Ontario

Government of Ontario

Information & Technology Standards

Government of Ontario IT Standard (GO-ITS)

Number 25.6

Security Requirements for Firewalls

Version #: 1.2

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

UNCLASSIFIED

Last Review Date: 2012-11-15

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 Ministry of Government Services (MGS) 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.collaboration.gov.on.ca/mgs/occio/occto/our-services/technology-adoption/technical-standards-1/approved-go-its-standards/

Internet: http://www.ontario.ca/itstandards/

Summary

The Corporate Policy on Information and Information Technology Security requires that Government 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.

Firewalls are industry standard security devices commonly relied upon for boundary control and policy enforcement within IP networks. This standard sets out mandatory minimum requirements regarding the selection, configuration, and management of firewalls within the Government of Ontario.

Version Control

Date	Version	Author	Comment
Jan. 14, 2005	1.0	Doug Whyte, CSB	Approved changes authorized by Architecture Review Board
Oct. 1, 2008	1.1	Tim Dafoe, CSB	Major structural revisions, language adjustments, and significant content changes
Mar. 14, 2012		Tim Dafoe, CSB	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

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 the Ontario Government's networks and computer systems.

Government of Ontario networks must be protected from abuse and misuse. These threats can be reduced in part through the use of network security technology. There also exist legal, regulatory, compliance and business requirements that require information access control between internal ministries and agencies. Firewall technology provides an effective tool to implement these polices, via technical functionality and access control mechanisms.

This document sets out security requirements for firewall design, specification, and deployment within the Government of Ontario. The objective of this document is to ensure that firewall deployment results in an adequate and reliable degree of policy enforcement, permitting for the protection of Government 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 Corporate Security Branch (CSB), Ministry of Government Services. The Corporate Security Branch 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 the 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 Government of Ontario, in addition to any provincial agencies that use or leverage ministry or I&IT Cluster I&IT infrastructure, and all third party individuals and organizations that connect to the Government of Ontario integrated network for businesses 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 and risk mitigation 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 25.6 Security Requirements for Firewalls apply to:

- All ministries of the Ontario Government and any organization that uses a ministry's or I&IT Cluster's information technology infrastructure; and
- Network based firewalls and personal firewalls (software based firewalls for desktop/laptops).

1.6 Out of scope

These requirements do not address proxy servers, network interface card (NIC) packet filters, IP router feature sets, or switching technology (such as virtual network functionality). These devices and techniques **must** not be used in lieu of firewalls (as defined by the requirements in this document) for boundary enforcement purposes.

[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).

1.7 Principles

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

- Firewalls are the primary means by which the Government of Ontario performs reliable, robust policy enforcement and boundary control between external and internal IP networks, and within the broader managed network.
- The implementation of security devices such as firewalls does not diminish the need for Program Managers to ensure a Threat Risk Assessment (TRA) is conducted for each program, and appropriate security measures are in place to protect program applications, information and resources.
- Firewalls must be dedicated to their primary functionality (security policy and boundary enforcement), and not relied upon for the provision of secondary services.

[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

2. REQUIREMENTS

The following security requirements apply to all firewalls deployed within and/or on behalf of the Government of Ontario for the purposes of protecting I&IT assets:

2.1 Network/Enterprise firewalls

2.1.1 Base requirements

Each network/enterprise firewall device deployed for the purposes of protecting Government of Ontario networks and computer systems:

- **Must** be evaluated and certified, relative to a Protection Profile or Security Target deemed appropriate by CSB, at the Common Criteria (ISO/IEC 15408:2005 and ISO/IEC 18045:2005) *EAL 4* level or better[3];
- **Must** be based or built upon a dedicated appliance or hardware system;
- **Must** be based or built upon a hardened operating system specifically configured for the purpose of providing an enhanced level of security and functional assurance;
- **Must** employ a minimal number of functional components or modules within the operating system kernel to reduce the effective attack surface;
- **Must** be supported by an approved security services or product vendor;
- **Must** offer protection against denial of service (DoS) attacks, including known ICMP and UDP DoS techniques;
- **Must** offer anti-spoofing functionality to detect and drop deliberately forged and/or malformed traffic;
- **Must** perform a reliably high degree of network separation and boundary enforcement between internal and external interfaces;
- **Must** perform stateful packet inspection and filtering;
- **Must** deny all traffic from being forwarded unless specific traffic has been explicitly permitted by an authorized rule;
- **Must** offer a high degree of granularity and specificity for the configuration of rules or policies;
- **Must** deny IP source routing;
- **Must** utilize static IP addresses for all interfaces;
- **Must** boot and initialize in a closed state (e.g., one that denies traffic from being forwarded) until all firewall services are active;
- **Must** fail closed in the event of hardware or software failure;

[3] Within reason, given the potential complexity and stringent controls inherent in an evaluated device that markedly exceeds this level of assurance.

- **Must** perform reliable blocking or dropping of any IP traffic designated as undesirable within the rule set or firewall configuration;
- **Must** not rely on DNS information to obtain addresses for objects in the rule set or firewall configuration;
- **Must** not start or provide any unnecessary services, including, but not limited to the following:
  - HTTP, TFTP, FTP, "*r*" services (e.g., rlogin), UUCP, finger, DHCP, IPSec, PPTP;
  - Any type of automatic network protocol negotiation or routing protocols; and
  - Network boot protocols.
- **Must** provide policy/boundary enforcement for all connections to external networks;
- **Must** have external and internal interfaces connected to physically unique/discrete network switches (or similar network devices) in instances where sensitive data (as determined by ISPC) is transmitted/processed, or when deployed in a high-risk environment (as determined by a TRA);
- **Must** be dedicated to performing IP inspection and packet filter functions; and
- **Must** block or drop traffic originating on external interfaces that is obviously forged or commonly associated with attacks; examples of such traffic include:
  - Traffic appearing to come from a *localhost* address (e.g., 127.0.0.0/8);
  - Inbound traffic, when received on an external interface, with source addresses from reserved address space (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), or any multicast address (e.g., 224.0.0.0/10);
  - Outbound traffic, when received on an internal interface, containing an external IP address of a firewall interface in the source IP field;
  - Packets with the same IP address in the source address and destination address fields and with the same port number in the source port and destination port fields; and
  - Any other special cases, as per known network reconnaissance and intrusion techniques.

2.1.2 Network connections

- CSB **must** approve all connections external to the Government of Ontario that require ingress/egress provisions within a firewall rule set or configuration;
- Firewalls located at the network edge **must** provide for a *demilitarized zone* (DMZ) segment or network for the purposes of accepting end-user traffic from unknown or potentially unmanaged external networks;
- Interactive traffic (e.g., traffic associated with the actions of a remote end-user) **must** not be permitted for direct ingress to networks, with the exception of an appropriately defined DMZ;
- All firewall rules and configuration items **must** be validated on a quarterly basis; and
- When rules or configuration items are no longer required, all such rules or configuration items associated with the ingress or egress provision **must** be deleted within ten (10) business days.

.

2.1.3 Physical security

- All production firewalls **must** be operated within a facility where access is restricted to only those personnel with a documented and justified business need (e.g., authorized firewall administrators);
- All production firewalls **must** be operated within facilities with access to devices controlled by use of keys, combinations/codes, card access, biometric technology, or a combination thereof; and
- When providing temporary physical facility access to repair or maintenance personnel, or any others requiring authorized access to firewall devices, such individuals **must** be accompanied/escorted at all times by authorized personnel.

2.1.4 Access control

- There **must** be no circumvention of the intended path enforced by the firewall via any means (e.g., POTS modems, network tunnels, cables);
- Password standards **must** be enforced in accordance with GO-ITS 25.15 Password Management and Use requirements;
- General access control principles and requirements must be enforced in accordance with GO-ITS 25.0 General Security Requirements;
- Authentication and authorization for administrative access to firewalls **must** be performed via centralized methods as per the GO-ITS 24.0 Omnibus IT Standard and GO-ITS 25.0 General Security Requirements; and
- Administrative access to production firewalls **must** employ strong two-factor authentication.

2.1.5 Firewall management

- Each authorized firewall administrator **must** have a unique user account;
- Administrative access **must** be restricted to appropriate network security service staff, in accordance with the principles outlined in GO-ITS 25.0 General Security Requirements;
- Firewalls **must** be managed via a management console or similar service, with direct authentication to firewall devices prohibited for routine operations;
- Firewalls **must** be managed via secure sessions or connections that employ approved cryptography;
- Firewall management and/or administrative access from network interfaces external to the Government of Ontario **must** not be permitted;
- Firewall rule sets **must** be appropriately classified and protected as per ISPC;
- Firewall logs **must** be appropriately classified and protected as per ISPC; and
- Any organization within the scope of this document providing security services (e.g., firewall operations) to the Government of Ontario **must** provide CSB with immediate access to firewall configuration details upon request.

2.1.6 Simple Network Management Protocol (SNMP)

SNMP community strings **must** be selected in accordance with the GO-ITS 25.15 Password Management and Use standard, as well as the following 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 firewalls enforcing boundaries between security zones in 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 firewalls **must** differ from those used on other technology platforms (e.g., routers, switches, 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;
- Firewalls 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.

2.1.7 Logging

Logging **must** be consistent with GO-ITS 25.0 General Security Requirements. In addition to those requirements, the following are firewall specific requirements:

- Firewalls **must** be configured to forward log information to a centralized service located on an isolated, secure management segment that is itself protected by a firewall;
- Direct logging to the firewall management console **must** be disabled;
- Logs **must** be made 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;
- Logging and audit functions **must** be enabled to monitor all administrative access to and events on production firewalls; the following events in particular **must** be logged:
    - Account logon events (both successful and failed);
    - Creation, deletion, and modification of users and groups (both successful and failed);
    - Security policy changes (both successful and failed);
    - Changes to the system security state or run level (both successful and failed);
    - Privilege use (both successful and failed); and

- System events (e.g., system restart, system time adjustments).

- Firewall logs **must** be secured in storage and communication as per ISPC and other policy requirements;
- Firewall logs **must** contain the following information:
  - Source IP address, ports, and protocols for all traffic on any interface;
  - Destination IP address, ports, and protocols for all traffic on any interface;
  - Traffic flow information (ingress and egress);
  - Interface name or other identifier;
  - Firewall rules processed during forwarding;
  - Username for authentication, commands, or changes (if applicable);
  - System configuration changes;
  - Automated actions taken in response to input, and
  - Time stamps for all logged events;
- Three or more invalid access attempts within a sixty second interval **must** generate an alarm to indicate potential unauthorized activity;
- Firewall logs **must** be reviewed daily for intrusion and attack attempts; and
- CSB **must** be granted online access to firewall logs upon request.

2.1.8 Remote access

- Remote access to firewalls **must** be conducted through methods endorsed by CSB, and employ strong two-factor authentication;
- Remote administration of firewalls **must** be done in a manner that provides for two-factor authentication and connection security (e.g., encrypted sessions that employ approved cryptography);
- Modem connections to production firewalls **must** be prohibited;
- Separate, out-of-band network interface cards **must** be used for monitoring/administration;
- The Telnet protocol **must** be disabled; and
- The TFTP protocol **must** be disabled.

2.1.9 Change management

Change management procedures for firewalls must comply with the GO-ITS 35 Change Management standard. In addition to those requirements, the following are firewall specific requirements:

- Changes to firewalls **must** be tracked and documented, including technical details and impact assessment for the changes made;
- The date, time and name of the person responsible for each change must be recorded;
- Security patches **must** be installed as soon as practical (based on the severity of the issue corrected by the patch) and after appropriate testing;

- All rule changes which permit traffic from external networks with an ingress path to Government of Ontario internal networks **must** be approved by CSB prior to implementation;
- All changes **must** be tested and verified in a lab environment, unless there are mitigating circumstances preventing these activities from taking place (e.g. major emergency);
- All firewall rule change requests **must** include the following:
    - Requester information including name, contact information, ministry/agency information, cluster information, request date, and implementation date;
    - Detail explaining the rule and its function;
    - Expected working life of rule (including implementation and removal dates);
    - Source and destination information including application name, IP addresses, and ports;
    - Application information including name, owner, and owner contact information;
    - Business rationale associated with the request;
    - Impact statement associated with the request;
    - Test plan and back-out plan for the change;
    - Endorsement from the relevant Program Manager and Cluster Security Officer;
    - Endorsement from CSB and the Corporate Change Advisory Board;
- There **must** be periodic reviews of existing firewall rule sets; and
- Firewall rule sets should be rationalized as appropriate to maintain a compact configuration.

2.1.10 Configuration management

For each production firewall:

- The firewall configuration **must** be archived daily to a secure, isolated central server on a management segment;
- The firewall application and operating system (including software patches and updates) **must** be obtained from a trusted source that includes integrity checking;
- All default accounts and passwords **must** be replaced and configured securely, as per the GO-ITS 25.15 Password Management and Use standard;
- Any configuration changes which may result in the provision of access to external networks (including the addition or change of firewall rules) **must** be communicated to and reviewed by CSB (e.g., patches, hardware upgrades);
- Firewall configurations **must** be checked and tested, prior to and after implementation, for operating system and firewall application vulnerabilities;
- Firewalls **must** be centrally managed to provide a consistent level of security, and **must** be managed via a secure facility; and
- Access to firewall software (e.g., in repositories) **must** be limited, such that authorized firewall administrators are the only individuals with access.

2.1.11 Time synchronization

- All firewalls **must** obtain system time from a redundant and validated time source as per GO-ITS 25.0 General Security Requirements.

2.2 Desktop/Software/Personal firewalls

2.2.1 Base requirements

At a minimum, a personal desktop/laptop based firewall:

- **Must** operate at the network transport level, inspecting traffic on all interfaces prior to the point where the operating system forwards the information to client applications;
- **Must** perform stateful packet inspection and filtering;
- **Must** fail closed in the event of hardware or software failure;
- **Must** work/operate in conjunction with a VPN client (to protect clients connected via VPN tunnels);
- **Must** log system events, exceptions, and blocked traffic;
- **Must** employ a centralized policy management and reporting infrastructure;
- **Must** be transparent to users, and integrate seamlessly with the client operating system, without resulting in significant performance degradation;
- **Must** offer the capability to lock the firewall configuration and protect it from alteration;
- **Must** not rely on end users to make security-related decisions (e.g., provide choices via dialog boxes or questions);
- **Must** deny inbound connections to the client system, unless explicitly permitted by the policy.
- **Must** have the ability to make policy changes without rebooting or shutting down the system or firewall software.
- **Must** have the ability to group personal firewalls with similar policy requirements for flexibility and ease of management (e.g., such that a given branch or agency may have its own configuration);
- **Must** protect (e.g., encrypt) and mutually authenticate all central management traffic (e.g., policy changes, logging, and reporting);
- **Must** support passwords that conform to the requirements outlined in GO-ITS 25.15 Password Management and Use; and
- **Must** support role-based separation of duties for operations (e.g., permitting policy administration and activity monitoring to be delegated to different groups or individuals).

2.2.2 Logging and reporting

- Detected network attacks **must** be reported to the management console, and the malicious traffic **must** be logged either locally or remotely;
- Logged data **must** identify the source and destination of traffic;
- Attempts to stop and start a software or personal firewall, or introduce local policy changes, **must** be reported to the management console; and
- The management server **must** have the ability to produce customized reports as required.

2.2.3 Configuration management

- Firewall policies, patches and software updates **must** be managed according to the GO-ITS 35.0 Change Management Guide; and
- CSB **must** endorse any firewall policy changes for software, desktop, or personal firewalls.

3. RESPONSIBILITIES

Users of Firewalls

All firewall users are responsible for:

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

Program Managers

Program Managers are responsible for:

- Reviewing and approving business case for firewall rule change requests; and
- Completing Information Security and Privacy Classification and Threat Risk Assessments for new projects which require the deployment of firewall and/or security technology.

Infrastructure Technology Services (ITS)

ITS is responsible for:

- Managing network provider contracts for the provision of security services that may include firewall management;
- Implementing, managing and operating firewalls in accordance with the requirements in this document and other applicable Government policies and standards;
- Maintaining the firewall rules for devices deployed on Government of Ontario networks;
- Ensuring that appropriate security safeguards are in place to protect firewall devices, including those stipulated in this document and GO-ITS 25.0 General Security Requirements;
- Ensuring that the firewall logs are securely maintained, available when needed for investigations, and retained in accordance with this standard; and
- Monitoring Government of Ontario networks for unwanted traffic, and immediately notifying CSB contacts for appropriate action.

Network Service Provider

The Network Service Provider is responsible for:

- Implementing, managing and operating firewalls in accordance with the requirements in this document, GO-ITS 25.0 General Security Requirements, and other applicable Government policies and standards;
- Maintaining the firewall rules for devices within the Government of Ontario network which fall inside the scope of the network vendor contract;
- Ensuring that appropriate security safeguards are in place to protect the firewalls, including those stipulated in this document;
- Ensuring that the firewall logs are securely maintained, available when needed for investigations, and retained in accordance with this standard; and
- Monitoring managed networks for undesirable or suspicious traffic (on a daily basis) and immediately notifying CSB contacts for appropriate action.

Corporate Security Branch

The Corporate Security Branch (CSB) 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 firewall logs (on a daily basis) to detect malicious traffic and network attacks;
- Assessing the firewall change requests and defining solutions to meet the stated needs;
- Approving the firewall changes prior to their deployment into production;
- Authorizing use of debug or diagnostic modes on firewalls; and
- CSB reserves the right to require inspection, evaluation, and if necessary, removal of any resources that lower or defeat network security objectives.

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	MGS Corporate Security Branch

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

5. 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.

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

Authentication: 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.

Common Criteria: The Common Criteria is a framework within which end-users can specify their security requirements, vendors can implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate products to determine if they actually meet those claims. The Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standardized manner.

Confidentiality: The result of safeguards enforcing access to information consistent with the sensitivity of information, competitive position, and legislative requirements (e.g., FIPPA, PIPEDA, PHIPA).

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

Encryption: The transformation of data using cryptography into a form unreadable by anyone without the correct decryption key, ensuring 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.

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.

POTS (Plain Old Telephone Service): The provision and/or use of traditional wired telephone service to a telephone set, including analog data services.

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.

Protection Profile: A Common Criteria document published to identify the security functionality or requirements desired for a class of products intended for a particular purpose.

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.

Security Target: A Common Criteria document published to describe the security properties of the target of evaluation.

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 (as determined by ISPC).

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-attached devices for conditions that warrant administrative attention. Its latest revision is SNMPv3 is considered a full internet standard denoting the highest achievable maturity level since it offers three important security services, authentication, privacy and access control.

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

6. APPENDIX A: TRAFFIC MANAGEMENT

Permitted Internet traffic

This refers to traffic that can be forwarded via a firewall protecting Government of Ontario I&IT resources from an unmanaged network (e.g., the Internet). Such firewalls **must** deny, by default, all ingress traffic. The following services may be permitted for egress, however:

- HTTP / HTTPS
- FTP (preferably for authorized FTP sessions and known hosts only)
- DNS (queries from authorized internal DNS servers only)
- SMTP (for authorized SMTP servers only to prevent abuse)
- NTP (only from authorized internal hosts to known time servers)
- Encryption and key exchange protocols

Permitted DMZ traffic

This refers to traffic that can be forwarded via a firewall protecting Government of Ontario I&IT assets located within a demilitarized zone (DMZ). The firewall **must** deny, by default, all ingress and egress traffic. The following services may be permitted for ingress, however:

- HTTP / HTTPS
- SMTP (to authorized SMTP servers)
- DNS (queries to authorized DNS servers, and zone transfers from authorized hosts)
- Administration and support protocols (for management from internal networks)

Permitted external partner traffic

This refers to traffic that can forwarded via a firewall protecting Government of Ontario I&IT assets within internal networks but that provide authorized, documented access to third parties in partner or customer relationships with the Government. Such firewalls **must** deny, by default, all ingress and egress traffic, and ingress will be permitted based on business requirements and TRA findings.

Permitted internal traffic

This refers to traffic that originates within the Government of Ontario. These firewalls manage traffic within the integrated network, and can permit the following services:

- SSH (in both directions, from management zones)
- SNMP (in both directions, from authorized networks to authorized destinations)
- NTP (in both directions, from authorized internal hosts to known time servers
- ICMP ECHO REQUEST in both directions (for troubleshooting and management use)
- Administration and support protocols (for management from internal networks)

7. APPENDIX B: 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)
☐	Strategy, Policy and Planning Branch, ICS	
☐	Controllership Branch, (Corporate Architecture) ICS	
	Infrastructure Development Branch & ITS, OCCSD	
☑	Corporate Security Branch	May 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)	
☐	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)
Firewalls	Adherence to these security requirements will reduce the risks to Government I&IT resources. Requirements are in line with current practice and impact should thus be minimal.	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

International Common Criteria Portal:

http://www.commoncriteriaportal.org/

ISO/IEC Standards:
http://www.iso.org

Document history

Updated October 2008

- Changed contact information to reflect organizational changes
- Added details based on feedback received from end users of standard
- Adjusted to reflect current enterprise service offerings
- Minor changes to language
- Adjusted roles and responsibilities to reflect new agreement with integrated network provider
- Enhanced Common Criteria content
- Clarified permitted traffic, log requirements, linkages to external standards

Updated March 2012

- Organizational updates
- Updated hyperlinks and references
- Minor adjustments and errata

Updated June 12th, 2012

- Updates to consultations

Updated November 15th, 2012

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

Copyright