



Government of Ontario IT Standard (GO-ITS)

Number 25.19

Access Control

Version #: 1.0

Status: Approved

Prepared for the Information Technology Standards Council (ITSC) under the delegated authority of the Management Board of Cabinet

UNCLASSIFIED

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 Information Technology Standards Council (ITSC) under 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. 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.gov.on.ca/mgs/en/IAndIT/STEL02_047295.html

Summary

The Information and Information Technology (I&IT) Security Directive 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.

The security of information systems relies in part on the application of access control. This standard describes mandatory minimum requirements regarding access control management for I&IT resources operated by, or on behalf of, the Government of Ontario.

Version Control

Date	Version	Author	Comment
Feb. 2 nd , 2009	--	Tim Dafoe, CSB	Draft document created
Dec. 10 th , 2009	1.0	Tim Dafoe, CSB	Document revised, ITSC feedback included, presented for approval by ITSC and ARB

Table of Contents

1. INTRODUCTION	5
1.1 Purpose of the standard	5
1.2 Versioning and change management.....	5
1.3 Contact information	5
1.4 Terms.....	6
1.5 Application and scope	6
1.6 Principles	7
2. REQUIREMENTS.....	8
2.1 Mandatory controls	8
2.1.1 Administration requirements.....	8
2.1.2 Technical requirements	9
2.1.3 Access to accounts and credentials	9
2.1.4 Logging	9
2.1.5 Time synchronization.....	10
2.1.6 Review	10
2.1.7 Sensitive information	10
3. RESPONSIBILITIES	11
4. ACKNOWLEDGEMENTS	13
5. DEFINITIONS	14
6. APPENDIX: ADDITIONAL INFORMATION	16

1. INTRODUCTION

1.1 Purpose of the standard

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

Access control is a technical means by which to define system users, manage I&IT assets, and grant access to I&IT resources. Appropriate design and management of access control systems is required to safeguard assets and ensure user accountability. This document sets out security requirements for the design and operation of access control systems.

1.2 Versioning and change management

Ongoing ownership and responsibility for maintenance and evolution of this document resides with the Corporate Security Branch (CSB), Ministry of Government Services. The Corporate Security Branch will provide advice on the interpretation and application of these security requirements and manage any updates to the document when the need arises.

1.3 Contact information

	Contact 1	Contact 2
<i>Name/Title</i>	Charlotte Ward, Manager, Policy and Administration	Tim Dafoe, Senior Security Policy Advisor
<i>Organization/Ministry</i>	Ministry of Government Services	Ministry of Government Services
<i>Division</i>	OCCIO	OCCIO
<i>Branch</i>	Corporate Security Branch	Corporate Security Branch
<i>Section/Unit</i>	Security Policy	Security Policy
<i>Office Phone</i>	(416) 327-9385	(416) 327-1260
<i>E-mail</i>	Charlotte.Ward@ontario.ca	Tim.Dafoe@ontario.ca

1.4 Terms

Within this document, certain words are used that require precise interpretation from readers. The following are the precise requirements associated with the following terms:

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

1.5 Application and scope

This standard applies to all ministries of the Government of Ontario, in addition to any provincial agencies that use or leverage ministry or I&IT Cluster I&IT infrastructure, and all third party individuals and organizations that connect to the Government of Ontario integrated network for businesses purposes, unless exempted in a Memorandum of Understanding.

As new GO-ITS standards are approved, they are deemed mandatory for all project development and procurement opportunities. When implementing or adopting any GO-ITS standard or GO-ITS standard update, ministries and clusters **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 information¹, 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 25.19 Access Control standard applies to:

- All ministries of the Ontario Government and any organization that uses a ministry's or I&IT Cluster's information technology infrastructure;
- Any organization that uses ministry or I&IT Cluster information technology infrastructure;
- Any third party organizations (and their staff) that connect to the Government of Ontario integrated network for business purposes, unless exempted in a Memorandum of Understanding; and
- Any access control system associated with the above, regardless of deployment within a production environment or staging/test/development environment.

¹ Sensitive information as defined per Information Security and Privacy Classification (ISPC) policy (<http://intra.pmed.mbs.gov.on.ca/mbc/pdf/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf>).

1.6 Principles

The following principles are stated in accordance with the Information and Information Technology Security Directive:²

- Access control is the primary means by which authorized users of I&IT assets are defined and provided with access to resources.
- I&IT planning and sound management must ensure the continuous availability of information; this includes the ability to access information or shared resources without resort to emergency measures during typical I&IT operations.
- The credentials, accounts, and electronic identities assigned to individuals are a means to provide integrity and accountability when I&IT assets are accessed.
- Appropriate sponsor-level management authority, for access control decisions and requests outside the scope of daily operations, is defined as a Director or above.
- Education of authorized users regarding appropriate use of assigned privileges and their credentials is vital to successful access control implementation and operation.
- Appropriate assignment and use of elevated system privileges (e.g., those reserved for use by system administrators) is crucial to enterprise security efforts.

² The Information and Information Technology Security Directive can be found at:
http://intra.pmed.mbs.gov.on.ca/mbc/pdf/Management_of_IT-Dir.pdf

2. REQUIREMENTS

The following security requirements apply to all access control systems deployed to safeguard Government of Ontario information, networks and computer systems:

2.1 Mandatory controls

2.1.1 Administration requirements

Access control systems:

- **Must** conform to and support documented business and security requirements (e.g., the rationale for deploying an access control system);
- **Must** meet the access control requirements stated in GO-ITS 25.0 General Security Requirements;
- **Must** be managed in a manner that requires that users are individually authorized by the relevant, responsible program manager (with documentation);
- **Must** be managed such that all authorized users of the system (and the roles, rules and/or privileges associated with their accounts or credentials) are documented;
- **Must** be managed such that authorized user accounts or credentials that are no longer in use, or no longer required (e.g., due to a change in employee role) are identified and removed with 24 hours of notification;
- **Must** be managed such that frequent and routine searches for redundant or duplicate entries in access control databases are conducted;
- **Must** be managed such that expired entries in access control databases are not assigned to new users (to prevent expired privileges being provided to users who do not require them);
- **Must**, in instances where passwords are assigned, support password management that is consistent with the direction described in GO-ITS 25.15 (Security Requirements for Password Management and Use);
- **Must** only provide system administrators with elevated privileges through the assignment of accounts or user profiles dedicated to system or device maintenance (as opposed to assigning these rights to existing accounts or profiles used for general purpose computing);
- **Must** assign elevated privileges on a “need for use” basis (or per event), such that these privileges are not provided for an unnecessary duration;
- **Must** assign elevated privileges in accordance with the *principle of least privilege* described in GO-ITS 25.0 General Security Requirements, and only where documented business requirements exist for the assignment of elevated privileges (e.g., authorized system administrators or content managers);
- Should be managed in a manner that requires authorized users to be provided with a written statement of the access rights and responsibilities for the system; and
- Should be managed in a manner that requires authorized users to sign a use agreement that indicates their acceptance of disclosed access rights and responsibilities.

2.1.2 Technical requirements

Access control systems **must** be centrally deployed and managed. The design and operation of centralized access control systems **must** include resilience and redundancy to reduce impact if failures occur.

Access control systems **must** grant access only after authorization and authentication procedures are complete, and a successful result has been returned for the credentials presented and/or the initiated session.

Cryptography deployed as a technical safeguard within an access control system (e.g., to pass credentials over a network connection or provide for integrity assurance) **must** meet the requirements described in GO-ITS 25.12 Use of Cryptography.

2.1.3 Access to accounts and credentials

Program managers **must** not be permitted to request the following:

- Access to a user's credential or identity as assigned by an access control system;
- Access to data, files, etc. stored by a user whereby access to such information is managed by an access control system; and
- Information encrypted by a user through the use of a key or cryptographic process controlled by an access control system, even if desired for recovery purposes.

Program managers **must** ensure that employees use central repositories, shared folders, or other mechanisms such that any critical work products remain accessible to relevant staff. In such instances, effective management of project information is the primary means by which access to such information should be safeguarded.

Program managers **must** act to protect the integrity of credentials granted to users. This **must** include the following:

- Ensuring appropriate handling of user credentials;
- Ensuring appropriate education for users regarding the use and security of their credentials, and any related access control system or identity service (e.g., GO-PKI); and
- Ensuring that inappropriate requests that could harm the integrity of user accounts, assigned credentials, or electronic identities are not accepted.

2.1.4 Logging

Logging **must** be consistent with GO-ITS 25.0 General Security Requirements. The following types of log information **must** be generated by access control systems:

- System logs (e.g., errors, system run level, security events, status);
- Activity monitoring (e.g., connection source/initiation, sessions, authentication failures, actions); and
- Audit logs (e.g., credential use, channel, invoked privileges, protected object access, violations).

2.1.5 Time synchronization

To maintain the integrity of log information, all access control systems **must** obtain system time from a redundant and validated time source as described in GO-ITS 25.0 General Security Requirements.

2.1.6 Review

The activity monitoring and audit log information produced by access control systems **must** be periodically reviewed to detect indications of misuse or attack. Possible indicators of such events are described in GO-ITS 25.0 General Security Requirements.

Accounts and privileges granted via access control systems **must** be periodically reviewed to ensure they are correctly allocated. Credentials or accounts associated with elevated system or application privileges (e.g., those used for system administration, user account administration, or content management) **must** be subject to more frequent review.

2.1.7 Sensitive information

The robustness and reliability of access control systems, and the credentials they rely on, should be increased in environments where sensitive information (as defined by ISPC policy) is processed or stored (or where a TRA has identified elevated risk). The increased requirements for confidentiality, integrity, and non-repudiation in these environments should be reflected in the type of access control deployed for use.

The degree of identity assurance associated with credentials, and the number of authentication factors required prior to access, are examples of increased robustness and reliability.

3. RESPONSIBILITIES

Users

All users of I&IT systems or applications subject to access control are responsible for:

- Complying with Government directives, policies and agreements when using Government equipment and services;
- Ensuring the security of their accounts and credentials; and
- Reporting any suspected security breaches to the OPS Service Desk.

Program Managers

Program Managers are responsible for:

- Complying with the requirements in this document;
- Authorizing and approving appropriate requests for employee and contractor access; and
- Submitting appropriate requests only regarding access to information controlled by an access control system.

Directors

Directors are responsible for:

- Complying with the requirements in this document; and
- Acting as an appropriate authority for specific types of requests (e.g., those associated with recovery of information controlled by an access control system).

Cluster Security Offices

The Cluster Security Offices and staff are responsible for:

- Promoting adherence with the requirements in this document within their area of responsibility.

Infrastructure Technology Services (ITS)

ITS is responsible for:

- Managing network service provider contracts for the provision of security services, when required, that may include an access control component;
- Implementing, managing and operating access control systems in accordance with the requirements in this document and other applicable Government policies and standards;
- Ensuring that appropriate security safeguards are in place to protect access control systems, including those stipulated in this document and GO-ITS 25.0 General Security Requirements; and

- Ensuring that the logging requirements describing in this document are met (both for services operated by ITS and by network service providers).

Network Service Provider

The Network Service Provider is responsible for:

- Implementing, managing and operating access control systems in accordance with the requirements in this document, GO-ITS 25.0 General Security Requirements, and other applicable Government policies and standards;
- Ensuring that appropriate security safeguards are in place to protect access control systems, including those stipulated in this document; and
- Ensuring that the logging requirements describing in this document are met, with all logs securely maintained, available when needed for investigations, and retained in accordance with this standard.

Corporate Security Branch

The Corporate Security Branch (CSB) is responsible for:

- Maintaining this standard and all other applicable IT security standards, policies, procedures and related guidance on behalf of the Government of Ontario;
- Ensuring that the logging requirements describing in this document are met for any service operated by CSB;
- Developing educational materials and tools to assist users in appropriate use and protection of credentials and assigned privileges; and
- Operating GO-PKI.

Ontario Internal Audit

The Ontario Internal Audit Division is responsible for:

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

4. ACKNOWLEDGEMENTS

4.1 Editors

Full Name	Cluster, Ministry and/or Area
Tim Dafoe	MGS Corporate Security Branch

4.2 Contributors

Full Name	Cluster, Ministry and/or Area
Colin Easton	OCCTO CAB
Kit-Mei Chan	MTO
Brady Thompson	OCIPO

4.3 Consultations

The following individuals were consulted:

Charlotte Ward, MGS Corporate Security Branch

Gerard Francis, Ontario Internal Audit

Bill Zeng, MGS Corporate Security Branch

Rajan Mistry, MGS Corporate Security Branch

4.4 Reviewers

The following groups have reviewed this standard:

Ontario Internal Audit

OCCIO ITS

Security Architecture Working Group

5. DEFINITIONS

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

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

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

Authorization: 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).

Credentials: Evidence provided to prove the claimed identification (e.g., presenting related contextual information or tokens in order to access electronic resources).

Cryptography: The transformation of data into a form unreadable by anyone (encryption) 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.

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

Elevated privileges: Enhanced rights and/or administrative control, assigned to a user, over a particular I&IT resource or class of resources.

Information: The meaning derived from or assigned to facts or data, within a specified context.

Information Technology Resources: Those resources (hardware, software, data etc.) associated with the creation, storage, processing and communication of information in the form of data, text, image and voice.

Integrity: The authenticity, accuracy and completeness of data that can be affected by unauthorized or accidental additions, changes and/or deletions.

Network: IT systems that can be made of one or both of the following components:

- Local Area Network (LAN) - Network of Information technology systems wholly situated at one geographical address;
- Wide Area Network (WAN) - located over more than one geographical site.

Non-repudiation: The quality embodied by services where transaction and identity assurance are managed to the degree that receipt of information or completion of transactions cannot reasonably be denied by participants.

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.

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.

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

6. APPENDIX: 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

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)
Access Control Systems	Adherence to these security requirements will reduce the risks to Government I&IT assets. Requirements are in line with current practice and impact should be minimal.	Compliance with these requirements

References

GO-ITS 25 Security Standards:

<http://intra.collaboration.gov.on.ca/mgs/occto/our-services/technology-adoption/technical-standards-1/approved-go-its-standards/>

ISO/IEC Standards:

<http://www.iso.org>

ISPC Policy:

<http://intra.pmed.mbs.gov.on.ca/mbc/pdf/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf>

Document History

Created: *February 2009*

- Created document
- For approval by ITSC / ARB

Edited: *June 2009*

- Adjusted existing content and formatting
- Included management access content

Edited: *October 2009*

- Numbering change from GO-ITS 25.17 to GO-ITS 25.19 as per ITSC
- Inclusion of input from Ontario Internal Audit
- Final changes prior to review by ITSC/ARB

Edited: *November 2009*

- ITSC feedback incorporated
- Changed “Cluster Security Officers” to “Cluster Security Offices and staff” as per new CSO direction
- Format and some errors corrected

Edited: *December 2009*

- Final CSB and ITSC feedback incorporated

Endorsed: *December 16, 2009*

- IT Standards Council endorsement

Approved: *January 21, 2010*

- Architecture Review Board approval

Copyright

© Queen's Printer for Ontario, 2010