



**CORPORATE SECURITY
INFORMATION TECHNOLOGY**

**Security Requirements for
Wireless Local Area Networks**

Government of Ontario IT Standards (GO-ITS)

Document No. 25.5

Version 1.8

Status: Approved

OCCIO

**MANAGEMENT BOARD SECRETARIAT
CORPORATE SECURITY BRANCH**

Last Review Date: June 29, 2005

Foreword

Government of Ontario Information & Technology Standards (GO-ITS) are the official publications on the standards, guidelines, technical reports and preferred practices adopted by the Information Technology Standards Council under delegated authority of the Management Board of Cabinet. These publications support the Management Board Secretariat's responsibilities for coordinating standardization of Information and Technology in the Government of Ontario.

Publications that set new or revised standards provide policy guidance and administrative information for their implementation. In particular, they describe where the application of a standard is mandatory and specify any qualifications governing its implementation.

Table Of Contents

<i>Purpose of the Standard</i>	4
<i>Versioning and/or Change Management</i>	4
Contact Information	4
<i>Application and Scope</i>	5
<i>Principles</i>	6
<i>Security Requirements</i>	7
Security Assessments	7
Education and Training.....	7
Wireless LAN Implementation	8
User Account Management	8
Identity Authentication and Authorization	8
Computing Devices on WLANs	9
Implementation of Wireless Access Points	9
Management of Wireless Access Points	10
Monitoring Wireless LANs	10
<i>Responsibilities</i>	11
WLAN Users	11
Program Managers	11
Cluster Chief Information Officers	11
I&IT Clusters	11
iSERV Ontario	12
Integrated Network Service Provider.....	12
Corporate Security Branch	12
<i>Definitions</i>	13
<i>Appendix A: IEEE 802.11 SSID Naming Standard</i>	16
<i>Appendix B: Additional Information</i>	17
Type of Standard	17
Publication	17
Consultation.....	18
Impacts to Standards.....	19
Impacts to Existing Environment	19
<i>References</i>	20
<i>Errata</i>	21
<i>Copyright</i>	21

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.

Wireless Local Area Networks (WLAN) provide a means to quickly network local computing devices and enable users to roam with their portable computing devices within a building or facility. However, without proper risk mitigation measures, radio signals from WLANs can be captured easily by individuals outside the building and used to intercept confidential Program information and/or gain unauthorized access to resources.

This document sets out security requirements for WLANs within the Government of Ontario (the Government). The objective of this document is to ensure that the use of WLANs does not result in unacceptable risks to Government Information and Information Technology (I&IT) resources.

Versioning and/or Change Management

On-going ownership and responsibility for maintenance and evolution of this document resides with the Corporate Security Branch, Office of the Corporate Chief Information Officer. 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.

Contact Information

	Contact 1	Contact 2
<i>Name</i>	Doug Whyte, Manager	Earl Kuntz, Security Policy Advisor
<i>Organization/ Ministry</i>	Management Board Secretariat	Management Board Secretariat
<i>Division</i>	OCCIO	OCCIO
<i>Branch</i>	Corporate Security Branch	Corporate Security Branch
<i>Section/ Unit</i>	Strategy and Contingency Services	Security Policy
<i>Office Phone</i>	416-327-3084	416-327-2326
<i>E-mail</i>	doug.whyte@mbs.gov.on.ca	earl.kuntz@mbs.gov.on.ca

Application and Scope

Government of Ontario IT Standards and Enterprise Products apply (are mandatory) for use by all ministries/clusters and to all former Schedule I and IV provincial government agencies under their present classification (Advisory, Regulatory, Adjudicative, Operational Service, Operational Enterprise, Trust or Crown Foundation) according to the current agency classification system.

Kindly refer to http://intra.pmed.mbs.gov.on.ca/mbc/pdf/Agency_Establishment&Accountability-Dir.pdf for a list of provincial government agencies with their classification under the current classification system, as well as their previous Schedule under the former Schedule system.

Additionally, this applies to any other new or existing [agencies designated by Management Board of Cabinet](#) as being subject to such publications, i.e. the [GO-ITS](#) publications and mandatory [Enterprise Products](#) - and particularly applies to Advisory, Regulatory, and Adjudicative Agencies (see also procurement link, [OPS paragraph](#)). Further included is any agency which, under the terms of its Memorandum of Understanding with its responsible Minister, is required to satisfy the mandatory requirements set out in any of the Management Board of Cabinet Directives (*c.f.* Operational Service, Operational Enterprise, Trust, or Crown Foundation Agencies).

As new GO-IT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity). When implementing or adopting any GO ITSC standards or GO ITSC standards updates, 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 in place and employed.

For security involving sensitive information, 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 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.

For the purposes of this document, any reference to ministries or the Government includes applicable agencies.

Out of Scope:

These requirements do not apply to other types of wireless communication; e.g., BlackBerries, cell phones.

Principles

These principles are in accordance with the “Information and Information Technology Security Directive”:¹

- 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: accountability, confidentiality, integrity, availability, reliability and auditability.
- WLANs are inherently vulnerable to data interception and unauthorized access and to being used as a platform to attack other areas of the Integrated Network. 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 risk assessments are conducted for each program and appropriate security measures are in place to protect program applications, information and resources.

¹ The Information and Information Technology Security Directive can be found at:
<http://intra.security.gov.on.ca/resources/default.asp>

Security Requirements

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

Must	This requirement is not optional. Without this, the system is deemed to be insecure.
May	The implementer <i>may</i> choose to take one or more of a selection of options, but <i>must</i> make a choice of one or more, as dictated within the context of the item.
Should	The implementer <i>must</i> choose this action, <i>unless</i> business functionality dictates otherwise. Exceptions <i>must</i> be detailed and approved in writing, by management, as modifications to the standard practice.

Security Assessments

WLANs are discouraged when high sensitivity Program information or services are potentially involved. Before a WLAN is deployed, the Program area must consider the sensitivity² of the relevant Program information and the risks involved as determined by a Threat/Risk Assessment that has been endorsed by the Corporate Security Branch.

Education and Training

Network and technical staff must be 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 and/or applications they will access via a WLAN, and the procedure for promptly reporting any suspected security compromise.

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, GO-ITS 25.10 Security Requirements for Mobile Devices³.

² The Information Security and Privacy Classification Policy and Operating Procedures can be accessed at <http://intra.security.gov.on.ca/resources/>

³ GO-ITS 25 Security Standards can be accessed at: <http://intra.security.gov.on.ca/resources/>

Wireless LAN Implementation

WLANs must only be deployed in situations where the Program/Business area has a clear business need (e.g., need for roaming, excessive cost of installing cabling in an old building) and the risks involved are acceptable (see Security Assessments).

As WLANs within the Government are part of the Integrated Network, only an authorized solution can be implemented and only with the approval of the Cluster Chief Information Officer or his/her delegate.

A registry of WLAN implementations must be maintained by the I&IT Clusters that includes: the ministry/branch using the WLAN, the sensitivity of the Program information involved, the location of the WLAN, the wireless standard in use, the Service Set Identifier (SSID) and contact information for the Program Manager responsible for the WLAN.

User Account Management

WLAN accounts must only be provided to Government employees or contractors who have a valid business reason. Their access to a given WLAN Access Point must be authorized by the responsible Program Manager or his/her delegate.

WLAN accounts must not be shared and must be terminated promptly when no longer required.

A secure and up-to-date list must be maintained of all individuals who have WLAN accounts (WLAN users). The list of WLAN users must include their contact information, the WLAN Access Points that they are authorized to access, the Programs/Branches involved, the date that access was granted and terminated, and the name and title of the Program Manager who authorized their access to a given Access Point.

In the case of a WLAN account for a peripheral device (e.g., print server), the list of WLAN users must include the individual responsible for the peripheral device.

Identity Authentication and Authorization

Access to a WLAN Access Point connected to the Integrated Network must only be granted to an individual whose identity has been authenticated and only if he/she is authorized by the Program Manager responsible for the WLAN (see User Account Management).

The authentication/authorization mechanism must be centralized⁴ and based on the IEEE 802.1x standard as specified in GO-ITS 24 Omnibus IT Standard (e.g., IETF RADIUS standard as specified in GO-ITS 24 Omnibus IT Standard for the authentication, authorization and accounting (AAA) server). The implementation of the authentication/authorization mechanism must comply with GO-ITS 25 Security Standards.

There must be mutual authentication between the user and the authentication/authorization server.

⁴ Although the authentication/authorization mechanism must be centralized, the administration of the user profiles may be decentralized; i.e., performed by the I&IT Clusters.

Computing Devices on WLANs

Only Government-issued computing devices⁵ can be used on a WLAN that is connected to the Integrated Network.

Wireless adapters on Government-issued computing devices must be compliant with approved IEEE 802.11 standards as specified in GO-ITS 24 Omnibus IT Standard, up-to-date⁶ and configured with ad hoc mode turned off (i.e., infrastructure mode only) to prevent unauthorized wireless access to the device and its data.

Computing devices must be configured to prevent users from establishing a separate connection with another network while connected to the Integrated Network via a WLAN.

Peripheral devices that are connected to a WLAN must be configured for a secure WLAN connection (e.g., use of an authenticated wireless print server with encryption).

Implementation of Wireless Access Points

Implementers of Government WLANs must ensure that the Access Point (AP) equipment is:

- Configured to protect information communicated during the establishment, existence, and completion of a connection between computing devices and the WLAN AP⁷;
- Compliant with the current IEEE 802.11 standards and the FIPS-compliant AES encryption standard (used by IEEE 802.11i) as specified in GO-ITS 24 Omnibus IT Standard and endorsed by the Corporate Security Branch for wireless LAN deployments within the Government;
- Separated from the Integrated Network by a firewall and capable of supporting intrusion detection;
- Protected against physical access by unauthorized individuals (i.e., tamperproof);
- Configured to avoid radio interference by automatically switching radio channels when interference is detected;
- Deployed to minimize radio signal coverage beyond the intended service area; e.g., positioning of antenna;
- Configured with a non-default WLAN name (i.e., SSID) that conforms with SSID naming conventions (see Appendix A) and does not contain any identifying information about the Government program using the WLAN;
- Hardened against discovery and attack using guidelines as supplied by the Corporate Security Branch and the I&IT Cluster; and
- Maintained in compliance with current Corporate and Cluster technical standards and procedures.

⁵ This document does not repeat other requirements for Government-issued computing devices that are stipulated in corporate and cluster standards, policies and procedures; e.g., inactivity lockout, acceptable use, software administration, patch management, disposal of equipment and media.

⁶ Updates that address known vulnerabilities in adapters must be applied promptly.

⁷ End-to-end encryption may be required for some sensitive Government Programs as recommended by the Program area's Threat/Risk Assessment (i.e., WLAN encryption may not be sufficient).

Management of Wireless Access Points

Administrative access to WLAN AP must be limited to authorized and trained technical staff whose identity is authenticated using a strong authentication mechanism.

Any remote administration must be carried out via a secure connection.

AP management protocols should be disabled when not being used.

Monitoring Wireless LANs

The Integrated Network must be monitored for unauthorized installations of WLANs and installations that do not comply with the requirements in this document. Such installations should be immediately disconnected from the Integrated Network.

A log must be clearly defined and implemented for the authentication mechanism used to authenticate the identity of WLAN users. The log must be secured, made tamper resistant, and retained in accordance with the standard established for the retention of firewall logs.

Responsibilities

WLAN Users

All WLAN users are responsible for:

- Complying with Government directives, policies and agreements when using Government equipment and services;
- Ensuring security safeguards installed to protect their wireless computing device are not disabled or tampered with; and
- Reporting any suspected security breaches as instructed by the I&IT Cluster.

Program Managers

Program Managers are responsible for:

- Completing an Information Security and Privacy Classification and Threat/Risk Assessment with the support of the Cluster Security Officer and ensuring that the risks involved are acceptable;
- Authorizing individual employees and consultants to have access to a WLAN Access Point in their program area;
- Ensuring that an individual's access to a WLAN Access Point is terminated promptly when no longer required; and
- Reporting any security exposures or suspected security incidents as instructed by the I&IT Cluster.

Cluster Chief Information Officers

Cluster CIOs are responsible for authorizing the implementation of all WLANs in ministries and organizations supported by the I&IT Clusters based on the business need and a risk assessment.

I&IT Clusters

The I&IT Clusters are responsible for:

- Ensuring that a Threat/Risk Assessment is completed before proceeding with a request for a WLAN implementation;
- Maintaining an up-to-date registry of WLAN implementations and a list of all WLAN users that include the information as required 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;
- Providing support and help desk services to WLAN users; and
- Supporting security incident reporting and management procedures.

Cluster Security Officers are responsible for:

- Supporting Program Managers in the completion of an Information Security and Privacy Classification and Threat/Risk Assessment for any proposed deployment of a WLAN; and
- Monitoring and ensuring that the Cluster's WLAN implementations comply with the requirements in this document and other Corporate and Cluster policies and standards.

iSERV Ontario

iSERV ONTARIO contracts an external organization to provide Integrated Network services for the Ontario Government.

iSERV ONTARIO is responsible for:

- Ensuring that the Agreement(s) with the Integrated Network Service Provider binds them to address the requirements in this document;
- Providing services to support the identity authentication and authorization mechanisms; and
- Ensuring that a security assessment on the WLAN service is completed when a change is made that could introduce new threats or vulnerabilities.

Integrated Network Service Provider

The Integrated Network Service Provider is responsible for:

- Implementing, managing and operating WLAN access points in accordance with the requirements in this document and other Government policies and standards;
- Maintaining the firewall rules on standalone firewalls separating Access Points from the Integrated Network;
- Ensuring that appropriate security safeguards are in place to protect the WLANs, including those stipulated in this document;
- Ensuring that the audit log for the authentication server is securely maintained, available when needed for investigations, and retained in accordance with the standard established for the retention of firewall logs; and
- Monitoring the Integrated Network for WLANs that are unauthorized or do not comply with these requirements, and immediately notifying Government contacts for appropriate action.

Corporate Security Branch

The Corporate Security Branch is responsible for:

- Recommending cryptographic algorithms that are deemed sufficiently secure for use within the Government;
- Accessing the WLAN logs as needed for investigations into attacks or inappropriate behaviour, and notifying the appropriate individuals of suspected security breaches; and
- Monitoring compliance with the requirements in this document in conjunction with iSERV ONTARIO, the Integrated Network service provider, and the I&IT Clusters.

Definitions

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

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

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

Certificate: The public key of an entity, together with some other information, rendered unforgeable by digitally signing it with the private key of the CA that issued it. The certificate format is in accordance with X.509 and RFC2459.

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

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

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

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

DMZ (demilitarized zone): A small network inserted as a "neutral zone" between an organization's internal network and the Internet. The DMZ contains computing devices that are Internet-facing and outside the Corporate firewall. Since these devices are vulnerable to attack, they should be protected from the Internet by a firewall.

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

Encryption: The transformation of data using cryptography into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy 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.

IEEE 802.1X: An IEEE security standard for authentication that features dynamic distribution of session keys and 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. 802.11 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 (e.g., 802.11b). The 802.11i standard features 802.1X authentication protections and the Advanced Encryption Standard (AES) for encryption protection.

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.

Malicious Code: Unauthorized software that is surreptitiously installed on a computer to enable a perpetrator to access or damage I&IT resources, or to use the computer to attack other computers on the network (e.g., viruses, worms, denial of service attacks).

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.

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

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

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

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.

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. The SSID should be shared only with those having legitimate need to access the network.

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

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

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) in that it allows the client computing device access to the network 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.

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 issues with WEP encryption and the 802.1X authentication standard.

Appendix A: IEEE 802.11 SSID Naming Standard

This document provides standards on SSID naming convention for IEEE 802.11 Wireless Access Points deployed with in Government of Ontario.

The SSID for an Access Point is based directly on its Managed Service Unit Identifier (MSU ID). The OPS Managed Service Unit Identifier Naming Convention should be referenced for details on the creation of an MSU ID, which consists of:

- The OPS Wall Plug ID (up to 10 characters)
- Location code (up to 9 characters) (aka EHD Remedy Division/Branch Code)
- 3 digit sequential number

Although an Access Point's SSID is based on its MSU ID, it cannot be identical. SSIDs must be alphanumeric (i.e., the colons that are part of MSU IDs must be dropped). In addition, to make the street address more obscure to potential attackers, the SSID has the street number immediately after the OPS Wall Plug ID.

Examples:

1. An Access Point at 155 University Avenue, Toronto with an MSU ID of ***D45:TOR155UNI:001*** would have an SSID of ***D45155TORUNI001***
2. An Access Point at 77 Wellesley, Toronto with an MSU ID of ***987654:TOR77WEL:060*** would have an SSID of ***98765477TORWEL060***

Appendix B: Additional Information

Type of Standard

Check One	Type of Standard
<input checked="" type="checkbox"/>	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.).
<input type="checkbox"/>	Information Standard – specifications for a data format (e.g., XML schema, metadata, and/or related data models)
<input type="checkbox"/>	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.)
<input type="checkbox"/>	Architecture Standard – application patterns, architecture and standards principles governing the design and technology decisions for the development of major enterprise applications
<input type="checkbox"/>	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
<input type="checkbox"/>	Internal Standard
<input checked="" type="checkbox"/>	External Standard

Consultation

Check	Area	Date: (month/year)
<input checked="" type="checkbox"/>	Technical Standards Unit, Corporate Architecture and Standards Branch, OCCTO	May 2005
<input checked="" type="checkbox"/>	Corporate Architecture and Standards Branch (CASB Architects), OCCTO	Sept 2004
<input type="checkbox"/>	Infrastructure Development Branch & iSERV, OCCSD	
<input checked="" type="checkbox"/>	Corporate Security Branch	Aug 2004
<input type="checkbox"/>	Strategy, Policy, Planning and Management Branch (SPPM, OCCS)	
<input type="checkbox"/>	Corporate ACT and Domain Working Groups	
<input type="checkbox"/>	– Information Architecture Domain (IADWG)	
<input type="checkbox"/>	– Technology Architecture Domain (TADWG)	
<input type="checkbox"/>	– Application Architecture Domain (AADWG)	
<input checked="" type="checkbox"/>	– Security Architecture Working Group (SAWG)	Oct 2004
<input type="checkbox"/>	Cluster ACT/ARB (for Cluster standards promoted to Corporate standards)	
<input checked="" type="checkbox"/>	IT Executive Leadership Council (ITELC)	March 2005
<input checked="" type="checkbox"/>	IT Standards Council (ITSC)	May 2005
<input checked="" type="checkbox"/>	ITSC Wireless Working Group	Nov 2004
<input checked="" type="checkbox"/>	Cluster Security Officers	Oct 2004
<input checked="" type="checkbox"/>	Network Office, iSERV	Sept 2004
<input checked="" type="checkbox"/>	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 25	GO-ITS 25.5.1 Best Practices: Wireless Local Area Networks: IEEE 802.11 supplement this document.	Refer to Best Practices for guidance
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 Environment

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

Application(s) or Infrastructure Impacted	Describe Impact	Recommended Action (or page number where details can be found)
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

Information and Information Technology Security Directive:

<http://intra.security.gov.on.ca/resources/default.asp>

Information Security and Privacy Classification Policy and Operating Procedures:

<http://intra.security.gov.on.ca/resources/>

Operating Procedure on Usage of I.T. Resources:

http://intra.pmed.mbs.gov.on.ca/mbc/pdf/I&IT-Operating_Procedure_Usage.pdf

GO-ITS 25.5.1 Best Practices: Wireless Local Area Networks: IEEE 802.11:

<http://intra.security.gov.on.ca/resources/>

Approved Internal Government of Ontario Information Technology Standards (GO-ITS)

http://intra.itsc.gov.on.ca/scripts/index_.asp?action=31&P_ID=1893&U_ID=0&N_ID=2

Approved Public Government of Ontario Information Technology Standards (GO-ITS)

<http://www.itstandards.gov.on.ca>

Errata

Approved by ITSC: May 18, 2005

Updated May 19, 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 section to have Doug Whyte as contact manager rather than Dale Tasker.
- 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.

Approved by Architecture Review Board: June 29, 2005

Copyright

© Queen's Printer for Ontario 2005.