Government of Yukon
Information Technology Security Framework

Table of Contents

1 Introduction and Background

This framework document was prepared in response to the growing awareness of the importance of information technology (IT) security. The Auditor General has, on several occasions, identified the lack of a formal IT security policy or framework within the Government of Yukon (the "government").

This framework document was reviewed and endorsed by the Information Resource Management Committee on February 21, 2006.

IT security is defined as the:

> *"safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information."*

For the purposes of the government, the term 'IT security' will also include the safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store or dispose of information electronically.

The International Standards Organization (ISO) Guidelines for Management of Information Technology Security (ISO 17799) are used as the government's standard reference and model for the development and implementation of this IT security framework.

2 Purpose and Objectives

The purpose and objectives of the government's IT Security Framework are to:

- protect government and public information, government assets and employees;
- define reasonable high-level IT security measures to foster confidence in electronic service delivery and meet legal and practical business obligations;
- aid the development of detailed policies, procedures, guidelines and standards, for specific IT equipment, networks, systems, and applications; and
- identify the requirements and responsibilities covering the security management of the IT systems within the government.

3 Scope and Application

All government departments, corporations and business partners connected to and making use of government IT equipment, networks, systems and applications must adhere to the requirements of this framework.

Corporations and business partners will adhere to this framework through the acceptance of the terms and conditions of relevant service agreements.

4 Roles and Responsibilities

4.1 Highways and Public Works, Information and Communications Technology (ICT)

ICT is a branch within the Department of Highways and Public Works responsible for developing the government IT Security Framework as well as:

- Corporate Security Architecture
- Drafting security policies, procedures, guidelines and standards for review by the appropriate committees or groups
- High-level risk assessments and security awareness programs
- Communicating with national counterpart organizations regarding IT security issues and industry best practices

ICT is responsible for all IT security measures outlined in this framework unless responsibility for any specific aspect of IT security has been specifically delegated to a department or assigned to a corporation per sections 4.3 and 4.4 below.

ICT has the authority to:

- Approve or reject any changes in government IT equipment, networks, systems, applications or procedures that affect IT security
- Review any government IT security violations

ICT is responsible for ensuring the effective and efficient management of the government's information infrastructure and IT assets. Given the potential negative impact of service delivery failures due to security breaches, ICT together with all departments and corporations must work collaboratively to ensure that appropriate security measures are applied to all government IT activities.

4.2 Information Resource Management Committee (IRMC)

As defined in GAM Directive 2.3, IRMC has the role to "develop and co-ordinate the corporate view on the management and integration of information resources by providing a vision of affordable, accessible, and responsive IT that invests in the strategic needs of the government to deliver services". This role includes responsibility for endorsing this high-level IT security framework document.

4.3 Departments

Deputy Heads are accountable for some elements of IT security within their own departments. Deputy Heads may appoint an individual responsible for ensuring

that all government security policies, procedures, guidelines and standards are adhered to within their respective departments.

4.4 Corporations

Corporations will adhere to this framework through the acceptance of the terms and conditions of relevant service agreements.

Corporations may choose to initiate independent third party IT security audits of shared government IT equipment, networks, systems and applications provided proper notice is given and any findings or reports are shared with ICT.

4.5 Employees

All government employees are required to adhere to the terms outlined in the Government of Yukon IT Security Framework, and all government security policies, procedures, guidelines and standards.

Employees are responsible for making every reasonable effort to protect government IT equipment, networks, systems, applications, and information.

4.6 Business Partners

Business partners include but are not limited to, individuals in the private sector, agencies, NGO's, other authorized users and all other governments connected to and making use of government IT equipment, networks, systems and applications.

Business partners are responsible for safeguarding their own equipment and ensuring their hardware and or software causes no harm to government IT equipment, networks, systems, applications, or information.

Business partners are responsible for safeguarding any government equipment and the information in their custody, or used in performance of their duties.

5 Security Assessments and Audits

Security risks to information and IT assets must be continuously assessed and managed throughout the life of their programs and services.

Security assessment and audits include activities such as:

- Threat and Risk Assessments;
- Privacy Impact Assessments; and
- IT Security Audits.

5.1 Threat and Risk Assessments

A Threat and Risk Assessment provides the justification for IT security risk management decisions. IT Security measures above the regular procedures must be applied when justified by a Threat and Risk Assessment.

Threat and Risk Assessments should be conducted for every program, system or service.

If significant changes are made to programs, systems or services, Threat and Risk Assessments must be updated.

5.2 Privacy Impact Assessments

The Privacy Impact Assessment is both a due diligence exercise and a privacy and security risk management tool. Privacy breaches can be either real or perceived. Both real and perceived breaches can seriously damage the government's reputation and relationship with the public and potentially cause harm to an individual whose personal privacy is breached.

If a new system or enhancement deals with the collection, storage, use, or disclosure of personal information, a Privacy Impact Assessment is recommended. A Privacy Impact Assessment can be especially important if the IT project or enhancement involves sensitive information or information shared with other governments.

5.3 IT Security Audits

System performance must be continuously monitored to detect risks such as unauthorized usage or potential attacks.

If auditing reveals an anomaly, it must be determined whether the cause is a security incident, a hardware or software problem, or an increase in client demand.

A security audit log function must be included in all IT systems. Audit logs must be reviewed regularly for unusual activity. Automated, real-time, incident detection tools must be incorporated into systems that are critical or that contain highly sensitive information.

6 Access Controls and Measures

6.1 Authorization and Access Controls

Appropriate access controls must be in place for all IT systems. Access controls deal with identification, authentication and authorization and are applied at different layers such as network, operating systems, application and data.

Access to sensitive or confidential IT systems must be limited to those individuals who require specific access to fulfill their job requirements.

Users must ensure that the threats and vulnerabilities of networks and systems they plan to connect to do not adversely affect the security of government IT equipment, networks, systems, applications or information.

Connections to the internal government network must be controlled and must be limited to managed, secured systems that are subject to the same controls and policies as the government internal systems. Verification of remote security must take place prior to accessing the government network.

All network access requirements to or from third parties will be provided through a controlled access point. No other access points are allowed.

6.1.1 Identification

All individuals who require access to protected IT systems must be uniquely identified to allow for accountability of usage and actions.

Authentication techniques should validate the identity of all users and be consistent with the value and sensitivity of the information and potential risks.

6.1.2 Authentication

Users are responsible for safeguarding their passwords and other authentication mechanisms.

6.1.3 Authorization

Procedures must be in place for authorizing access to and use of IT equipment, networks, systems, applications and information.

Unauthorized users must be denied access and all failed attempts must be logged.

6.2 Security Zones

A Security Zone is an area or grouping within which a defined set of security measures are applied to achieve a specific level of security.

Zones are used to group together information and IT systems with similar security requirements and levels of risk, and to ensure that each zone is segregated from another.

The sensitivity of the information and IT systems governs the definition of, and access to, each zone.

All government IT equipment, networks, systems and applications will be categorized into appropriate security zones.

6.3 Equipment Classification and Controls

An equipment database and/or inventory should be maintained and kept up to date. This inventory should detail specifics about equipment such as: type, make, use, location, ID, security level, accessibility, connected systems, physical and environmental protection, etc.

Based on their asset value and/or the programs they host, access to specific types of equipment must be restricted. System critical equipment will be classified as such and only qualified, specific personnel will be authorized to have both physical and virtual access.

Electronic equipment, systems and media should be physically protected from: unauthorized access, theft, fire, flood, loss or fluctuation of power, and other hazards.

7 Operational Management of IT Security

7.1 System Planning and Acceptance

The implementation of all new systems should include documentation of: threat and risk assessment, privacy impact assessment and any unique specified security requirements. An end-to-end IT security review must take place and any new system must meet all existing security policies, procedures, guidelines and standards. All systems must be tested and meet the documented IT security criteria prior to implementation.

7.2 System Integrity

All systems must be properly tested, configured and regularly maintained by qualified personnel.

All essential software and information should be regularly backed up.

Only trusted and known sources of software should be used. This will reduce the threat of unintended functioning errors and protect against malicious software, such as viruses and hidden scripts that compromise security.

Practices and controls, such as scanning for unauthorized software, strengthening network and system defenses, monitoring and security auditing, should be in place.

7.3 Change Management

A formal change management and change control process should be implemented. Part of this process should include a review and analysis of any proposed system changes to ensure security is not compromised.

Controls must exist to ensure that any additions, modifications or removal of elements of the IT infrastructure are authorized, approved, tested, and documented.

7.4 Disaster Recovery and Business Continuity

In the event of an interruption of services, procedures must exist to recover the IT infrastructure and enable the processing of critical applications to recommence on a timely basis. These procedures must be documented, tested, and proven workable.

These procedures and their documentation should be periodically reviewed and updated as necessary.

A procedure should also be established for the communication of system threat and disaster situations, including the notification to the appropriate operational staff, managers and all other affected parties. Individuals listed as contacts and their contact information must be regularly updated.

7.5 Security Incidents

All security incidents must be reported as soon as possible to the appropriate security contact.

A single point of contact or designated group should be responsible for fielding all reports of incidents.

Security breach response procedures must be documented and followed in order to mitigate damage, contain the cause of the incidents and restore services.

Procedures can include incident investigation, isolation or disconnection of the system and or recovery of affected systems.

For every major IT security incident that occurs, a post-incident analysis should be performed and a report prepared outlining the chain of events during the incident, including:

- the time when the incident was detected;
- the actions taken;
- the rationale for decisions;

- details of communications;
- management approvals or direction; and
- external and internal reports.

7.6 Security Audit Information and System Logs

The confidentiality, integrity and availability of security log data must be protected. Access to sensitive security log data must be strictly controlled, and individuals with such privileged access must be aware of their legal and policy responsibilities. Privacy must be respected when handling, retaining, and sharing personal information gathered as part of logging security data.

Retention requirements for audits and security data logs should be based on program requirements, government legislation, and specific policies.

7.7 Disposal of IT assets

Procedures should be in place to ensure IT security is not compromised during the disposal of equipment, software, and/or information.

8 Security Framework Implementation

8.1 Potential Topics to be Covered by Other IT Security Documents

The following are *examples* of potential topics that will be covered in policies, procedures, guidelines and standards:

- General Standards and Best Practices for IT Security
- Glossary of IT Security Terms
- Identification of Strategic or Critical Infrastructure and Systems
- Information Sharing Agreement Guidelines
- Security Incident Procedures
- Security Zone Standards
- Computer Use Guidelines
- Threat and Risk Assessment Guidelines
- Privacy Impact Assessment Guidelines
- Business Partner Access
- Usage of Personal Digital Assistants (PDAs), and other Wireless and Portable Devices
- Remote Access Usage

- Website Blocking Standards
- Password Guidelines
- User Agreements
- Compliance with Software Licenses
- Cryptology and Encryption Procedures

8.2 IT Security Document Completion Process

ICT will draft IT security policies, procedures, guidelines and standards. Depending on the nature and scope of these documents, they will be reviewed and/or endorsed by one or more of the following inter-departmental committees or groups: DMRC, IRMC, DALC, PRC, DSMG, HRMAC, and/or SAUG.

8.3 Communication of Security Measures

IT security documents should be widely communicated and available to all government employees, business partners, and all other individuals with access to government information and IT assets.

8.4 Training and Awareness

Government employees, business partners, and all other individuals with access to government information and IT assets must be informed and regularly reminded of IT security responsibilities, concerns and issues.

General IT security awareness should be provided as part of employee orientation. IT security awareness should be incorporated into any general security awareness program.

Specific IT security training should be made available to all individuals with significant IT responsibilities.

8.5 Periodic Review of IT Security Documents

All IT security documents should be reviewed periodically to ensure they are accurate and up to date. The implementation of new IT security documents should be monitored, reviewed and modified as necessary.

In addition to internal reviews, periodic independent reviews of government IT security documents should be conducted.