Ontario

Government of Ontario


## Government of Ontario IT Standard (GO-ITS)

## Number 25.1

# Security Requirements for Routers and Switches

**Version #: 1.3**

**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 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.

Routers and switches are key components within Government of Ontario information networks. Without appropriate devices configuration and management, attackers targeting routers and switches may disrupt or compromise not only these networks, but also the systems that rely upon them.

## Version Control

| Date | Version | Author | Comment |
|---|---|---|---|
| Jan. 14, 2003 | 1.0 | Doug Whyte, CSB | Original document approved by Architecture Review Board (ARB) |
| Oct. 1, 2008 | 1.1 | Tim Dafoe, CSB | Major structural revisions, language adjustments, and significant updates to technical content, vendor consultation, final version for ARB |
| Mar. 14, 2012 | | Tim Dafoe, CSB | General minor update as per document history |
| June 12, 2012 | | Tim Dafoe, CSB | Updated consultation list |
| Nov. 15, 2012 | 1.2 | Tim Dafoe, CSB | Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 1.2 |
| Jan. 19th, 2015 | 1.3 | Tim Dafoe, SCS | Minor updates per ARB rationale (administrative updates, ISO/IEC alignment),draft document version changed to 1.3 |

# Table of Contents

# 1. INTRODUCTION

## 1.1 Purpose of the standard

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

The operation of any large IP network is dependent upon effective use of routers and network switches. Without robust enterprise networking, systems and applications cannot function properly. The security of these devices and the correctness of their configurations are therefore critical to safeguarding Government of Ontario Information and Information Technology (I&IT) resources.

This document sets out security requirements for routers and switches within the Government. The objective of this document is to ensure that deployment of and reliance on routers and/or switches will not result in unacceptable risks to I&IT resources.

## 1.2 Versioning and change management

On-going 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 words are used which require precise interpretation from readers. The following are the precise requirements 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

This Standard applies to all ministries of the Ontario Government, 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.

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.

The GO-ITS 25.1 Security Requirements for Routers and Switches apply to all ministries of the Ontario Government and any organization that uses a ministry's or I&IT Cluster's information technology infrastructure.

## 1.6 Principles

The following principles are stated in accordance with the Corporate Policy on Information and Information Technology Security:[2]

- Ministries and agencies **must** be assured that I&IT resources are safeguarded by sound router and switch configuration. This assurance is expressed in terms of confidentiality, integrity, availability, accountability, reliability and opportunity for audit.
- The implementation of recommended security measures for routers and switches does not diminish the need for Program Managers to ensure a Threat Risk Assessment (TRA) is

[1] As determined via the 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) and/or TRA process.

[2] The Corporate Policy on Information and Information Technology 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

conducted for each program and appropriate security measures are in place to protect program applications, information and resources.

- For various reasons (e.g., change control and operational issues), routers and switches **must** be used for roles whereby the primary functionality (e.g., managing network traffic) of these devices is deployed as intended; these devices **must** not be relied upon exclusively for the provision of secondary services (e.g., access control, packet filtering, or high security assurance functions), even if these devices are described as supporting, or are expressly capable of, such functions.

# 2. REQUIREMENTS

## 2.1 Base standards for IP routers

At a minimum, each network router deployed within or operated on behalf of the Government of Ontario **must** meet the following requirements:

- The device **must** be capable of securely storing hashed passwords in configuration files;
- The device **must** perform IP network traffic routing;
- The device **must** use access control lists only for network management (e.g., route filtering, traffic management) and not for assurance of network security design or function;
- The device **must** employ authentication measures for dynamic route updates;
- The device **must** possess the ability to discard unwanted traffic (e.g., packets with RFC 1918 source addresses on external interfaces);
- The device **must** support interactive session/login timeouts;
- The device **must** possess the ability to maintain route state tables;
- The device **must** be dedicated to performing network routing functions;
- The device **must** not support IP source routing, or the support **must** be disabled;
- The device **must** not support ICMP directed broadcasts;
- The device **must** not proxy ARP requests;
- The device **must** possess the ability to perform anti-spoofing functions;
- All device IP addresses **must** be configured explicitly, and **must** not be assigned dynamically;
- The device should not support the Telnet protocol;
- The device **must** have TCP and UDP small services disabled, if present;
- Unnecessary services, including (but not limited to) the following **must** be disabled unless required, and additional mitigation has been employed to reduce the associated risk:
    - TFTP, FTP, "*r*" services (e.g., rlogin), UUCP, finger, RIP, DHCP, IPSec, PPTP; and
    - Network boot protocols.
- Router interfaces with different security levels (e.g., associated with varying Security Zones) should not connect to the same physical switch for high-risk situations or environments; physical (not logical or virtual) separation should be used; and
- IP traffic that is obviously forged, or should not be passed as a function of sound network management practice, should be dropped. Some examples include:
    - Packets appearing to originate from *localhost* (e.g., 127.0.0.0/8);
    - Inbound traffic destined for external interfaces from a reserved internal address (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16);
    - Inbound traffic destined for external interfaces from a multicast address (e.g., 224.0.0.0/10);
    - Outbound traffic on an internal interface that contains an external interface address as a source address;
    - Packets with identical source and destination addresses; and

- Any other special cases as required, particularly when such traffic originates from external sources (e.g., a network that is not managed by or on behalf of the Government of Ontario).

## 2.2 Base standards for network switches

At a minimum, each network switch deployed within or operated on behalf of the Government of Ontario **must** meet the following requirements:

- The device **must** be capable of securely storing hashed passwords in configuration files;
- The device **must** use any available access control functions for network management and segmentation purposes only, and not to provide for assurance of security design or controls;
- The device **must** deny all unapproved or unauthorized updates (e.g., ports, trunk, spanning tree);
- The device **must** possess the ability to drop malicious or unwanted traffic;
- The device **must** support interactive session/login timeouts;
- The device **must** be dedicated to performing Ethernet switching functions;
- The device **must** not support ICMP directed broadcasts;
- The device **must** not proxy ARP requests;
- The device **must** possess the ability to perform layer two anti-spoofing functions;
- The device **must** be configured to deter typical layer two denial of service attacks (e.g., attacks against spanning tree protocol, DHCP, ARP, or MAC address caching) via a port security feature or similar function;
- All device IP addresses **must** be configured explicitly, and **must** not be assigned dynamically;
- The device **must** not have VLAN 1 assigned to any port;
- The device **must** assign a unique native VLAN number to Ethernet trunks (e.g., one that is not assigned to normal switch ports);
- To protect against documented vulnerabilities, the device **must** be used in conjunction with layer three access control when private virtual LANs (PVLANs) are used to provide network segregation and a layer three router is present on the segment where PVLANs have been implemented;
- The device should not support the Telnet protocol.
- The device **must** have TCP and UDP small servers disabled, if present; and
- Unnecessary services, including (but not limited to) the following **must** be disabled unless required, and additional mitigation has been employed to reduce the associated risk:
    - TFTP, FTP, "*r*" services (e.g., rlogin), UUCP, finger, RIP, DHCP, IPSec, PPTP;
    - Any type of automatic / dynamic Ethernet trunk support / negotiation; and
    - Network boot protocols.

## 2.3 Physical security

- Router or switch devices **must** be placed in a locked room accessible only to authorized personnel;
- Physical devices (e.g., PC cards, modems) used to connect to the router or switch **must** be protected from unauthorized use while in storage;

- Any operations or storage room should be free from electrostatic or magnetic interference and be environmentally maintained via HVAC, fire, and other systems;
- If continuous operation of the router or switch is critical, an uninterruptible power supply (UPS) should be installed and spare components kept on hand; and
- Physical access procedures for routers and switches deployed within high-risk environments or which support the operation of systems processing sensitive information **must** be subject to authorization, change control, and relevant physical access control techniques as stated within GO-ITS 25.0 General Security Requirements.

## 2.4 Access control

- There **must** be no circumvention of the intended traffic path supported by the router and/or switch by any means (e.g., the use of modems, network tunnels, proxies, cables);
- All access to Government of Ontario routers and/or switches **must** comply with GO-ITS 25.0 password management and use requirements;
- Authentication and authorization for router and/or switch access **must** be performed via a centralized method, as per the GO-ITS 24.0 Omnibus IT Standard; and
- Administrative access to routers and/or switches should employ centralized two-factor authentication.

## 2.5 Router and switch management

- Operational access **must** be restricted to appropriate network security service staff;
- Routers and/or switches should be managed via a management console; direct sessions to individual routers and/or switches should be avoided;
- Router and/or switch management sessions originating from external network interfaces **must** not be permitted, unless they are authorized, documented, and approved via agreements;
- Each authorized administrator **must** be assigned a unique account for use, in accordance with GO-ITS 25.0 General Security Requirements;
- A secure session (e.g., an IPSec tunnel, SSH session, HTTPS transport security) employing approved cryptography (i.e., GO-ITS 25.12) should be used for management of routers and/or switches; and
- The contents of configurations and access control lists **must** be classified and protected in accordance with the Information Security and Privacy Classification (ISPC) policy.

## 2.6 Simple Network Management Protocol (SNMP)

SNMP community strings **must** follow GO-ITS 25.0 password selection conventions, as well as the following additional conventions specific to this document:

- The SNMP community string **must** contain at least one special character (e.g., *%* or *&*);
- SNMP community strings **must** be unique for the routers and/or switches in each security zone of a multi-tier environment;
- Production SNMP community strings **must** not be the same as those used in development or test environments;
- SNMP *read* and *write* community strings **must** be different, and not based upon a similar string;

- SNMP community strings for routers and/or switches **must** differ from those used on other technology platforms (e.g., firewalls, servers), and not based upon a similar string;
- SNMP ingress **must** be prohibited from any network not managed by or on behalf of the Government of Ontario, unless authorized, documented, and approved via agreements;
- Routers and/or switches should use SNMP v3 (designed with security requirements in mind) as a minimum standard;
- SNMP management access **must** be limited to specific systems;
- SNMP traps and/or queries **must** only be permitted to and from dedicated central management hosts located on an isolated, secure management network available only to authorized administrative staff; and
- SNMP *write* access should be disabled where possible.

## 2.7 Logging

Logging **must** be consistent with the controls described in GO-ITS 25.0 General Security Requirements. In addition to those requirements, the following router and/or switch specific requirements **must** be implemented:

- Routers and/or switches **must** be configured to send all logs to centralized logging servers located on a management segment protected by a layer three firewall;
- Logs **must** not be sent directly to a management console;
- Logs **must** be available for online review for a minimum of six months;
- Archived logs **must** be maintained for two years and safeguarded as per ISPC;
- Archived logs **must** be made available for online review within five business days;
- Router and/or switch logs should include interface names/addresses; and
- Routing, VLAN, and PVLAN events (creation, modification, deletion) should be logged.

## 2.8 Remote access

- Remote access to routers and switches **must** be conducted in a manner endorsed by the I&IT Strategy and Cyber Security Division, and employ two-factor authentication;
- Remote administration of routers and switches **must** be established through RAS access employing approved cryptography (e.g., IPSec or SSL/TLS VPN);
- Discrete, out-of-band network interfaces should be used for administration;
- If TFTP cannot be disabled due to business requirements, its use **must** be limited to access from an isolated, secure management network available only to authorized administrative staff; and
- The use of out-of-band modems should be avoided unless business requirements dictate such functionality, in which case PSTN use should be avoided, and a TRA should be completed to identify the risk involved.

## 2.9 Change management

Change management procedures **must** be compliant with GO-ITS 25.0 General Security Requirements and the GO-ITS 35.0 Change Management standard. In addition to those requirements, the following are router and/or switch specific requirements:

- Changes made to routers and switches must be tracked with details of the changes made (e.g., date, time, name of the person responsible, and the business requirement for the change);
- All software configuration and hardware changes with potential impact to operations **must** be tested and verified in a lab environment, unless there are mitigating circumstances preventing these activities from taking place (i.e., a major emergency);
- Security patches **must** be installed as soon as practical (based on severity of patch), after appropriate testing;
- All router and/or switch change requests **must** include the following:
    - Requester information including name, contact information, ministry/agency information, cluster information, request date and implementation date;
    - Duration of validity (start date and end date);
    - Application information including name, owner, and owner contact information;
    - Business rationale for request;
    - Impact statement of request;
    - A test plan and back-out plan for the change; and
    - Sign off from Program Manager and relevant Change Advisory Board; and
- Routers and switches **must** be centrally managed to provide a consistent level of security, and must be managed via a secure facility.

## 2.10 Configuration management

- Router and switch configurations **must** be archived to a central server in a management segment;
- The router and switch software base (including software patches, hot fixes and updates) **must** be obtained from a trusted source that includes integrity checking;
- All default account names **must** be replaced with new IDs where possible, and passwords changed as per GO-ITS 25.0 password management requirements;
- Device configurations **must** be backed up daily, and kept in a secure location;
- Any major configuration changes with potential security implications **must** be communicated to the I&IT Strategy and Cyber Security Division (e.g., firmware upgrades and patches, hardware changes, or alterations to enterprise VLAN or PVLAN strategy);
- Configurations **must** be checked and tested, prior to and after implementation, for configuration errors and related vulnerabilities; and
- Access to router and switch software repositories **must** be restricted to network administrators.

## 2.11 Time synchronization

- All routers and/or switches **must** obtain system time from a redundant and validated reference time source as per GO-ITS 25.0 General Security Requirements.

# 3. RESPONSIBILITIES

## Users

Users are responsible for:

- Complying with Government directives, policies and agreements when using Government equipment and services;
- Ensuring security safeguards installed to protect the computing devices assigned to them are not disabled or tampered with; and
- Reporting any suspected security incidents or breaches to the OPS Service Desk.

## Program Managers

Program Managers are responsible for:

- Reviewing and approving business cases for device change requests, for network devices that fall under Cluster responsibilities, and lie outside vendor support contracts; and
- Completing Information Security and Privacy Classification and Threat Risk Assessments for new projects involving the deployment of network technology.

## Clusters

IT Clusters are responsible for:

- Supporting program managers where required in the completion of Information Security and Privacy Classification and Threat Risk Assessments;
- Managing device changes for network devices that fall under Cluster responsibilities (if any), and lie outside central vendor support contracts; and
- Monitoring Cluster device change requests (if any) to ensure that they comply with the requirements in this document and other Government policies and standards.

## Infrastructure Technology Services (ITS)

ITS is responsible for:

- Implementing, managing and operating delegated internal routers and switches in accordance with the requirements in this document and other applicable Government policies and standards;
- Maintaining the configuration details for any internal routers and switches under ITS control;
- Ensuring that appropriate security safeguards are in place to protect any internal routers and switches under ITS control, including those stipulated in this document;
- Ensuring that the logs are securely maintained, available when needed for investigations, and retained in accordance with this and related standards; and
- Monitoring Government of Ontario networks for traffic patterns that may cause negative operational impact, and immediately notifying relevant I&IT Strategy and Cyber Security Division contacts for appropriate action.

### Network Service Provider

The Network Service Provider is responsible for:

- Implementing, managing and operating routers and switches within the scope of contractual arrangements, in accordance with the requirements in this document and other applicable Government policies and standards;
- Maintaining the configuration details for the routers and switches it controls;
- Ensuring that appropriate security safeguards are in place to protect the routers and switches within the scope of contractual arrangements, including those stipulated in this document;
- Ensuring that the logs are securely maintained, available when needed for investigations, and retained in accordance with this and related standards; and
- Monitoring Government of Ontario networks for undesirable traffic, and immediately notifying relevant I&IT Strategy and Cyber Security Division contacts for appropriate action.

### 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 standard and all other applicable IT security standards, policies, procedures and related guidance on behalf of the Government of Ontario;
- Reviewing logs to detect malicious traffic and network attacks;
- Assessing change requests and working with change managers to accommodate efforts;
- Approving any relevant changes prior to their deployment in production environments;
- Authorizing use of diagnostic probes or diagnostic modes on routers and switches; and
- Conducting any required inspection, evaluation, and if necessary, removal of any resources that reduce the efficacy or defeat Government of Ontario network security practices (e.g., rogue, malfunctioning, and/or unknown hardware).

### Ontario Internal Audit

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.

# 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 |
|---|---|
| Earl Kuntz | MGS Corporate Security Branch |
| Mano Pancharatnam | MGS Corporate Security Branch |

## 4.3 Consultations

The following individuals were consulted:

Charlotte Ward, MGS Corporate Security Branch

Rob Chiarelli, MGS Corporate Security Branch

## 4.4 Reviewers

The following groups have reviewed this standard:

OCCIO ITS

# 5. DOCUMENT HISTORY

*Version 1.0 Approved by Architecture Review Board: January 14, 2003*

*Version 1.1 Endorsed by IT Standards Council (ITSC): September 17, 2008*

*Updated October 1, 2008:*

- Changed contact information to reflect organizational changes
- Added details based on feedback received from OCCIO ITS end-users
- Adjusted to reflect enterprise solution being piloted and readied for deployment
- Minor changes to language to improve clarity and technical correctness
- Adjusted roles and responsibilities to reflect new agreement with integrated network provider
- Edits to move some address references to CIDR notation
- Expanded base configuration requirements
- Adjusted content based on technical input from network operations
- Adjusted roles based on ITSC feedback

*Version 1.1 Approved by Architecture Review Board: October 16, 2008*

*Updated March 14, 2012:*

- Organizational updates
- Updated hyperlinks and references
- Minor errata

*Updated November 15, 2012:*

- Minor changes approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 1.2

*Updated January 19, 2015:*

- Minor changes as per ARB rationale (administrative/organizational updates, ISO/IEC alignment), draft document version changed to 1.3

*Version 1.3*

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

# 6. DEFINITIONS

**Access:** Gaining entry to an electronic network provided by the Government to its employees and other authorized individuals on or outside government premises, including telework.

**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).

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

**ARP:** Address Resolution Protocol, a layer two protocol commonly used for translating hardware assigned Ethernet MAC addresses to IP addresses on a network.

**Border Gateway Protocol (BGP):** The core routing protocol of the Internet. It works by maintaining a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rulesets.

**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.

**Denial of Service (DoS):** It is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

**Domain Name Service (DNS):** The service that provides for domain names, serving as a "phone book" for the Internet by translating human-readable computer hostnames (e.g., www.example.com) into the IP addresses (e.g., 208.77.188.166) required by networking equipment to deliver information. The service is an essential component of contemporary Internet use.

**Dynamic Host Configuration Protocol (DHCP):** A protocol used by networked devices (*clients*) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

**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 using cryptography into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure confidentiality by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data.

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

**File Transfer Protocol (FTP):** A network protocol used to transfer data from one computer to another through a network, such as over the Internet. FTP is a commonly used protocol for exchanging files over any TCP/IP based network to manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access).

**Finger:** The *finger* protocol is a deprecated simple network information exchange for human-oriented status and user information. Supplying detailed information as e-mail addresses and full names was considered acceptable and convenient in the early days of the Internet, but is now considered inappropriate for privacy and security reasons. In the past, *finger* information was a frequent source of initial data when attackers planned attacks.

**Hardening:** The systematic elimination of known vulnerabilities through software or firmware updates and patches, and through proper system and security configuration.

**HVAC:** A commonly used acronym that denotes *heating, ventilating, and air conditioning* (for reference to environmentally managed facilities).

**Internet Control Message Protocol (ICMP):** One of the core protocols of the Internet protocol suite. It is chiefly used by networked computers' operating systems to send error messages, indicating, for instance, that a requested service is not available or that a host or router could not be reached.

**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.

**Network:** IT 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;
- Wide Area Network (WAN) - located over more than one geographical site.

**Packet Filtering:** Packet filtering acts by inspecting the "packets" which represent the basic unit of data transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).

**Program:** A specific program or service within a Ministry.

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

**PVLAN:** A private, logically isolated virtual LAN segment supported by a network switch that has enhanced levels of segregation from other systems on the same segment, due to strong layer two controls on devices with such support.

***r* Services:** *r*-services provide a variety of methods for executing commands via a remote host, but they also generate serious security concerns. Some examples of these include *rlogin* and *rexec*.

**Routing Information Protocol (RIP):** A commonly used interior gateway protocol (IGP) routing protocol on internal networks (and to a lesser extent, networks connected to the Internet), which helps routers/firewalls dynamically adapt to changes of network connections by communicating information about which networks each router/firewall can reach and how far away those networks are.

**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.

**Sensitive Information:** Information that if released without authorization would cause harm, embarrassment, or unfair economic advantage, e.g. a breach of confidentiality of personal information, unauthorized modification of financial data, or a release of pre-budget information and strategic planning documents.

**Small Services:** A suite of simple network servers intended for diagnostic use, present on some network services and servers. These services can be abused, and are considered deprecated.

**SNMP (Simple Network Management Protocol)**: This protocol forms part of the Internet Protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network

management systems to monitor network devices for conditions that warrant administrative attention. The latest revision (SNMP version 3) offers important security services (authentication, communications security, and access control).

**Source Routing:** A routing feature that permits sender of a packet to specify the route the packet takes through the network. Source routing is widely disabled on modern-day LANs and WANs.

**Spoofing:** A situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining leverage over a process or trust relationship.

**Telnet:** A terminal emulation program for TCP/IP networks such as the Internet, commonly used to initiate interactive sessions with remote hosts. Telnet was designed in the early days of networked computers, and is considered both deprecated and vulnerable to attack.

**Trivial File Transfer Protocol** (**TFTP**)**:** A simple file transfer protocol, with the functionality of a very basic form of FTP. It is still used to transfer small files between hosts on a network, such as when a remote X Window System terminal or a thin client boots from a network server.

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

**Unix to Unix Copy (UUCP)**: A suite of computer programs and protocols allowing remote execution of commands and transfer of files and email between computers.

**Virtual Private Network (VPN):** A communications network tunneled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

**VLAN:** A logically isolated virtual LAN segment supported by a network switch.

**VTP:** VLAN Trunking Protocol, a dynamic protocol intended to help administrators with the burden of managing VLAN creation and deletion on enterprise networks. In some configurations, VTP can be vulnerable to subversion by attackers.

# 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) | June 2008 |
| ☐ | 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) | |
| ☐ | Cluster ACT/ARB (for Cluster standards promoted to Corporate standards) | |
| ☑ | IT Standards Council (ITSC) | September 2008 |
| ☐ | Network Management Committee | |

### 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 24 | GO-ITS 24 provides technical standards and specifications for standards profiles such as GO-ITS 39.1 | Compliance |

### Impacts to Existing Environments

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

| Application(s) or Infrastructure impacted | Describe Impact | Recommended Action (or page number where details can be found) |
|---|---|---|
| Routers & Switches | Adherence to these security requirements will reduce the risks to Government I&IT resources but may result in some increased administrative and operational overhead | 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

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

*IANA RFC 1918,* February 1996
http://www.rfc-editor.org/rfc/rfc1918.txt

*IANA RFC 3300*, September 2002
http://www.rfc-editor.org/rfc/rfc3330.txt

## Copyright & Disclaimer