Ontario

Government of Ontario

Information & Technology Standards

Government of Ontario IT Standard (GO-ITS)

Number 25.8

Security Requirements for Servers

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 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.

Servers are a critical component of Government of Ontario I&IT strategy and infrastructure, as they provide the processing, storage, and application execution capability necessary to deliver services. As an integral component of these services, however, servers are both highly visible to attackers and susceptible to attack. To prevent compromise and subversion of servers within service delivery and operational environments, security requirements must be identified and adhered to for the design, development, deployment, management, and decommissioning of servers 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. 2nd, 2008	1.1	Tim Dafoe, CSB	Major structural revisions, language adjustments, and significant content overhaul
Mar. 14th, 2012		Tim Dafoe, CSB	Minor update as per document history
June 12th, 2012		Tim Dafoe, CSB	Updated consultation list
Nov. 15th, 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 computing and network infrastructure operated by, and on behalf of, the Government of Ontario is comprised of numerous components including servers. The level of risk posed to servers can be reduced significantly through the use of appropriate security methods and safeguards. There also exist legal, regulatory, compliance and business requirements that require certain kinds of diligence regarding the operation of Government servers.

This document sets out security requirements for servers deployed by, or operated on behalf of, the Government of Ontario. The objective of this document is to ensure that server operations do not result in unacceptable risks to Government of Ontario 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 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 Government of Ontario ministries, 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/or 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 25.8 Security Requirements for Servers apply to:

- All ministries of the Government of Ontario, and any organization that uses a ministry's or I&IT Cluster's information technology infrastructure; and
- All platforms and operating systems intended for use as servers.

[1] As determined via the Government's 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.

1.6 Principles

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

- Servers are a significant target for attack and misuse given their functional role to process data, provide access to information, perform transactions, and mediate services. It is critical that those deploying servers on behalf of the Government of Ontario understand that a robust security posture is required for all deployed server platforms, and that groups **must** exercise care in both the design and operation of servers.
- Ministries and agencies **must** be assured that I&IT resources are not jeopardized when servers are deployed and managed. This assurance is expressed in terms of confidentiality, integrity, availability, accountability, reliability and the opportunity for audit.
- The implementation of security measures on servers 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.

[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

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

2.1 Base standards

- Unnecessary network services on servers **must** be disabled (these services vary substantially between server platforms, but **must** be identified and disabled for every server instance);
- As per the least privilege principle outlined in GO-ITS 25.0 General Security Requirements, servers **must** operate using only those applications and software components required for their intended functionality and role;
- Hardware components not in use should be disabled or removed;
- Malware controls (and related software and/or services) **must** be deployed on any server platform capable of supporting them; and
- The operating system software/firmware revision and patch level **must** be kept current for the given release, in accordance with any requirements for approved standard products, and in a manner that supports production operations.

2.2 Physical security

- Production servers **must** be placed in a locked room accessible only to authorized personnel;
- Any operations or storage room should be free from electrostatic or magnetic interference and be environmentally maintained via HVAC, fire suppression, and other systems;
- If continuous operation of a production server is critical, an uninterruptible power supply (UPS) should be installed and spare system components kept on hand; and
- Physical access procedures for servers deployed within high-risk environments or which support the operation of systems processing sensitive information **must** be subject to authorization, change control, and all relevant access control as stated within GO-ITS 25.0 General Security Requirements.

2.3 Access control

- Password standards, and the mandatory requirement to eliminate default system passwords, **must** be enforced in accordance with the requirements stated in the GO-ITS 25.0 standard; and
- Authentication and authorization for server access **must** be performed via a centralized method, as per the GO-ITS 24.0 Omnibus IT Standard and GO-ITS 25.0 General Security Requirements.

2.4 Operating systems

- Operating systems on servers **must** be hardened against attack and misuse, using appropriate industry standard or best practice guidance for the hardening of the specific deployed platform, prior to being placed into production.

2.5 Server management

- As per GO-ITS 25.0 General Security Requirements, every authorized administrator of a server **must** be assigned, and use, a unique user account;
- Administrative access to servers in production environments **must** require strong, two-factor authentication;
- Any assignment of system privileges on servers **must** be restricted to authorized staff, and be granted via unique user accounts;
- Servers **must** be managed locally, or remotely through the use secure connections (e.g., those with secure session controls that provide for communications security via approved cryptography);
- Server management should be conducted from dedicated, secure management segments;
- Management of servers via sessions that originate from locations outside the Government of Ontario managed network **must** not be permitted, unless authorized via agreements (e.g., service providers that provide support or service from external locations);
- Application software installed on server systems **must** be hardened against attack and misuse, using appropriate industry standard or best practice guidance for the hardening of the specific application installed, prior to being placed into production.
- The I&IT Strategy and Cyber Security Division **must** have access to server configuration details upon request;
- Servers should not support the Telnet protocol; and
- The TFTP protocol and all "*r*" services (e.g., rlogin) **must** be disabled.

2.6 Logging and monitoring

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

- Servers **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 should be securely transferred to centralized logging servers;
- Logs **must** be available for online review for a minimum of six months;
- Archived logs **must** be maintained for two years and classified/safeguarded as per ISPC;
- Archived logs **must** be made available for online review within five business days;
- Consecutive failed access attempts **must** generate an alarm;
- Activity logs **must** contain at least the following, if applicable:
    - User name;
    - Configuration changes or actions associated with the user, connection, or session;
    - Source of inbound connection or session (e.g., device, node, IP address); and
    - Time stamp with date;
- Activity logs **must** be reviewed daily to detect indications of misuse, intrusion, and/or attack; and

- Activity logs **must** provide information regarding server use, the following events **must** be logged as a minimum requirement:
    - Duration of sessions, with time stamps for login and logout;
    - Local and remote authentication attempts (successful and failed);
    - Attempts to manage accounts, users, and groups (successful and failed);
    - Attempts to alter policies or the rights assigned to users (successful and failed);
    - Attempts to alter the system run level or security settings (successful and failed);
    - Escalation and/or use of system privileges (successful and failed); and
    - System events, such as server reboot or system time changes (successful and failed).

2.7 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 servers 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 servers **must** differ from those used on other technology platforms (e.g., routers, firewalls), 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;
- Servers 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.

2.8 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 server specific requirements:

- Changes made to servers **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);
- Server operating systems will require periodic patching and updates, which **must** be installed as soon as practical (based on severity of patch) and after appropriate testing;

- 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 (e.g., a major emergency);
- All server 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;
- Any change control process implemented for the management of servers **must** account for the complete lifecycle of the servers (e.g., from the planning stage, through to implementation and management, eventually resulting in removal and/or disposal); and
- Accurate documentation of changes **must** be kept throughout the lifecycle of production servers.

2.9 Configuration management

- Server configuration information **must** be archived to a secure central location;
- Server configuration information **must** be backed up daily;
- Operating system updates (e.g., software patches) **must** be obtained from a trusted source that includes integrity checking;
- Production server configuration changes with potential security implications **must** be communicated to and reviewed by the I&IT Strategy and Cyber Security Division (e.g., significant upgrades, mitigation strategies for security issues regarding vulnerabilities, patches, and/or workarounds);
- Configurations **must** be validated and tested, before and after implementation, for operating system and application vulnerabilities; and
- Servers **must** be centrally managed to provide a consistent level of security, and **must** be managed via a secure facility (e.g., a dedicated management segment protected by a layer three firewall, with access granted to authorized administrators only).

2.10 Time synchronization

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

2.11 Virtual servers

Virtual server technology is sometimes employed to reduce costs or consolidate infrastructure. It is critical that planning and risk analysis be conducted to ensure that this technology is used in an appropriate fashion in environments where sensitive data is processed or stored.

Use of virtual server technology **must** comply with GO-ITS 25.0 General Security Requirements. In addition, the following requirements apply for production servers within the Government of Ontario:

- Virtual server technology **must** not be deployed in an attempt to logically separate sensitive information from less sensitive or unclassified information;
- Virtual server technology **must** never be deployed as a sole or primary security safeguard in the design or operation of a server environment; and
- Virtual server technology **must** be complimented with additional security safeguards and planning when deployed in production environments.

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 their computing devices 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 cases for server change requests;
- Ensuring such changes comply with the requirements in this document; and
- Completing Information Security and Privacy Classification and Threat Risk Assessments for new projects that require server deployment.

Infrastructure Technology Services (ITS)

ITS is responsible for:

- Implementing, managing and operating servers which fall outside of vendor network support contracts in accordance with the requirements in this document and other applicable Government policies and standards;
- Managing changes for servers operated under ITS control in accordance with the requirements in this document;
- Maintaining the secure operation, confidentiality, availability, and integrity of any servers ITS deploys and manages;
- Ensuring that appropriate security safeguards are in place to protect the servers, including those stipulated in this document; and
- Ensuring that the server logs are securely maintained, available when needed for investigations, and retained in accordance with this standard.

Network Service Provider

The Network Service Provider is responsible for:

- Implementing, managing and operating servers within the scope of support contracts in accordance with the requirements in this document and other applicable Government policies and standards;

- Maintaining the secure operation, confidentiality, availability, and integrity of any servers it deploys and manages;
- Ensuring that appropriate security safeguards are in place to protect the servers, including those stipulated in this document; and
- Ensuring that the server logs are securely maintained, available when needed for investigations, and retained in accordance with this standard.

I&IT Strategy and Cyber Security Division (SCS):

SCS, 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 server and network logs to detect misuse, suspicious activity, and attacks;
- Assessing server change requests and defining solutions to meet the stated needs;
- Approving any relevant changes prior to their deployment in production environments; and
- Reserving 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	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

5. 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).

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.

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): Anattempt 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.

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 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.

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: One of the core protocols of the Internet protocol suite, ICMP is by networked devices 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.

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: 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 is an inspection of the data "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 (e.g., silently discard) the packet, or reject it (discard it, and send an error response to the source, often via the Internet Control Message Protocol (ICMP)).

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.

***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*.

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 incident 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.

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 (SNMP version 3) is considered a full Internet standard denoting the highest achievable maturity level, since it offers three important security services (authentication, communications security, and access control).

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.

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.

6. 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	
	Infrastructure Development Branch & ITS, OCCSD	
☑	Corporate Security Branch (Cyber Security Branch)	Jun. 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)
Servers	Adherence to these security requirements will reduce the risks to Government I&IT resources.	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 25 standards:

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

Document history

Updated October 2008

- Changed contact information to reflect organizational changes
- Added details based on feedback received from end users of standard
- Minor changes to language
- Adjusted roles and responsibilities to reflect new agreement with integrated network provider
- Included information regarding virtual servers
- Aligned with revised/approved GO-ITS 25 series standards

Updated March 2012

- Organizational updates
- Updated roles
- Updated hyperlinks and references
- Minor adjustment

Updated June 12th, 2012

- Updated consultation list

Updated November 15th, 2012

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

Updated January 19th, 2015

- Minor updates as per rationale submitted to ARB (administrative/organizational updates, ISO/IEC alignment), draft document version number set to 1.2

Version 1.3

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

Copyright & Disclaimer

For third party users, including government contractors and entities seeking to provide products or services to the Government of Ontario, the Government of Ontario does not represent or warrant to you the accuracy, suitability or completeness of the content of this document.