Ontario

Government of Ontario

Information & Technology Standards

Government of Ontario IT Standard (GO-ITS)

Number 25.7

Security Requirements for Remote Access Services

Version #: 2.3

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

UNCLASSIFIED

Last Review Date: 2015-03-18

Foreword

Government of Ontario Information Technology Standards (GO-ITS) are the official publications on the guidelines, preferred practices, standards and technical reports adopted by the Ontario Public Service under the delegated authority of the Management Board of Cabinet (MBC). These publications support the responsibilities of the Treasury Board Secretariat (TBS) for coordinating standardization of Information & Information Technology (I&IT) in the Government of Ontario. Publications that set new or revised standards provide enterprise architecture guidance, policy guidance and administrative information for their implementation. In particular, GO-ITS describe where the application of a standard is mandatory and specify any qualifications governing the implementation of standards.

All GO-ITS 25 Standards are based on the work of recognized global authorities in information and operational security, both in government and industry.

Copies of cited standards may be obtained as follows:

Intranet: http://intra.net.gov.on.ca/iit/services/iit-policies/

Internet: http://www.ontario.ca/government/information-technology-standards

Summary

The Corporate Policy on Information and Information Technology Security requires that Government of Ontario employees protect information that is received, created, held by, or retained on behalf of, Ontario ministries and agencies. Programs are responsible for the implementation of appropriate safeguards, based on an assessment of the risks involved. Remote Access Services (RAS) provide business advantages but the significant degree of risk associated with such services must be appropriately managed.

Version Control

Date	Version	Author	Comment
June 29, 2005	1.0	Earl Kuntz, CSB	Original ARB approval
April 19, 2006	2.0	Earl Kuntz, CSB	ITSC approved update
October 8, 2008	2.1	Tim Dafoe, CSB	Alignment with consultation and practices, general revisions, adjustment for ISPC, alignment with updated ITSC template, revisions for CSB input, revised authentication strategy, input from Audit and SAWG, final version for ARB
March 14, 2012		Tim Dafoe, CSB	Minor update per document history
June 12, 2012		Tim Dafoe, CSB	Updated GO-ITS references, consultation list
Nov. 15, 2012	2.2	Tim Dafoe, CSB	Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 2.2
Jan. 19, 2015	2.3	Tim Dafoe, SCS	Minor updates per ARB rationale (administrative updates, ISO/IEC alignment),draft document version changed to 2.3

Table of Contents

1. INTRODUCTION

This document is one in a series that defines operational principles, requirements and best practices for the protection of Government of Ontario networks and computer systems.

1.1. Purpose of the standard

This document sets out the security requirements for remote access services (RAS) for the Government of Ontario (the Government). The term *remote access services* as used in this document is intended to refer to any service that provides connections to the Government's computer network for authorized users (or unattended computer systems) that are physically external to the network (see Application and Scope). The objective of this document is to set standards for RAS implementation and operation such that remote access does not result in an unacceptable level of risk to Information and Information Technology (I&IT) resources.

1.2. Versioning and change management

Ongoing ownership and responsibility for maintenance and evolution of this document resides with the Strategy, Planning, and Enterprise Architecture Branch (SPEAB) of the I&IT Strategy and Cyber Security Division (SCS), or a successor division/branch. SPEAB/SCS will provide advice on the interpretation and application of these security requirements and manage any updates to the document when the need arises.

1.3. Contact information

	Contact 1	**Contact 2**
Name/Title	Alex Fanourgiakis, Manager	Tim Dafoe, Senior Security Policy Advisor
Organization/Ministry	Ministry of Government and Consumer Services	Ministry of Government and Consumer Services
Division	Cyber Security Division	Cyber Security Division
Branch	Cyber Security Strategy, Risk Management & Architecture Branch	Cyber Security Strategy, Risk Management & Architecture Branch
Section/Unit	Security Policy and Standards Unit	Security Policy and Standards Unit
Office Phone	(647) 982-5216	(416) 327-1260
E-mail	Alex.Fanourgiakis@ontario.ca	Tim.Dafoe@ontario.ca

1.4. Terms

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	The requirement is mandatory. Without it, the system is not considered secure.
Should	The requirement ought to be adhered to, unless exigent business needs dictate otherwise and the full implications of non-compliance are understood. All exceptions are to be documented and approved in writing by management, identifying the rationale for the exception to standard practice.

1.5. Application and scope

GO-ITS 25 security requirements apply to all ministries of the Government of Ontario, any provincial agencies that use a ministry's or I&IT Cluster's information and information technology infrastructure, and all third party individuals and organizations that connect to the government of Ontario integrated network and use computerized devices for Government purposes unless exempted in a Memorandum of Understanding.

Additionally, these requirements apply to any other new or existing agencies designated by Management Board of Cabinet as being subject to such publications. Further included is any agency which, under the terms of its Memorandum of Understanding with its responsible Minister, is required to satisfy the mandatory requirements set out in any of the Management Board of Cabinet Directives (*cf*. Operational Service, Operational Enterprise, Trust, or Crown Foundation Agencies).

As new GO-ITS standards are approved, they are deemed mandatory for all project development and procurement opportunities. When implementing or adopting any GO-ITS standard or GO-ITS standard update, ministries and I&IT Cluster **must** follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management, risk mitigation, and control selection mechanisms are employed.

For security involving sensitive information[1], if it becomes known that sensitive information is deemed at serious risk then immediate remedial action **must** be taken to mitigate the risk by applying the tools, methods, procedures etc. as per the relevant GO-ITS security document.

Unless stated otherwise in this document, these requirements apply to all categories of RAS users, including:

- Ontario Public Service (OPS) staff and contractors connecting from locations that are not considered part of the managed Government of Ontario network (e.g., home, small remote offices, when in the field, vendor offices, client sites, or a temporary office);

[1] Sensitive information as defined per Information Security and Privacy Classification (ISPC) policy (http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.18.14.34.52.PSU_res/$File/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf).

- OPS Service Delivery Partners working mostly from external organization offices;
- OPS Program Clients with special access working mostly from client sites; and
- Vendors with approved special access requirements.

These requirements apply to all information technologies that support connections to the Government network for individual machines and single users that are outside the managed perimeter boundary of the Government of Ontario integrated network. This includes all types of connections (e.g., fixed circuit, satellite, wireless, POTS dial) and all types of computing devices (e.g., portable computers, mobile devices) used to establish a remote connection.

1.6. Out of scope

These requirements do not apply to:

- Access to applications located outside the managed, internal perimeter of the Government of Ontario integrated network (e.g., public access to web servers intended as Internet sites); and
- Managed broadband links between the Government of Ontario integrated network and external enterprise networks (e.g., the External Network Access or ENA service).

1.7. Principles

These principles are stated in accordance with the Corporate Policy on Information and Information Technology (I&IT) Security:[2]

- Remote access to the Government network provides a means for individuals to access Government applications and/or data from remote locations. However, there are serious security risks inherent in the provision of RAS that **must** be managed.
- Ministries and agencies **must** be assured that I&IT resources are not jeopardized by the provision of remote access to the Government network. This assurance is expressed in terms of accountability, confidentiality, integrity, availability, reliability and opportunity for audit.
- Computing devices used for remote access to the Government network are a *de facto* extension of that network, and as such are subject to Government security requirements. Computing devices used to access RAS **must** be subject to the same secure operating practices as devices connected to networks within the managed network perimeter.
- Users are individually accountable for their actions when using RAS to access the Government network. All corporate and cluster policies regarding the use of IT resources apply to the use of RAS.

[2] The Corporate Policy on Information and Information Technology (I&IT) Security can be found at: http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2011.08.09.10.22.28.JV4_res/$File/corporatePolicyIandITSecurity.pdf

- The implementation of security measures to safeguard RAS does not diminish the need for Program Managers to ensure risk assessments are conducted for each program and appropriate security measures are implemented to protect program applications, information and other resources.

2. REQUIREMENTS

The following security requirements apply to remote access systems:

2.1. Education and training

Technical staff that develop, implement, and/or manage remote access systems **must** be aware of the requirements set out in this document.

All remote access system users **must** be given training on:

- The procedures and best practices that **must** be followed to securely use RAS;
- The Acceptable Use of I&IT Resources Policy and other related OPS policies as they apply to remote access to the Government network and the use of Government-issued computing devices[3];
- The sensitivity of the program information and/or applications as established in accordance with Information Security and Privacy Classification Policy and related operating procedures, and restrictions on the information (e.g., that which may not be stored on remote systems or removed from Government premises);
- Secure processing, transmittal and disposal of sensitive program information when working off-site in accordance with the Information Security and Privacy Classification Policy and operating procedures;
- The security safeguards needed to protect their remote computing device and their responsibilities for ensuring that these safeguards are in place;
- Best practices for RAS users to prevent access to Government information, equipment and/or applications by unauthorized individuals; and
- The procedure for promptly reporting any suspected security compromise as instructed by the I&IT Cluster.

Depending on their activities, RAS users may require additional education and/or training in accordance with other policies and/or best practices (e.g., GO-ITS 25.10 Security Requirements for Mobile Devices).[4]

[3] The Acceptable Use of I&IT Resources Policy can be accessed at http://intra.net.gov.on.ca/iit/wp-content/blogs.dir/842/files/2014/02/acceptableIIT_Policy.pdf

[4] GO-ITS 25 security standards can be found at http://intra.net.gov.on.ca/iit/services/iit-policies/

2.2. User account management

RAS accounts **must** be provided to only those individuals, and automated devices, such as kiosks and public access terminals (PATs), which need remote access to Government applications and/or data to carry out authorized functions, and are approved for such access by the appropriate Program Manager.

Accounts **must** not be shared, and **must** be terminated promptly in accordance with GO-ITS 25.0 General Security Requirements when no longer required. In cases where security concerns exist regarding an employee with RAS privileges (e.g., due to plans for or results of a forensics investigation) and are communicated to the employee's supervisor or manager, authorization to suspend or remove RAS accounts **must** be granted, and the RAS account in question **must** terminated immediately, upon receipt of notice.

An up-to-date list of all individuals with RAS accounts **must** be maintained. The list **must** include the users' contact information, identify the authorizing Ministry, branch, and manager, and should describe both the program applications and information that the user is authorized to access remotely.

2.3. Identity authentication

The identity of the connecting user **must** be authenticated, upon the initiation of each RAS session, using an approved authentication mechanism that is based on proof of possession of either a hardware token or a soft[5] token (e.g., a cryptographic key).

Before non-OPS users (e.g., contractors, service partners) are issued digital credentials for RAS, their identity **must** be verified, and they **must** sign an agreement to acknowledge their responsibilities (e.g., the GO-Security Token external subscriber agreement). Their digital credentials **must** have an expiry date no later than the termination date of their contract with the ministry or agency. The appropriate Program Manager **must** approve and document any extension beyond the expiry date.

2.4. Remote sessions

With the exception of kiosks and PATs, termination of RAS sessions **must** occur after a period of inactivity not exceeding thirty minutes. Such a safeguard will reduce the likelihood that unauthorized users will successfully access RAS via unattended devices.

Approved cryptographic controls (e.g., algorithms and/or implementations thereof and key lengths described within GO-ITS 25.12) **must** be deployed to protect information communicated during session establishment and subsequent duration of connection of any RAS session, such that the confidentiality and integrity of all data transmitted is adequately protected from interception or attack.

RAS users **must** not be permitted to establish another network connection while connected to the Government network via a RAS connection (e.g., support for split-tunneling **must** be reliably disabled on the local network interface).

---

[5] An example of a *soft token* is an Entrust EPF file (e.g., a GO-PKI certificate) stored on the local drive of a portable computer or a generic USB device. Certain applications accessed via a RAS may require stronger authentication, depending on the risks involved, as determined by a TRA (e.g., a more robust, secure hardware token).

2.5. Remote computing devices and software

The overarching principle of remote access to the Government of Ontario network is that remote devices **must** be operated in accordance with, and maintain, a level of security commensurate with that enforced upon devices connected within the internal managed network.

To achieve this principle, all connected RAS devices **must**:

- Have operating systems and software that are up to date, securely configured, properly hardened, and maintained (e.g., ongoing application of required security patches);
- Be protected with a centrally managed personal or desktop firewall, or part of a managed network environment protected by an enterprise firewall; and
- Be protected with anti-malware software with signatures or other detection methods that are automatically kept up-to-date, via either central management or a vendor-provided service.

2.6. Remote computing devices used by Government of Ontario staff

Only Government-issued computing devices should be used for remote access to the Government of Ontario network. These devices are subject to corporate and cluster policies, standards and procedures for IT resources. Government equipment **must** only be used in accordance with the published Operating Procedures for Use of I&IT Resources and other related OPS policies.

OPS staff members may only use a non-Government computing device for remote access if the device and its configuration have been approved by the Cluster Chief Information Officer or his/her delegate and endorsed for use by the I&IT Strategy and Cyber Security Division. The staff member **must** also sign an agreement to acknowledge that:

- They are responsible for ensuring that the device continually meets the security requirements in this document;
- They are aware of the procedures and best practices that they **must** follow to protect Government information and resources including issues such as privacy, classification/handling of information (see ISPC policy), access to information (see Education and Training), and disposal (as per published requirements); and
- They understand that the Government reserves the right to withdraw access if the remote computer fails at any time to comply with the requirements in this document, or if other reasons for concern exist.

Publicly accessible non-Government computers[6] **must** never be used for remote access; such systems may be compromised, and used by intruders to capture supplied credentials and/or the information handled during the RAS session.

[6] Non-government computers that are publicly accessible may lack integrity (e.g., presence of malware) and cannot be relied upon for Government business use.

2.7. Unattended Service Kiosks and Public Access Terminals

Some Government systems, such as unattended service kiosks and public access terminals (PATs) provide limited access to Government services or information that may require RAS.

The program area responsible for the operation of any kiosk or PAT that requires RAS **must** ensure the design and implementation of the kiosk and/or PAT meets the requirements in both this document and GO-ITS 25.0 General Security Requirements. The responsible program manager **must** ensure that developers for kiosk and/or PAT solutions are aware of these requirements, and that any associated credentials and/or device certificates provided for the kiosk and/or PAT are deployed in an appropriate fashion. Any device certificates provided for this purpose **must** be used in compliance with GO-PKI user agreements and associated policies.

RAS account information associated with kiosk or PAT devices **must** include the name and contact information for the responsible program manager.

Any kiosk or PAT implementation using RAS **must** be hardened against attack, and configured to deny interactive session access or administrative control to public users of these services.

2.8. External RAS users

Government programs may request that remote access to the Government of Ontario network be provided to individuals in external organizations (e.g., consultants, service delivery partners, or clients with special access).

Contracts with external organizations that will involve remote access **must** require compliance with this document, in particular with respect to:

- Protection of the computing devices and supporting infrastructure that are used by their staff and/or contractors for remote access; and
- The awareness of their staff and/or contractors regarding the procedures and best practices that they **must** follow to protect Government information and resources including issues such as privacy, classification and/or handling of information (see ISPC policy), access to information (see Education and Training), and disposal (as per ISPC policy).

Agreements with external organizations that involve the provision of remote access **must** also stipulate that the Government of Ontario:

- Authorizes the organization only to access specific Government applications via RAS, and only to use and potentially store specific Government information[7];
- Requires appropriate disposal of Government information in accordance with ISPC policy; and
- Reserves the right to withdraw remote access if the organization does not comply with the requirements in this document at any time.

[7] Authorization to store sensitive information on remote devices should not be given unless essential for the completion of the work, and a business case has been documented and approved.

2.9. RAS and sensitive information

Sensitive information (as defined by ISPC policy or a TRA) should not be downloaded and stored on the remote device initiating the RAS connection. Government Programs that authorize sensitive information to be stored on the remote connecting device **must** first ensure that:

- Additional security safeguards are in place for the remote device (e.g., full-volume encryption, compliant with GO-ITS 25.12 requirements, protecting all stored data, physical security measures, and any safeguards as recommended by the Program TRA); and
- The RAS users involved have received ISPC training, are aware of the sensitivity of the information they are likely to handle, have been instructed as to the best practices involved in protecting the information, and understand the procedures for the secure disposal of data (and/or computing devices, media on which sensitive Government information has been stored) as per ISPC.

2.10. RAS implementation

Equipment used to provide and support RAS gateways[8] **must** be:

- Placed in a DMZ environment, such that the devices are outside the managed perimeter boundary of the Government of Ontario integrated network;
- Up to date, properly hardened (as per section 2.5 of this document), and maintained with the understanding that RAS gateways are security operations and boundary control devices; and
- Subject to vulnerability assessment (or other security testing and evaluation measures) performed or endorsed by the I&IT Strategy & Cyber Security Division.

Administrative access to RAS equipment **must** be limited to authorized and trained technical staff whose identity is authenticated using a strong and centrally administered authentication mechanism. Any remote administration **must** be carried out via a secure connection (i.e., encrypted using GO-ITS 25.12 approved cryptography, and authenticated). All administration and diagnostic functions on servers associated with the RAS deployment **must** be protected as per the guidance in GO-ITS 25.8.

Controls **must** be in place to limit the access of RAS users to only the specific program applications and data that they are authorized to access remotely.

[8] A gateway (or concentrator) is a computer system or device that is the initial point of RAS user contact from the Internet, and allows access to another computer or network subject to successful authentication.

2.10.1. Monitoring RAS use

A central RAS audit log **must** be clearly defined and regularly monitored to ensure that an appropriate record of events is both maintained and reviewed. All log entries **must** be clock synchronized, formatted, protected, retained, and handled in accordance with the requirements stated in GO-ITS 25.0 General Security Requirements.

2.10.2. Security assessments

The RAS infrastructure is a boundary control for the Government of Ontario enterprise network. It therefore **must** be subjected to Threat Risk Assessment and security testing and evaluation prior to and following implementation. These assessments **must** additionally be performed whenever there is a change to the technology, physical design, or other elements that may introduce new threats or vulnerabilities and increase risk.

The service provider or deploying Government program area with responsibility for the RAS implementation **must** ensure these assessments are performed.

3. RESPONSIBILITIES

RAS Users

All RAS users are responsible for:

- Complying with Government directives, policies and agreements when using Government equipment and services;
- Adhering to RAS and related procedures for the acquisition and use of their account;
- Protecting their PKI profile and/or their GO-Security Token from being copied or removed from their possession;
- Complying with Corporate, Ministry, and/or agency procedures for the processing and/or handling of sensitive information when working off-site;
- Ensuring security safeguards installed to protect their remote device are not disabled or tampered with;
- Exercising good judgment regarding the selection of a remote device used to connect to the RAS service, avoiding public terminals;
- Ensuring that Government information and devices are protected from access by unauthorized individuals; and
- Immediately reporting any suspected security breaches to the IT Service Desk.

Program Managers

Program Managers are responsible for:

- Authorizing and documenting the assignment of RAS accounts for users based on their job requirements;
- Ensuring that a request for the termination of a RAS account is submitted promptly when no longer required, or if a RAS user fails to or deliberately does not comply with the security requirements in this document;
- Ensuring that RAS users are aware of and adequately trained in their responsibilities as set out in this document, and other related Government policies;
- Ensuring that the risk posed by unattended kiosk and PAT devices with RAS credentials is mitigated via education of developers, supplying contact information, properly managing any assigned credentials, and ensuring any kiosk or PAT device has been hardened against attack as per both this document and GO-ITS 25.0;
- Reporting any security exposures or suspected breaches regarding RAS to the IT Service Desk; and
- Ensuring that contracts with consulting firms, service delivery partners, and clients with special access needs include provisions for compliance with these requirements;

Infrastructure Technology Services (ITS)

ITS contracts an external organization to provide RAS services for the Ontario Government (RAS Service Provider). ITS is responsible for:

- Managing the vendor contract for the provision of an enterprise RAS deployment;
- Ensuring that the Service Level Agreement with the RAS Service Provider binds them to the requirements in this document;
- Monitoring the administration, operations and security of the RAS infrastructure for adherence to these requirements and all relevant OPS policies and standards;
- Providing IT Service Desk services to remote users and reporting security incidents to the I&IT Strategy and Cyber Security Division;
- Providing directory services to support identity authentication;
- Ensuring that all remote user profiles are synchronized with their local profiles;
- Ensuring that security testing and evaluation of the RAS gateway is completed whenever there is a change that could introduce new threats or vulnerabilities; and
- Ensuring that RAS deployments have a current Threat Risk Assessment and Security Plan (e.g., including a disaster recovery capability and a business continuity plan).

RAS Service Provider

The RAS Service Provider is responsible for:

- Implementing, managing and operating RAS in accordance with the requirements in this document;
- Ensuring that appropriate security safeguards are in place to protect the RAS infrastructure, including those stipulated in this document;
- Supporting a TRA and security testing and evaluation (STE) for the RAS implementation, in instances where this responsibility lies with the provider as the implementing vendor; and
- Ensuring that log information for the RAS infrastructure is securely maintained, regularly reviewed, and made available when needed for investigations in accordance with both this document and GO-ITS 25.0 General Security Requirements.

Cluster Chief Information Officers

Cluster CIOs are responsible for authorizing a member of the OPS to use his/her non-Government computing device for remote access.

I&IT Clusters

I&IT Clusters are responsible for:

- Maintaining up-to-date lists of their Cluster staff and external users who have been granted RAS accounts;
- Ensuring that Government-issued devices used for remote access meet applicable corporate and cluster requirements for Government IT equipment;

- Ensuring that the required agreement is signed by members of the OPS who are permitted to use a non-Government computing device for remote access;
- Ensuring that requests for the termination of RAS accounts are submitted promptly to the IT Service Desk when RAS users fail to or deliberately do not comply with the security requirements in this document;
- Administering patch management for Government-issued computing devices used for remote access; and
- Supporting security incident reporting and management procedures as per GO-ITS 37 Incident Management.

Ontario Shared Services

Ontario Shared Services (OSS) is responsible for:

- Providing PKI help desk services for GO-PKI certificates (e.g., password recoveries, certificate revocations); and
- Administering GO-PKI subscribers in accordance with GO-PKI policies and procedures.

Ontario Internal Audit Division

The Ontario Internal Audit Division is responsible for:

- Conducting periodic audits of pertinent activities to test compliance with security standards;
- Communicating with appropriate management about the risks identified and the severity of those risks; and
- Working with management to identify the needed management action plans to mitigate the risks noted during the course of an audit and conducting follow-up as required.

I&IT Strategy and Cyber Security Division (SCS)

The I&IT Strategy and Cyber Security Division, or a successor division/branch, is responsible for:

- Maintaining this and other GO-ITS 25 series standards;
- Performing and/or endorsing security testing and evaluation for the RAS implementation;
- Endorsing authentication mechanisms and cryptography for the Government of Ontario (i.e., GO-ITS 25.12);
- Approvals for anti-malware software and the firewalls that can be used to protect computing devices used for remote access to the Government network;

- Operating the GO-PKI Certificate Authority;
- Operating the GO-Security Token Registration Authority;
- Monitoring network traffic for attacks and inappropriate activity; and
- Monitoring compliance with these requirements in conjunction with ITS, the RAS Service Provider, OSS, Internal Audit, and I&IT Clusters, and taking appropriate action upon non-compliance.

4. ACKNOWLEDGEMENTS

4.1 Editors

Full Name	Cluster, Ministry and/or Area
Tim Dafoe	I&IT Strategy & Cyber Security Division

4.2 Contributors

Full Name	Cluster, Ministry and/or Area
Charlotte Ward	MGS Corporate Security Branch
Earl Kuntz	MGS Corporate Security Branch
Mano Pancharatnam	MGS Corporate Security Branch

4.3 Reviewers

The following groups have reviewed this standard:

Ontario Internal Audit Division

5. DOCUMENT HISTORY

Version 1.0 Approved by Architecture Review Board (ARB): June 29, 2005

Updated: February 16, 2006

- Changed Application and Scope section to make it clear that the standard applies to any service providing a connection to a device (e.g., server) inside the Government network (e.g., not just the VPN service).
- Changed Identity Authentication section to use more general description of requirement (aligns with requirement description in other GO-ITS security document).
- Changed section on Remote Computing Devices Used by OPS Members to make it clear publicly accessible non-Government computers must never be used for remote access.

Version 2.0 Endorsed by IT Standards Council (ITSC): April 19, 2006

- Changes noted above (dated February 16/06) endorsed by ITSC

Updated: February 2008

- Changes made to reflect changes to the OPS organization chart, transition to new network service provider, and introduction of GO-Security Token as new authentication method for RAS.

Updated: May-July 2008

- Edit for tone and technical items, ITSC format, consistency.
- Incorporated input from Internal Audit.

Version 2.1 Endorsed by ITSC: August 20, 2008; Approved by ARB: October 16, 2008

Updated: March 2012

- Organizational details updated
- Updated hyperlinks and references
- Minor errata and adjustment

Updated: June 12th, 2012

- Updated consultations
- Minor GO-ITS numbering error in references

Updated: November 15th, 2012

- Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 2.2

Updated: January 19th, 2015

- Minor updates as per ARB rationale (administrative/organizational updates, ISO/IEC alignment), draft document version set to 2.3

Version 2.3

- Endorsed by Architecture Review Board: March 18, 2015
- Approved by Information Technology Executive Leadership Council (ITELC): April 16, 2015

6. DEFINITIONS

Access: Entry to an Electronic Network provided by the government to its employees and other Authorized individuals on or outside government premises including telework situations.

Access Controls: Procedures/devices designed to restrict entry to a physical area (physical access controls) or to limit use of a computer/communications system or computer stored data (logical access controls).

Accountability: The obligation to answer for results and the manner in which responsibilities are discharged. Accountability cannot be delegated.

Authenticate: To establish the validity of a claimed identity of a user prior to gaining access (e.g., passwords, access cards).

Authorize: To grant permission to access resources according to a predefined approval scheme.

Availability: The degree of readiness expected of information systems and IT resources to deliver an appropriate and timely level of service, regardless of circumstances.

Certificate: The public key of an entity, together with other information, made authentic when digitally signed with the private key of the CA that issued it. Certificate formats are described within the X.509 and RFC 2459 specifications.

Certificate Revocation List (CRL): A list of revoked PKI certificates that is created and signed by the CA that issued the certificates. A certificate is added to the list if it is revoked (e.g., because of suspected key compromise).

Certification Authority (CA): An authority trusted to issue and manage PKI keys, certificates, and Certificate Revocation Lists.

Confidentiality: The preservation of a degree of secrecy consistent with the sensitivity of information, competitive position, and legislative requirements (e.g., FIPPA).

Data: Any formalized representation of facts, concepts or instructions suitable for communication, interpretation or processing by a person or by automatic means.

DMZ (*de-militarized zone*): A network intended as a buffer between an organization's internal network and an unmanaged network, such as the Internet. The DMZ contains computing devices that are Internet-facing and considered to be outside the managed network perimeter.

Electronic Network: Computers and computer systems that can communicate with each other and, without restricting the generality of the foregoing, includes the Internet, Networks internal to an institution, as well as closed networks external to an institution.

Encryption: The transformation of data via cryptography into a form unreadable by anyone not in possession of the required key. It can provide for data confidentiality by keeping the information hidden from any individual or entity for which it was not intended.

Firewall: Software or a hardware device that acts as a security barrier between two networks and mediates access between those two networks according to an approved set of rules.

Gateway: A computer that is the initial point of user contact from the Internet and allows access to another computer or network.

Hardening: The systematic elimination of known vulnerabilities through software or firmware updates and patches, and through proper system and security configuration (in keeping with the principles of *least access* and *least privilege*). Hardening is often performed on equipment prior to deployment, to ensure it is robust and can withstand typical electronic attacks.

Information: The meaning derived from or assigned to facts or data, within a specified context.

Information Technology Resources: Those resources (hardware, software, data etc.) associated with the creation, storage, processing and communication of information in the form of data, text, image and voice.

Integrity: The authenticity, accuracy and completeness of data that can be affected by unauthorized or accidental additions, changes and/or deletions.

Malware: Software and/or program code/instructions inserted into a system, usually covertly, with the intention of compromising one or more of confidentiality, integrity, or availability associated with the system or the data it processes. This includes traditional “virus”, “trojan”, and “worm” software as well as “sniffer”, “logger”, “backdoor”, “trapdoor”, and “rootkit” threats.

Network: Information technology systems that can be made of one or both of the following components:

- Local Area Network (LAN) - Network of Information technology systems wholly situated at one geographical address; and
- Wide Area Network (WAN) - located over more than one geographical site.

Personal Firewall: Software or a hardware device that acts as a security barrier between a personal computer and a network, and mediates access between that computer and the network according to a set of rules.

Program Manager: The person responsible for the continued development, operational control, implementation, monitoring, etc. of a specific business program or service within a Ministry.

Public Key Infrastructure (PKI): A structure of hardware, software, people, processes, and policies that employs digital signature and encryption using public and private key pairs to enable parties who were previously unknown to each other to establish trust relationships, and to conduct secure and confidential communication, transactions, and information exchange.

Registration Authority: An authority trusted to register authorized users for GO-Security Tokens.

Responsibility: The obligation to perform a given task or tasks associated with a specific role.

Risk: A potential opportunity or threat that may impact on an organization’s ability to meet its business objectives.

Safeguard: A protective and precautionary measure to prevent a security threat from happening.

Subscriber: A member of the CA domain. A party who is the subject of a certificate and who is capable of using, and is authorized to use, the private key, that corresponds to the public key in the certificate. Responsibilities and obligations of the subscriber would be as required by the Certificate Policy and as described in the Subscriber Agreement.

User: A person authorized to access and use Information and Information Technology resources.

7. APPENDIX A: ADDITIONAL INFORMATION

Type of standard

Check One	Type of Standard
☑	Implementation or Process Standards – requirements or specifications, which may include best practices and guidance, for the implementation of a technology or the performance of an activity related to the use of technology, applicable throughout the provincial government (e.g., mandatory O/S configuration requirements, security procedures, change management procedures, web page design requirements etc.).
☐	Information Standard – specifications for a data format (e.g., XML schema, metadata, and/or related data models)
☐	Technical Standard - networking and communications specifications, protocols, interfaces (API's) (e.g., standards adopted from recognized standards development organizations such as W3C, OASIS or IETF such as TCP/IP, XML, SOAP, etc.)
☐	Architecture Standard – application patterns, architecture and standards principles governing the design and technology decisions for the development of major enterprise applications
☐	Product Standard – an enterprise-wide product which is mandatory for use such as a single corporate-wide application, which all ministries and agencies use to record and access their HR information.

Publication

Please indicate if this standard should be restricted to publishing on the Internal (Intranet) IT Standards web site or whether it is intended for publishing on the public (Internet) Government of Ontario IT Standards web site.

Check One	Publish as Internal or External
☐	Internal Standard
☑	External Standard

Consultation

Check	Area	Date: (month/year)
☑	ARB	Dec. 2014
☐	Strategy, Policy and Planning Branch, ICS	
☐	Controllership Branch, (Corporate Architecture) ICS	
☑	Corporate Security Branch (Cyber Security Branch)	Feb. – Jun. 2008
☐	Information Privacy and Archives	
☐	Strategy, Policy, Planning and Management Branch (SPPM, OCCS)	
	Corporate ACT and Domain Working Groups	
☐	- Information Architecture Domain (IADWG)	
☐	- Technology Architecture Domain (TADWG)	
☐	- Application Architecture Domain (AADWG)	
☐	- Security Architecture Working Group (SAWG)	
☐	Infrastructure Consolidation projects: - Enterprise Email Services - Servers and Data Centres - Desktop Management - Service Management	
☑	IT Standards Council (ITSC)	August 2008

Impacts to standards

List any existing GO-ITS that may be impacted or associated with this standard.

GO-ITS #	Describe Impact	Recommended Action (or page number where details can be found)
GO-ITS 25.0	Other GO-ITS 25 documents supplement this document.	Compliance with additional GO-ITS 25 documentation is recommended.

Impacts to existing environment

List any significant impacts this standard may have on the existing I&IT environment.

Application(s) or Infrastructure Impacted	Describe Impact	Recommended Action (or page number where details can be found)
All	Adherence to these security requirements will reduce the risks to Government I&IT resources.	Compliance with these requirements.
All	Implementation of these security requirements will produce some impact due to additional complexity and/or cost due to authentication requirements (e.g., GO-Security Token).	Compliance with these requirements.

References

Management and Use of Information & Information Technology (I&IT) Directive:
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.04.11.09.46.33.J6N_res/$File/ManagementOfITDir.pdf

Corporate Policy on Information and Information Technology (I&IT) Security:
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2011.08.09.10.22.28.JV4_res/$File/corporatePolicyIandITSecurity.pdf

Information Security & Privacy Classification Policy:
http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.18.14.34.52.PSU_res/$File/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf

Acceptable Use of I&IT Resources Policy:

http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2011.04.01.13.19.10.NBJ_res/$File/acceptableI&IT_Policy.pdf

GO-ITS 25 standards:

http://intra.net.gov.on.ca/iit/services/iit-policies/

GO-ITS 25.0 – General Security Requirements

GO-ITS 25.8 – Security Requirements for Servers

GO-ITS 25.10 – Security Requirements for Mobile Devices

GO-ITS 25.12 – Use of Cryptography

GO-ITS 37 – Incident Management

Copyright & Disclaimer