentiality restrictions.

General

The *Interpretation Act* definition of "record" includes all recorded information, whatever the media or format. Information management is a core component of government infrastructure and ensures that critical characteristics such as authenticity, reliability, integrity and usability of a record are preserved and protected for as long as required.

Government must appropriately provide access to, manage, preserve and dispose of its records in compliance with the *Document Disposal Act*, the *Freedom of Information and Protection of Privacy Act*, and other relevant legislation, policies and standards, in order to:

- ensure government accountability;
- provide evidence of its activities and organizational structure;
- document its responsibilities, rights and entitlements; and
- preserve records of enduring value.

Records deemed to have enduring value will be preserved in the government archives. Government records are eligible for final disposition when their scheduled active and semi-active retention periods have expired.

The Government of British Columbia standards for the classification and scheduling of its records are documented in the Administrative Records Classification System (ARCS), the Operational Records Classification Systems (ORCS), ongoing records schedules and other approved records schedules. ARCS and ORCS support the automated scheduling and classification of records within an Enterprise Document and Records Management System (EDRMS). The implementation of the government standard EDRMS software in conjunction with other digital preservation practices and procedures (e.g., storage and media management, metadata standards) supports government's requirements for long-term records preservation.

Policy

a) Governance of Recorded Information

1. Government must manage all records created and received during the conduct of its business activities.
2. Ministries must establish and maintain a recorded information management program.
3. Ministries must establish and maintain a forms management program.
4. Government records must be managed and preserved to remain authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format.
5. Ministries transferring records to off-site storage must use approved records centres.

See CPPM chapter 15, Security.

b) Classification, Scheduling and Maintenance of Government Records

1. Ministries must implement and maintain the government standard records classification and scheduling systems (i.e., ARCS, ORCS, Ongoing Records Schedules).
2. Ministries must develop records classification systems for their operational records (ORCS).

3. Ministries must use the government standard Enterprise Document and Records Management System (EDRMS) when implementing an electronic document and records management system.
4. Government records must remain authentic, reliable and accessible after any conversion or migration from one media, format, or system to another.

c) Storage and Disposition of Government Records

1. Government records must be disposed of securely in accordance with approved records retention and disposition schedules and asset management processes.
2. Ministries must establish internal records disposition procedures.
3. Government records scheduled for archival retention must be maintained in a manner that preserves their integrity and authenticity up to and throughout transfer to the government archives.
4. Government records scheduled for destruction must be destroyed in a method appropriate for the recording media and that maintains the security of the information and the privacy of individuals.

See CPPM chapter 6, Disposal of Surplus Assets, chapter 8, Asset Management and chapter 20, Loss Management.

Part IV: Sharing of Government Information

Objectives

- Adhere to government strategic directions for information management.
- Respond to citizens' needs and expectations of connecting with government electronically, and increasing government accountability to the public.
- Improve ministry products, services and programs.
- Enhance understanding of information used to make decisions.
- Promote efficient and effective sharing while leveraging experience and knowledge of data already collected within government.
- Exchange personal information between a public body and a person, a group of persons or an organization, as allowed within privacy and ministry-specific legislation regarding personal information.

General

Government information is an asset that may be under the custody or control of a ministry or other government agency but is collected for, and owned corporately by, the Crown, i.e., the Province. To achieve the government's goal of effective and efficient citizen-centred service delivery, and to improve public service outcomes, the sharing of relevant information by authorized users must be done across service teams and for common or integrated programs. Sharing of information must be allowed under the *Freedom of Information and Protection of Privacy Act* or another enactment prior to disclosure. The authorized and appropriate use of information within government benefits the citizens and the Government of British Columbia. In particular:

- Routine release is the disclosure of information held by a public body without the necessity of a more costly formal Freedom of Information request.
- Contacting government electronically is becoming a normal part of communications between government, businesses and citizens in British Columbia. An employee's work email address is defined in the *Freedom of Information and Protection of Privacy Act* as contact information and is not therefore personal information. However, the release of a government email address may be restricted in cases involving employee health and safety issues.
- Legally mandated information-sharing requests, e.g., where requirements to disclose information for legal cases or Inquiries, are to be addressed to the appropriate ministry solicitor, Legal Services Branch.

Policy

a) Routine Release of Information

1. Ministries must promote the routine release of information, where allowed by the Freedom of Information and Protection of Privacy Act.
2. Ministries may charge fees for information made available routinely, as pre-approved by Treasury Board.

b) Internal Use of Government Information Assets

1. Originating ministries providing information to internal-to-government users must not charge for information in its basic format. The originating ministry is to determine the basic format for the information. Special circumstances to be negotiated between the two parties.
2. The originating ministry must allow access to information for internal-to-government users in its basic format in the most cost-effective manner (e.g., intranet website). Information access costs are to be borne by the requesting ministry.
3. The information held by the originating ministry must be considered the correct or official version. Internal-to-government users must ensure that the most current version of information be used.
4. Requesting ministries do not have the right to reproduce, market or distribute information to external-to-government users without the approval of the originating ministry. Originating ministries should develop and provide liability disclaimers appropriate for the information being disseminated.
5. To protect confidentiality and security, the information being shared must be documented and shared only on a need-to-know and least privilege basis.

See CPPM chapter 7, section 7.3.2 Fees and Licenses, Privacy Protection Schedule (PPS) and Procurement, Part I, 6.3.3.e, Administration, policy 12.

c) Publication of Government Email Addresses

1. Government email addresses, including generic office email addresses, must be kept up to date and published in the British Columbia Government Directory except where exempted for health and safety reasons.
2. Generic office email IDs may be used when required to meet operational requirements. A specific, designated owner must manage each generic office email ID.
3. Individual alias email IDs must not be used.
4. Government email addresses must not be made available electronically in bulk form external to government (e.g., electronic files, distribution lists).
5. Government e-mail addresses must use the government naming convention (i.e.,firstname.surname@gov.bc.ca) and must not include a host name.

d) Disclosure Requirements for Legal Proceedings

1. Ministries must list all relevant records in their custody or control under the Attorney General's discovery of documents.
2. Government records destruction schedules must be suspended during court orders for Demand of Discovery.
3. Records disposition must be suspended during legally mandated reviews (e.g., litigation, document discovery, and commissions of inquiry.)

e) Crown Copyright

See CPPM chapter 6 Procurement, section 6.3.4.e, Crown Copyright.

f) Intellectual Property

See CPPM chapter 6 Procurement, section 6.3.4.f., Disposal of Intellectual Property.

12.3.4 Electronic Identity Management

Objectives

- Interact electronically with businesses and citizens to conduct business transactions.
- Facilitate the legal use of electronic signatures in e-services between government and citizens and businesses.
- Provide assurance to users of e-services that the privacy, confidentiality, integrity and security of their information will be maintained to the highest possible standard.
- Promote public confidence in management of the identity and eligibility information used for government electronic service delivery.

General

BC government strategic direction includes a commitment to integrate services and to deliver them electronically where possible. This strategy supports a client-centric framework that will assist and enable ministries to deliver services better through improved access to business and citizen online services.

To enable electronic service delivery, the BC government passed the *Electronic Transactions Act* to support its move into the global electronic economy. The principle purpose of the Act is to provide legal equivalence between paper and electronic documents and signatures, except in limited circumstances.

Identity management consists of a number of processes that include:

- registration and issuing of electronic identities and credentials;
- identity proofing - how government proves an individual is who they claim to be;
- authentication - how government knows a user is who they claim to be when accessing services online;
- authorization - decisions about what services an individual is eligible for; and
- access controls - controls around what information a user will see and how users' views will be managed.

Policy

a) Electronic Signatures

1. Ministries must consider the benefits of using electronic signatures in all e-service initiative designs, and choose the manner of signature(s) that best serves the initiative.

b) Identity Management

1. All users must have a unique application user logon profile.
2. Government e-services requiring user authentication must use the Enterprise Security Gateway for authentication, unless an exemption has been granted by the Government CIO.

12.3.5 Information Technology Management

Objectives

- Promote the principles and best practices of project management in all information and technology projects.
- Provide a context for overall government direction within which ministries can establish their information and technology architecture directions.
- Maximize information technology system to system and human to system interoperability.
- Maximize effectiveness and efficiency of information technology implementation and operations.
- Encourage compatibility and supportability across the government's information and technology environment.
- Lower service costs to government through effective information technology procurement practice.
- Optimize the use, performance and cost of information technology resources.

General

In British Columbia government strategic direction includes a commitment to integrate services and to deliver them electronically where possible. This strategy supports a client centric framework that will assist and enable ministries to deliver services better through improved access to business and citizen online services.

Professional project management is the basis for developing sound strategic and operational information and technology initiatives. Project management includes incorporating best practices, standards and proven methodologies to foster a consistent formal approach that maximizes success in information and technology initiatives.

Corporate information technology standards serve as a "building code" to provide client centered services regarding interoperability, efficiency, security and privacy while recognizing that the least amount of regulation promotes innovation and where appropriate, competition. This will result in some standards being high-level (e.g., statements of best practices, industry standards, and recognized leading methodologies) while others, of necessity, will be at a lower level (e.g., services, products, or tools).

The purpose of corporate shared services is to employ best practices in cost control, optimizing return on investments, implementing standardization and improving the effectiveness and efficiency of services, products and tools. The Government CIO has authority to identify where a corporate approach should be used in planning for shared services, new initiatives and procuring information and technology assets. (see CPPM Chapter 6, section 6.3.5 a, Information Management and Information Technology Procurement).

Evaluations provide assurance to Treasury Board, the Government CIO and senior ministry management that information technology best practices, policies, standards and guidelines have been implemented and are functioning effectively across government. Routine evaluation of information technology is a change management methodology that impacts daily operations, service delivery planning, modifying existing systems or implementing new systems, and forms a key component of Enterprise Risk Management feeding into the annual business planning cycle.

Policy

a) Information and Technology Project Management

1. Responsibility for the management and control of information and technology projects resides with executive-level program management through the annual IRMP process.
2. Ministries must select a methodology for the development of information systems appropriate for the size, complexity, nature and cost of the development project.
3. A Project Steering Committee must be established to provide direction and decision making for any high-risk major development project.
4. Major information and technology projects must be monitored against a documented master project plan.
5. Post Implementation Reviews must be done on all major projects.
6. Development of information systems must be conducted by the private sector unless an exemption is granted by the Government CIO.
7. Information system application plans that will use or interface with a shared computer facility or service must include a government-wide approach and, where available, use shared services to achieve economies of scale in the use and management of information and technology.
8. Development of new financial systems or enhancements, changes or revisions to existing ones must be formally approved in accordance with CPPM chapter 13, Financial Systems and Controls.
9. Development of new electronic commerce systems or enhancements, changes or revisions must be formally approved by Banking and Cash Management to ensure compliance with payment card industry (PCI) standards.

See CPPM chapter 7, section 7.3.8 - Acceptance of Electronic Payments, and the IM/IT Standards Manual.

b) Information Technology Standards

1. Standards and exemptions from published standards, must be approved by the Government CIO.
2. Standards must support the efficient, secure operation of systems while maintaining privacy.
3. Standards must provide the least amount of regulation to promote innovation and competition, where appropriate.

4. Standards must maximize effectiveness and efficiency for information technology planning, design, implementation and operations.

c) Information and Technology Procurement and Unsolicited Proposals

1. Government-wide approaches and standards must be used in information and technology asset procurement and in managing unsolicited information and technology proposals by vendors.

See CPPM chapter 6, section 6.3.5, Information Management and Information Technology Procurement.

d) Information Technology Operations and Evaluation

1. Ministries, in conjunction with Workplace Technology Services, must establish and maintain inventories of computer hardware, software and related communications equipment.
2. Ministries must identify a funding source in the annual ministry information technology plan for the evaluation of compliance, system or security controls identified for a project, system or application.

See CPPM chapter 8, Asset Management and chapter 20, Loss Management.

12.3.6 Information and Technology Security

Objectives

- Ensure appropriate security measures are established for all data, information, applications, hardware, associated documentation and computer facilities.
- Support incorporation of privacy principles in the design of information systems.
- Support access to data, software and computer facilities, based on demonstrated need and authorization.
- Ensure information is viewed and managed as an asset that must be protected commensurate with its value.
- Select only those vendors who will undertake to comply with the security policies of this chapter when contracting for data processing services or engaged in alternate service delivery initiatives.

General

Security is the responsibility of all employees, contractors and others who have access to, use or manage the information and technology assets of government. Information systems security includes the protection of personal data, systems, documentation, computer-generated information and facilities from accidental or deliberate threats to confidentiality, integrity or availability. Security policies apply to all locations where information is processed or stored by, or on behalf of government (e.g., Workplace Technology Services, ministry and contracted computer facilities).

Policy

a) Security

1. A formal management framework will be established to initiate, implement, monitor and enforce information and technology security within the Government of British Columbia.
2. Security requirements must be assessed, identified and documented to determine security implications and control requirements when there is a requirement for third parties to access government assets. Security controls must be documented and agreed to with the third party.
3. Information and technology assets must be classified, inventoried and recorded with an identified owner who is responsible for achieving and maintaining appropriate protection of those assets.
4. Users of government assets must continue to be aware of, and understand, their role in reducing the risk of theft, fraud or misuse of government assets. Changes in responsibilities, roles, contracts or employments must be managed.
5. Operating procedures must be documented and monitored to ensure the correct and secure operation of information and communication technologies.

6. Third party service delivery agreements must be monitored for compliance, and changes managed to ensure that the services delivered meet or exceed specified requirements.
7. Operational requirements for new systems must be established, documented and tested prior to acceptance and use. Future capacity requirements should be made to reduce the risk of system overload or failure.
8. Documents, computer media, data and system documentation must be protected from unauthorized disclosure, modification, removal or destruction.
9. Data and information exchanges within government, or with an external entity, must be secure and managed through a documented process.
10. Government information and technology assets will be monitored regularly and logs maintained to identify inappropriate access, use, or other security events.
11. Access to information, systems, and business processes must be managed and controlled on the basis of business and security requirements.
12. Access to, or from, internal and external networks and network services must be managed and controlled.
13. Security requirements must be assessed, identified, documented, and agreed to during all stages of development.
14. The security controls of new or modified information systems and services must be reviewed prior to implementation.
15. Information and technology assets will be protected commensurate with the identified risks and security requirements.
16. Information security incidents, events and weaknesses must be managed and communicated to the Government Chief Information Officer for corrective action, if appropriate.
17. Information security management requirements must be integrated into the business continuity planning process to protect information systems and communication technologies from disasters, loss of service or information security failures.
18. The security of information systems and communications technologies must be regularly reviewed to ensure compliance with applicable legislation, policies, standards and documented security controls.

See CPPM chapter 15, Security and CPPM M, Loss Reporting, and the Information Security Policy Manual.

12.4 Information and References

12.4.1 Definitions

Administrative Records Classification System (ARCS) – The government-wide standard for classifying, filing, retrieving and disposition scheduling of administrative records. ARCS also includes freedom of information and protection of privacy designations. ARCS is a block numeric system, reflecting function and subject. See also ORCS.

Application – A collection of computer hardware, computer programs, databases, procedures and knowledge workers that work together to perform a related group of services or business processes.

Attorney General's discovery of documents – A demand for discovery of the documents which are or have been in the party's possession or control relating to any matter in question in the action, and the other party shall comply with the demand by delivering a list of the documents that are or have been in the party's possession or control relating to every matter in question in the action.

Basic format information – information used by the originating ministry to conduct its business. Examples could include raw data or value-added information in either electronic or hard copy formats.

Computer media – An object or device that electronic information is stored on. It includes, but is not limited to, tapes, disks, diskettes and computer hard drives.

Court ordered for Demand of Discovery – The court may order that a party deliver a list of the documents that relate to a matter in question in the action to any other party and that, although not in the possession or control of the party against whom the order is made, are within that party's power.

Data – The data that is an individual fact (datum) or multiple facts (data), or a value, or a set of values, but is not significant to a business in and of itself. Data is the raw material stored in a structured manner that, given context, turns into information.

Data Custodian – A senior manager for a business area responsible for data requirements, standards, access rules, business training, etc. They define the business value, scope, standards and services of the organization's data within the context of their mandate.

Electronic Signature – Information in electronic form that a person has created or adopted in order to sign a record and that is in, attached to, or associated with, the record.

Government – Any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of British Columbia.

Government records – All records, regardless of physical format, that are received, created, deposited, or held by or in any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of British Columbia.

The Interpretation Act (RSBRITISH COLUMBIA 1996, c. 238, s. 29) defines "record" as follows: "'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."

Government records consist of records in every physical format, including electronic records, film, audio and audiovisual tapes.

Government records include cabinet ministers' records that are created and/or accumulated and used by a minister (or a minister's office) in developing, implementing and/or administering programs of government. Government records do not include legislative records.

The retention and final disposition of most government records is governed by the Document Disposal Act. See also Executive records, MLA records, Non-government records, Personal records.

Host Name – Any name that is included in an email ID that can be used to identify the network address of a computer.

Information – The data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision-making. The finished product as a result of the interpretation of the data.

Information and Technology Resources – Information and communications technologies, including data, information systems, network services (e.g., web services; messaging services); computers (e.g., hardware, software); telecommunications networks, and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants).

Information Management – The application of systematic planning, controls and standards to the creation, use, transmission, retrieval, retention, conversion, final disposition, and preservation of information resources in all formats, and the improvement of information handling systems of all kinds.

Information System – A system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output and control functions in relation to information and data. Normally used to describe computerized systems, including data processing facilities, data base administration, hardware and software which contain machine-readable records. A collection of manual and automated components that manages a specific data set or information resource.

Information Technology – The common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services.

Internet – The global interconnection of data networks or bulletin board systems that commonly use (but are not limited to) the Internet Protocol.

Least Privilege – A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Major Project – A project that is over six months duration or identified as high risk or cost greater than or equal to $250,000.

Master Project Plan – A document that describes the common vision of the project, the overall project management functions, specific deliverables and establishes the detailed project workplan and budget.

Need-to-know – A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office.

The need-to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on automated information systems.

The need-to-know principle is especially important in protecting the privacy of individuals as required by the *Freedom of Information and Protection of Privacy Act*.

Ongoing records schedule – A records schedule that authorizes the retention and final disposition, on a continuing basis, of the types of records described in the schedule. ARCS and ORCS serve as ongoing records schedules for ministry or agency administrative records and operational records. Special records schedules are another type of ongoing records schedules.

Operational Records Classification System (ORCS) – An integrated records classification and scheduling system tailored to the operational records of a specific function or program of government, in accordance with government-wide standards. ORCS facilitate classification, filing, retrieval and disposition; ORCS may also be used to identify vital records and freedom of information and privacy designations. ORCS is a block numeric records classification system, reflecting function and subject.

Originating ministry – The ministry or agency which is the prime or original holder of the information.

Payment Card Industry (PCI) Standards – payment systems standards issued through the international Payment Card Industry Security Standards Council and required by the payment card industry.

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.

Requesting ministry – The ministry or agency requesting information from the originating ministry. This policy will use the term "information" to encompass raw data, summaries, abstractions, consolidations and other products derived from data.

Routine Release – The disclosure of certain types of information as a matter of course without the necessity of a formal Freedom of Information (FOI) request. Routine release includes, but is not limited to, the release of records that have been designated as available without a formal request under section 71 of the Act. Routine release may be reactive (responding to requests for information when received) or proactive (systematically disseminating information in advance of requests using mechanisms such as the Internet, libraries, etc.).

Security event – An identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

User – Persons (including employees and contractors) authorized to access and/or use government information technology resources.

Vital Records – The records of government that contain information essential to:

- conduct of emergency operations during and immediately following a disaster;
- resumption/continuation of government services or operations;
- re-establishment of the legal, financial and functional responsibilities of government; and
- re-establishment of the rights and obligations of individuals, corporate bodies and other governments with respect to the Government of British Columbia.

12.4.2 Links

The following links will provide the reader with additional details and guidelines from the Office of the Government CIO

information management and information technology policies and standards, directives and memos, key support manuals and information technology security.

1. Legislation
    a. *Freedom of Information and Protection of Privacy Act* and Freedom of Information and Protection of Privacy Regulation (B.C. Reg. 323/93)
    Personal Information Protection Act and Personal Information Protection Act Regulations (B.C. Reg. 473/2003)
    Electronic Transactions Act
    b. *Document Disposal Act*

2. Branches

Knowledge and Information Services Branch
http://www.cio.gov.bc.ca/cio/kis/index.page?/

Freedom of Information and Protection of Privacy Policy and Procedures Manual
http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page?

IM/IT Supplemental Manual (currently under revision)
http://www.cio.gov.bc.ca/local/cio/about/documents/cpm12.pdf

Information Security Branch
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page?

Information Security Policy Manual
http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf

Information Access Operations
http://www.gov.bc.ca/citz/iao/records_mgmt

Recorded Information Management Policy and Procedures Manual
http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual/index.html

Provincial Treasury Banking/Cash Management - PCI DSS Resource Centre
http://gww.fin.gov.bc.ca/gws/pt/bcm/bankPCI.stm

Ministry of Finance

Financial Systems and Controls

Table of Contents

13.0 Financial Systems and Controls
- 13.1 Objectives
- 13.2 General
- 13.3 Policy
- 13.4 Information and References
  - 13.4.1 Approval
  - 13.4.2 Risk and Controls Review

13.1 Objectives

- ensure that financial and other systems are developed and implemented with due consideration to system development principles, generally accepted control and security standards, and are consistent with government business and systems strategic direction

13.2 General

Financial systems are a vital component in the delivery of government programs and services. When managed effectively, financial systems improve service to the public, enhance productivity and reduce costs.

Roles and Responsibilities

Ministries are responsible for their financial systems and ensuring compliance with policy and technology standards.

The Office of the Comptroller General is responsible for policy for financial systems and communication of control standards.

13.3 Policy

A financial system is any system that is used to exercise financial management, control and accountability over public monies or assets. Included are those systems (manual or automated) that are used to record, verify, report, generate and/or execute financial transactions, and those used for the management and control of assets, liabilities and assets held in trust.

1. Ministries are responsible for determining the methodology to be used in the development of financial systems. The methodology used must be consistent with government information technology and payment card industry (PCI) standards (see Risk and Controls Review for guidance).
2. Ministries must ensure that financial systems have sufficient and comprehensive controls to prevent and reduce the risk of loss, error, misuse or fraud to an acceptable level.
3. A risk and controls review must be performed and documented for a new financial system, and whenever there are significant modifications to an existing financial system. Qualified, independent and objective parties must carry out the review.
4. The scope of a risk and controls review depends on the nature and complexity of the financial system. A comprehensive review includes project management, systems development, general environmental controls and application-based controls (see Risk and Controls Review).
5. A financial system must receive executive financial officer approval prior to being placed into production. The executive

financial officer on the recommendation of the chief financial officer must approve implementation of a new financial system and significant enhancements to an existing financial system.

6. The ministry's executive financial officer, or chief financial officer where delegated, has overall responsibility for the ongoing operation of financial systems.
7. Ministries that require a financial system to interface with other systems must establish proper and integrated processes to secure financial information.
8. Where the financial system interfaces with the Corporate Accounting System (CAS), agreement must be established between the ministry and CAS that interface requirements have been tested and are working correctly before the system is moved into production.
9. For a financial system that interfaces with CAS, a copy of the financial system's risk and controls report must be made available to the Office of the Comptroller General (OCG) on request.
10. Ministries and central agencies are responsible to ensure that public facing payment services are developed in compliance with Payment Card Industry Data Security Standards and Provincial Treasury Banking Cash Management's approval process. Reference Acceptance of Credit Card Payments: PCI Compliance Standards Roles & Responsibilities

    Electronic Commerce Systems

    - Banking/Cash Management Branch, Provincial Treasury, determines and approves the standard suite of electronic payment options based on program type, delivery models for government, and payment card industry standards.
    - Electronic commerce systems must be tested and approved by Banking/Cash Management Branch, Provincial Treasury to ensure that adequate security and process standards are maintained including safeguarding identity information, the integrity and non-repudiation of transactions and data storage, retention and use.
    - Ministries must ensure that electronic commerce systems comply with the requirements of Banking and Cash Management, Provincial Treasury to prevent, remediate, and address identity theft and/or identity fraud incidents.
    - Third party service delivery agreements that support or include an electronic payment system for government, must comply with Banking/Cash Management Branch, Provincial Treasury requirements.
    - People who manage access to, or administer, electronic commerce systems must receive training on: safeguarding identity information obtained through e-commerce systems and processes; preventing identity theft and fraud; and responding to actual or suspected data or payment application or system compromises.
    - The Comptroller General is responsible for the PCI Incident Response Framework, which includes representatives from the Office of the Chief Information Officer.
11. Ministries must ensure financial system documentation is sufficient in detail to enable effective system maintenance and compliance requirements. This documentation must be completed prior to system implementation.
12. Ministries must establish and maintain an inventory of their financial systems. The inventory must be updated annually to capture any additions or changes, and be made available to OCG upon request.
13. Ministries must ensure that senior management approvals for accepting a new financial system, or a significantly modified system, are documented and retained (see Approval). A copy of the approval document must be provided to OCG upon request.

13.4 Information and References

13.4.1 Approval

System acceptance indicates that the financial system meets minimum control requirements, user objectives and business requirements. The following are approval guidelines for documentation and reporting of ministry financial systems:

- a statement by the chief financial officer, prior to implementation, that adequate system testing, user testing and, where necessary, interface testing has been successfully completed, and user manuals and other documentation are complete;
- approval and acceptance of the financial controls by the chief financial officer;
- approval and acceptance of the system by the executive financial officer. Sign off documentation should also include

project manager and system custodian approvals for the system in meeting business and control objectives, and payment card industry (PCI) standards (where applicable). Any new outsourced payment system must be certified as fully PCI compliant prior to deployment.

13.4.2 Risk and Controls Review

The risk and controls review requirements are outlined below. The risk and controls report should be attached to the ministry's financial system sign-off sheet.

I. General

A risk and controls review is a formal analysis of a financial system and the environment in which it operates. The objective of the review is to determine whether a system includes adequate controls to mitigate business risks. As part of the review, deficiencies in the system's ability to meet business risks and control objectives should be documented for redress.

II. Risk and Controls Report

The risk and controls report is a document that describes the overall assessment of a financial system, the controls and any deficiencies to support the overall assessment. The report should contain:

- a description of risks, the significance of a risk to the business, a description of the control and an assessment of the adequacy of each control for the risk identified, to assist in the overall evaluation; and
- an action plan to correct major deficiencies, including the date when the problem will be corrected and any follow-up required.

Risk Identification:

Identification of business and information technology risks, and any factors that will influence the risk assessment.

Risk factors that should be considered:

- the susceptibility of business assets to fraud or misappropriation;
- complexity of business transactions or degree of reliance on the system to account correctly;
- the degree of manual intervention and related potential for error involved in the system;
- decentralization of systems and complexity of user security profiles;
- interfaces with any third party systems; and
- reliance by the business on the continuing availability of the system.

Controls:

Some control areas to consider to support project management / systems development, general environmental and application based controls follow. Note that this is not a complete list:

a. System development should be based on clearly understood needs that are consistent with meeting government and ministry strategic objectives, including review of existing government systems to assess potential suitability.
b. Ministry senior management should support and be actively involved in the planning and use of information resources, and the development and implementation of new financial systems.
c. The project management team should be assigned clear roles and responsibilities. The team should have a sufficient level of authority and an appropriate mix of skills and experience to manage the project.
d. Ministry users should support development by actively planning and participating in defining requirements, and in verifying that the system meets their needs.
e. The design specifications should accurately and completely summarize user requirements.
f. The systems environment security design should be supported by a security threat and risk assessment.
g. User test and acceptance procedures to determine whether a project resulted in a specified application or level

of performance need to be conducted and documented.

h. Access to financial systems and applications should be restricted to only those staff whose responsibilities require the access. Also, require separation of incompatible functions, for example, custody of assets and access to asset data records.

i. Input validation to ensure data entry is authorized, accurate and complete.

j. Processing checks to ensure that all transactions are processed properly.

k. Output reviews to ensure the completeness, accuracy and validity of reported information and the adequacy of audit trails.

l. System interfaces that are designed and tested to protect the integrity of data exchange.

m. Applications that are fully understood by staff and comply with the ministry's information resource management plan.

n. Applications that are routinely monitored and properly evaluated.

o. Physical security to provide an environment that protects hardware and software from damage by unauthorized access and elements such as water, extreme temperatures and fire.

p. Back up of data and offsite storage for system operation recovery.

q. Recovery of computer operations in the event of a disaster.

Note: Additional guidance on information system controls and risks can be obtained by contacting Internal Audit and Advisory Services, OCG: Phone 250 387-6303.