System Security

Objective

The objective is to outline the system security required for financial systems.

Authority

The Financial Administration Act, 1993, clauses 5(a), 5(c), and 5(e), subsection 10(2), and sections 22 and 28

Applicability

This policy applies to the General Revenue Fund, and special purpose funds and trust money that are administered by ministries. See Appendix C Public Money.

Treasury Board Policy

.01 Ministries are to incorporate adequate security features into financial systems to prevent unauthorized access to the system.

.02 Ministries are to maintain an appropriate capability to restore records and processing capability after a processing interruption from system failure or from a disaster which causes destruction of a critical system component.

Provincial Comptroller Directives

.03 Ministries are to ensure data files, programs, forms and hardware facilities are adequately secured to ensure completeness, accuracy, authorization and validity of files and programs. Ministries may use the following techniques:

- Identify sensitive data files and programs and protect them to an appropriate level of security.
- Use software and hardware firewalls to restrict access to assets, computers and networks by external persons.
- Implement virus protection and update it regularly to protect against viruses and malicious software.
- Establish a security profile for each user that details the information access and transaction processing permitted and complements the appropriate segregation of duties. The security profile is updated when personnel or job duties change.
- Use security passwords to control access to computer files and programs with the system periodically and automatically requesting password changes.
- Restrict access to critical forms (e.g., special paper for cheques) to authorized personnel responsible for the initiation function.

- Restrict access to systems security software and related documentation to authorized personnel.
- Ensure documents, reports and files are placed in adequate storage facilities when not in use and sensitive data is locked up.
- Ensure hardware facilities are physically protected from unauthorized access and deliberate loss or damage.

Service Bureau Security Guidelines .04 Ministries are to ensure the requirements of Treasury Board policies and Provincial Comptroller's directives are met when using an information technology service bureau. Contracts with an information technology service bureau should specify adequate security requirements. The contract should require the service bureau to notify the ministry of any changes in the manner in which they are meeting the ministry's requirements.

Service Bureau Contract .05 Security requirements included in a contract with a service bureau may include:

- organization security controls and administration for development of policies and procedures to protect facilities, operations and information;
- system access controls for authorizing users and following up unauthorized access and security violations;
- system software controls over development, testing, implementation and documentation of new software and software modifications;
- data communications controls over access and changes to the data communications network through dial back procedures;
- facilities controls restricting access to facilities, physical security (smoke and moisture detectors, air conditioning) over hardware, software and files, proper disposal of confidential waste;
- computer operations controls to prevent/detect processing errors and unauthorized changes;
- personnel controls over segregation of duties, supervision and procedures for hiring, training and terminating employees;
- backup, storage, recovery controls and contingency plans including manual operations;
- resource list of alternate service bureaus capable of handling information processing;

- time frame for restoration of processing applications;
- virus protection;
- insurance protection program of the service bureau (although alone, insurance is not deemed to be protection); and
- other controls as deemed necessary and documented in the contract.

.06 The contract with the service bureau should provide for periodic independent security reviews of the service bureau every three years, with an internal memorandum annually. The security review may involve:

- the service bureau providing the ministry with an independent security audit report; and/or
- the ministry conducting their own review, either through internal staffing or hiring a third party.

A single audit of a service bureau whose services are contracted by several ministries will be satisfactory.

.07 Ministries should receive a copy of the contracted service bureau's financial statements and auditor's reports annually.

.08 The above list of requirements may be included in the standard Request for Proposal package, as minimum requirements for doing business with the Government, when tendering for service bureau services.

Disaster Recovery

.09 Ministries should ensure that critical business processes can be resumed after operations have been interrupted. The following techniques are used:

- All information and resources required to resume processing are backed up and stored off site. There should be sufficient off site backup storage of critical systems, data, transactions, files, supplies, documentation and special forms required to allow users to resume operations in the event of interruption.
- Prepare, maintain and periodically test a disaster recovery plan which documents actions to be taken to restore processing on a timely basis. Include procedures in this plan to:

- identify data that has been lost in a processing disruption;
- restore and maintain alternate processing; and
- recover processing at the original site.

.10 Ministries are to consider the degree of criticality for restoration of system processing in determining an acceptable time frame for restoration of system processing. Critical financial systems are those for which a disruption in processing would result in an impairment in the ability to manage financial resources, assets or liabilities under the ministry's control. Critical financial systems are those where senior management responsible for the system believes that a system disruption would result in one or more of the following:

- loss of substantial revenue or a prolonged delay in collecting revenues;
- significant adverse effect on cash flow;
- inability to produce management or financial information essential to managing a program;
- inability to obtain essential goods or services or make required payments;
- inability to meet legislative requirements;
- substantial idle staff; and/or
- inability to process a backlog when processing is restored.

.11 Critical financial systems must be capable of being restored to operation either through access to an alternate processing facility or through alternate means such as the implementation of a manual system on a temporary basis.

.12 Non-critical financial systems are subject to a less stringent requirement to restore processing. It may be acceptable to implement a totally manual backup system or to discontinue processing for a period of time, if the consequences are not significant.

.13 The permanent head of the ministry approves the disaster recovery plan.

.14 Personnel are to receive adequate training and supervision in emergency backup and recovery procedures.

.15 Ministries should document the required organizational responsibilities to regain normal operation on a timely basis and store it off site.

.16 Ministries are to identify applications that will be given top priority in reconstruction.

References

4000 Financial Systems
4005 Acquisition of Financial Systems
4010 Development of Financial Systems
4015 Implementing Financial Systems
4020 System Processing Controls
4130 Internal Audit Guideline

IT Security Services (ITD)