_____

Government of Ontario

Information
&
Technology
Standards

Government of Ontario IT Standard (GO-ITS)

Number 25.5
Security Requirements for Wireless Local Area Networks

Version #: 2.0

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

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.

Wireless Local Area Networks (WLAN) provide a efficient means to connect local computer systems via radio signals, and enable users to roam (using portable computing devices) within a building or facility. While business cases exist for the deployment of this technology, without proper safeguards the radio signals from WLANs can be used to gain unauthorized access to system and network resources, or be captured by attackers for the purpose of intercepting sensitive information.

Version Control

Date	Version	Author	Comment
May 18, 2005	1.0	Earl Kuntz, CSB	Original document endorsed by IT Standards Council (ITSC)
June 29, 2005	1.8	Earl Kuntz, CSB	Approved changes authorized by Architecture Review Board (ARB)
October 8, 2008	1.9	Tim Dafoe, CSB	Major revisions to roles and responsibilities, technical updates, adjustments to reflect enterprise solution, includes comments from ITSC reviewers, SAWG, and Audit, final version for ARB
March 14, 2012		Tim Dafoe, CSB	Updates as per document history
June 11, 2012		Tim Dafoe, CSB	Updates to GO-ITS references, consultations
Nov. 15, 2012	2.0	Tim Dafoe, CSB	Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 2.0

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.

This document sets out security requirements for wireless LANs (WLANs) within the Government of Ontario (the Government). The objective of this document is to ensure that use of WLANs will not result in an unacceptable level of risk to 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, 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 wording conventions are followed. There are precise requirements and obligations associated with the following terms:

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

1.5 Application and scope

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 integrated network and use computing 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 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 25.5 Security Requirements for Wireless LANs (WLANs) 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
- All information technologies that support WLANs, all computing devices that are networked using a WLAN, and all users of such devices.

1.6 Out of scope

These requirements are specific to IEEE 802.11 wireless LAN implementations, and do not apply to other types of wireless communication (e.g., BlackBerry, cellular phones, or Bluetooth technology).

---

[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 Security:[2]

- Ministries and agencies **must** be assured that I&IT resources are not jeopardized by the use of WLANs. This assurance is expressed in terms of confidentiality, integrity, availability, accountability, reliability and opportunity for audit.

- WLANs are inherently vulnerable to data interception, denial of service, unauthorized access, and may be seen by attackers as platforms from which to launch attacks on Government of Ontario (or other) computer networks. The security exposure of WLANs is fundamentally different than that of traditional wired networks. Significant security measures **must** be in place to minimize the risks associated with their use within the Government.

- The implementation of security measures to safeguard WLANs does not diminish the need for program managers to ensure Threat Risk Assessments are conducted for each program and appropriate security measures are in place to protect program applications, information and resources. The business requirement for WLAN deployment should be documented due to the increased vulnerability of these networks.

- An enterprise WLAN service **must** be compliant with this standard. Any interim or other WLAN deployment, however, **must** similarly be compliant with the requirements identified in this standard.

---

[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

2. REQUIREMENTS

The following security requirements apply to wireless LAN deployment and operation:

2.1 Assessment

Implementation or use of WLANs is discouraged when sensitive program information or services are involved, or when availability **must** be assured (particularly when determined via a Threat Risk Assessment (TRA). Before a WLAN is deployed, the program area **must** consider the sensitivity[3] of the relevant program information and the risks involved (as determined by ISPC policy and a TRA that has been endorsed by CSB). A TRA will determine the risk associated with the program as it relates to WLAN deployment, and may also produce recommendations for additional security consideration. Documented business rationale and management approval **must** exist for the deployment of WLAN services.

2.2 Education and training

Operations staff must be made aware of the risks inherent in the use of WLANs, and the safeguards that must be implemented to mitigate these risks.

All Government WLAN users must be aware of the sensitivity of information (as per ISPC policy) and related applications they will access via a WLAN, and the procedures involved in securely accessing WLAN services.

Depending on their activities, WLAN users may require additional education and/or training in accordance with other policies and/or best practices (e.g., GO-ITS 25.7 Security Requirements for Remote Access Services, and GO-ITS 25.10 Security Requirements for Mobile Devices).[4]

2.3 Wireless LAN implementation

WLANs **must** only be deployed in situations where the program/business area has a specific and documented business need (e.g., a requirement for roaming, or excessive cost of installing additional network cable in older buildings, or other rationale), and the risks involved have been determined to be acceptable (given the information handled by the program/business area).

Program managers **must** utilize authorized WLAN solutions for implementation (e.g., an offered enterprise WLAN service) within the Government if one is available. If such a solution is not made available, the Cluster Chief Information Officer or his/her delegate **must** authorize any other proposed implementations, and ensure they comply with the requirements stated in this document.

A registry of any non-enterprise WLAN implementations **must** be maintained by I&IT Clusters that includes the following information:

---

[3] As per the Information Security and Privacy Classification Policy (ISPC).

[4] GO-ITS 25 security standards can be found at http://intra.collaboration.gov.on.ca/mgs/occio/occto/our-services/technology-adoption/technical-standards-1/approved-go-its-standards/.

- The ministry, branch, or program using the WLAN;
- The sensitivity of the program information involved;
- The physical location of the associated access point(s);
- The specific IEEE wireless standard and associated security technology in use;
- The Service Set Identifier (SSID) for each deployed access point; and
- Contact information for the program manager and operations group responsible for the WLAN deployment.

Program managers and operations staff **must** be made aware that SSID values are public information (even when SSID announcement within IEEE 802.11 beacon frames is disabled on WLAN access point devices).

2.4 User account management

WLAN accounts **must** only be provided to Government employees or contractors who have a valid business reason for WLAN access. The responsible program manager or his/her delegate **must** authorize access to a given WLAN access point.

WLAN accounts **must** be managed in accordance with the requirements stated in GO-ITS 25.0 General Security Requirements. In particular, they **must** not be shared and **must** be terminated within 24 hours of provided notice, if access is no longer required.

A secure and current list of all individuals who have WLAN accounts **must** be maintained for each implementation. The list of WLAN users **must** include the following information:

- User contact information;
- The WLAN access points the user is authorized to access;
- The programs and/or branches involved;
- The date that access was granted and/or terminated; and
- The name and title of the program manager who authorized the user account.

In the case of a WLAN account intended for use by a peripheral device (e.g., a wireless print server or camera device), the list of WLAN users **must** include the individual responsible for the peripheral device. Any peripheral device using WLAN **must** be assigned an individual account, and these accounts **must** similarly be recorded in the list of current, authorized WLAN accounts.

2.5 Identity authentication and authorization

Access to a Government WLAN deployment **must** only be granted to an individual whose identity has been verified. The program manager responsible for the WLAN (see User Account Management) **must** authorize and document this access on a per-user basis.

The authentication/authorization mechanism for any WLAN operated within or on behalf of the Government **must** be centralized, and based on:

- The IEEE 802.1x standard as specified in GO-ITS 39.1 WLAN Technical Standard and

Specifications; and

- The IETF RADIUS standard as specified in GO-ITS 39.1 WLAN Technical Standard and Specifications.

The implementation of the authentication/authorization mechanism used **must** also comply with GO-ITS 25.0 General Security Requirements.

There **must** be reliable, robust mutual authentication between the computing device and the WLAN access point, as well as between the user and the authentication server. The user and device **must** be reliably associated.

The authentication process **must** take place before a network address is assigned to the client hardware the user is attempting to associate with the WLAN.

Failures to provide correct authentication credentials **must** result in denied access. All such instances **must** be logged, monitored, and reviewed.

2.6 Computing devices on wireless LANs

Only computing devices issued by the Government can be used on a WLAN. All other equipment **must** not be associated with or granted access to Government WLANs.

Wireless adapters on Government-issued computing devices **must** be:

- Compliant with approved IEEE 802.11 standards (as specified in the GO-ITS 39.1 WLAN Technical Standard and Specifications);

- Secure against known attacks and vulnerabilities[5]; and

- Configured with *ad hoc* mode disabled in a manner that cannot be reversed by the user (e.g., infrastructure mode only).

Computing devices **must** be configured to prevent users from establishing a separate connection with another network while connected to the Government network via a WLAN. Users **must** be prevented from circumventing this control.

Peripheral devices that are connected to a WLAN **must** be configured to employ authenticated, secure WLAN connections.

2.7 Wireless LAN equipment

2.7.1 Implementation of wireless access points

Government WLANs **must** deploy access point (AP) equipment that is:

- Configured to protect information communicated during the establishment and operation of any session or connection between Government computing devices and the WLAN AP;

- Compliant with current and approved IEEE 802.11 standards;

---

[5] To satisfy this requirement, software and/or firmware updates that address known vulnerabilities in adapters or related software **must** be applied promptly.

- Configured to employ approved cryptography endorsed by CSB for the protection of sensitive information, as per GO-ITS 25.12 Use of Cryptography;

- Separated using a DMZ design from the Government network by a stateful, layer-three boundary control device (e.g., firewall) that can operate in conjunction with a separate intrusion detection sensor;

- Protected against physical access by unauthorized individuals (e.g., tamperproof design or enclosure, physical security controls, and placement of access points in inconspicuous locations);

- Deployed to minimize radio signal coverage beyond the intended service area via the use of site surveys, position of antenna(s), or reduction in radio transmission power;

- Configured with a purposefully chosen SSID that does not contain any identifying information about the Government program using the WLAN;

- Configured such that the SSID value is not announced in 802.11 beacon frames;

- Configured with SNMP community strings that are compliant with GO-ITS 25.15 Password Management and Use, with SNMP version 3 enabled;

- Supplemented with additional access control and boundary control devices that augment the security capabilities of the WLAN implementation; and

- Maintained in compliance with current Corporate and Cluster technical standards and procedures.

End-to-end encryption may be required for some sensitive program areas as recommended by a TRA. WLAN encryption and/or authentication may not be sufficient for all applications.

2.7.2 Management of wireless access points

Administrative access to WLAN access points **must** be limited to authorized and trained technical staff. Administrative access to WLAN access points and associated firewalls or other access control devices should require two-factor authentication. Any remote administration **must** be carried out via a secure connection (e.g., using approved cryptography).

When an access point is being disposed of and/or removed from service, it **must** be wiped clean of configuration details (e.g., network information, cryptographic keys, and passwords).

Access point management protocols that are insecure or not utilized should be disabled.

All WLAN access points **must** support firmware upgrades so that patches, evolving security capabilities, and new technologies can be deployed as they become available and approved for use within the Government.

2.7.3 Monitoring wireless LANs

Networks **must** be monitored to detect unauthorized installations of WLANs and installations that do not comply with the requirements in this document. Such installations should be immediately disconnected from the Government network, as they represent an immediate and serious threat to the confidentiality and integrity of sensitive information.

All logging activity **must** be compliant (and have both a format and storage mechanism that complies) with the requirements stated in the GO-ITS 25.0 General Security Requirements.

Intrusion detection systems **must** support or be adapted to support the ongoing automated monitoring of WLANs.

Logging is essential for the provision of monitoring and accountability, and assists in identifying and tracking potential intruders. All authentication activity on the WLAN **must** be reliably and centrally logged, and client hardware should be linked to the authorized account of each individual granted WLAN access. These logs **must** be secured, made tamper resistant, reviewed regularly, and retained in accordance with GO-ITS 25.0 General Security Requirements.

3. RESPONSIBILITIES

WLAN Users

All WLAN users are responsible for:

- Complying with directives, policies and agreements when accessing or using Government information, equipment and services;
- Ensuring security safeguards installed to protect their wireless computing device are not disabled or tampered with;
- Ensuring that Government information and devices are protected from access by unauthorized individuals; and
- Reporting any suspected security breaches to the IT Service Desk.

Program Managers

Program Managers are responsible for:

- Documenting the business case for any WLAN deployment, unless an enterprise service is available and will be used;
- Ensuring that WLAN users are aware of and adequately trained in their responsibilities as set out in this document, and other related Government policies;
- Authorizing individual users and/or peripheral devices to be granted access to a WLAN, and documenting this access;
- Ensuring that individual access to a WLAN is terminated within 24 hours when no longer required;
- Ensuring that a TRA, business continuity plan (BCP), and disaster recovery plan (DRP) exist for WLAN implementations, unless an enterprise service is available and will be used;
- Reporting unauthorized WLAN implementations to the IT Service Desk; and
- Reporting any security exposures or suspected security incidents to the IT Service Desk.

Cluster Chief Information Officers

Cluster CIOs are responsible for:

- Reporting any security exposures or suspected security incidents to the IT Service Desk.
- Authorizing WLAN implementation in ministries and organizations supported by the I&IT Clusters based on business need and risk assessment, while enforcing the requirements in this document;
- Ensuring that employees use an enterprise WLAN solution, if one is available for use;
- Ensuring that a Threat/Risk Assessment is completed and endorsed by CSB before proceeding with a request for a WLAN implementation; unless an enterprise service is available for use; and

- Supporting security incident reporting and management procedures as per GO-ITS 37 Incident Management.

IT Clusters

IT Clusters are responsible for:

- Supporting program managers in the completion of Information Security and Privacy Classification and a Threat/Risk Assessment for any proposed deployment or new program use of a WLAN;
- Monitoring and ensuring that any WLAN implementations comply with the requirements in this document and other Corporate and Cluster policies and standards (if a enterprise service is not available for use), and taking action if unauthorized deployments are identified;
- For non-enterprise services, maintaining an up-to-date registry of local WLAN implementations, and a list of associated WLAN users that includes the information required in this document;
- Promoting use of an enterprise WLAN service; and
- Promoting WLAN security education and awareness within their cluster.

Infrastructure Technology Services (ITS)

ITS is responsible for:

- Managing the vendor contract for the provision of an enterprise WLAN service;
- Ensuring that agreement(s) with the network service provider shall bind them to the requirements in this document;
- Ensuring that computing devices used for access to a WLAN meet Corporate and Cluster requirements for Government IT equipment, including those stipulated in this document;
- Endorsing use of the enterprise WLAN service;
- Providing service desk and incident escalation support to WLAN users; and
- Ensuring that a security assessment on the WLAN service is completed when a major change is made that could introduce new threats or vulnerabilities, and adhering to all required change management policies and procedures.

Network Service Provider

The Network Service Provider is responsible for:

- Implementing, managing and operating enterprise WLAN access points in accordance with the requirements in this document and other applicable Government policies and standards;
- Maintaining the firewalls used to separate access points from the Government network and adhering to the GO-ITS 25.6 Firewalls standard;
- Ensuring that appropriate security safeguards are in place to protect the WLANs, including, at a minimum, those stipulated in this document;

- Ensuring that a site survey / assessment is conducted for any area to be covered by a WLAN implementation; and
- Ensuring that the audit log for the authentication server is securely maintained, reviewed regularly, made available when needed for investigations, and retained in accordance with GO-ITS General Security Requirements and all other relevant agreements.

Ontario Internal Audit Division

The Ontario Internal Audit Division is responsible for:

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

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;
- Ensuring that all stakeholders are informed and aware of their responsibilities in relation to WLAN by making this document available to them;
- Completing TRAs (or endorsing those completed by others) and security assessments;
- Managing, evaluating, and endorsing any exceptions to this standard;
- Endorsing authentication mechanisms and cryptography for use within the Government;
- Providing services to support the identity authentication and authorization mechanisms required for robust user management;
- Assessing the WLAN logs as needed for investigations into potential attacks or inappropriate behaviour, and notifying the appropriate individuals of suspected security breaches;
- Monitoring compliance with the requirements in this document in conjunction with ITS, the network service provider, Internal Audit, and the I&IT Clusters; and
- Monitoring the Government network for WLANs that are unauthorized, or do not comply with these requirements, and immediately notifying ITS or the Network Service Provider for appropriate action.

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

Kit-Mei Chan, Ministry of Transportation

4.4 Reviewers

The following groups have reviewed this standard:

Ontario Internal Audit Division

5. DOCUMENT HISTORY

Version 1.0 Endorsed by IT Standards Council (ITSC): May 18, 2005

Version 1.8 Approved by Architecture Review Board (ARB): June 29, 2005

- Added new template wording to start of Application and Scope section and made minor changes to existing text in that section.
- Changed Contact Information
- Changed WLAN Responsibilities for Integrated Network Service Provider to refer to "WLAN access points" rather than "WLANs" and dropped superfluous text in the Implementation of Wireless Access Points section.

Updated Draft June, 2008:

- Changed contact information to reflect organizational changes
- Added details based on feedback received from end users of standard
- Adjusted to be reflective of enterprise solution being piloted and readied for deployment
- Minor changes to language
- Adjusted roles and responsibilities to reflect new agreement with integrated network provider

Version 1.9 Endorsed by ITSC August 20, 2008; Approved by ARB October 16, 2008

Updated March 14th, 2012:

- Updated organizational details and roles
- Updated hyperlinks and reference
- Minor errata
-

Updated June 12th, 2012:

- Updated consultation details

Updated November 15th, 2012:

- Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 2.0

6. DEFINITIONS

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

Access Point: A WLAN access point is a small radio-based receiver/transmitter typically with one or two antennas. It is connected to a wired LAN (or broadband connection) via Ethernet. Computing devices equipped with wireless network adapters can connect to an access point, and gain access to the LAN.

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

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

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.

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.

Electronic Network: Computer systems that can communicate with each other via a medium, including the Internet, networks internal to an institution, and remote 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.

IEEE 802.1x: An IEEE standard for authentication that features a port-based authentication framework allowing the use of many types of authentication methods.

IEEE 802.11: A family of specifications developed by the IEEE for wireless LAN technology. The 802.11suite specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

IEEE 802.11i: An IEEE 802.11 security standard for wireless LAN technology established in 2004 that addresses security vulnerabilities with earlier 802.11 standards (802.11a/b/g). The 802.11i standard includes 802.1x authentication and support for the Advanced Encryption Standard (AES).

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.

Mutual Authentication: Also referred to as two-way authentication refers to two parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

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.

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.

RADIUS (Remote Authentication Dial-In User Service): A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize their access to the requested system or service.

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.

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).

SSID (Service set identifier): A common name that identifies a WLAN. Clients are normally configured with the SSID of the WLAN that they need to access. While the SSID should be shared only with those having legitimate need to access the network, it is public information (even when SSID broadcast is disabled).

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

Virus: An unauthorized program that copies itself into other programs whenever the trigger mechanism is executed.

Wireless adapter: A wireless adapter functions like a network interface card (NIC), and allows the client computing device to access a LAN via a wireless access point.

WLAN (Wireless LAN): A type of Local Area Network (LAN) that uses high frequency radio waves rather than wires to communicate and transmit data among nodes. It is a flexible data communication system implemented as an extension to (or as an alternative for) a wired LAN within a building or

campus. The physical data medium is placed into the public domain, however, introducing a number of vulnerabilities.

WPA (Wi-Fi Protected Access): A security standard established by the Wi-Fi Alliance as an interim standard to address WLAN security issues, while IEEE 802.11i was in development. It introduced TKIP (Temporal key integrity protocol) to address documented weaknesses within the WEP encryption scheme, and incorporated the 802.1x authentication standard.

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) GO 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	May 2005
☑	Controllership Branch, (Corporate Architecture) ICS	Sept 2004
	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)	Oct 2004
☐	Cluster ACT/ARB (for Cluster standards promoted to Corporate standards)	
☑	IT Executive Leadership Council (ITELC)	March 2005
☑	IT Standards Council (ITSC)	June 2008
☑	ITSC Wireless Working Group	Nov 2004
☑	Network Office, *ITS*	Sept 2004
☑	Network Management Committee	April 2005

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
GO-ITS 39.1	GO-ITS 39.1 provides technical standards and specifications for wireless LANs.	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)
Wireless LANs	Adherence to these security requirements will reduce the risks to Government I&IT resources that are inherent in the use of wireless LANs.	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.collaboration.gov.on.ca/mgs/occio/occto/our-services/technology-adoption/technical-standards-1/approved-go-its-standards/

> *GO-ITS 25.0 – General Security Requirements*
>
> *GO-ITS 25.7 – Security Requirements for Remote Access Services*
>
> *GO-ITS 25.10 – Security Requirements for Mobile Devices*
>
> *GO-ITS 25.12 – Use of Cryptography*
>
> *GO-ITS 25.15 – Password Management and Use*
>
> *GO-ITS 37.0 – Incident Management*
>
> *GO-ITS 39.1 – WLAN Technical Standard and Specifications*

Copyright