



**CORPORATE SECURITY
INFORMATION TECHNOLOGY**

**Security Requirements for
Password Management and Use**

Government of Ontario IT Standards (GO-ITS)

Document No. 25.15

Version 1.0

Status: Approved

**CORPORATE SECURITY BRANCH
MINISTRY OF GOVERNMENT SERVICES**

Last Review Date: February 28, 2006

Table Of Contents

1. Introduction	2
Summary	2
Foreword.....	3
Purpose	3
Versioning and/or Change Management	3
Application and Scope	3
Contact Information.....	4
Background.....	5
Principles	6
2. Requirements	7
General	7
Creating Passwords.....	7
Maintaining Passwords	8
Sharing or Disclosing	8
Administering Passwords.....	9
Auditing Passwords	9
Vendor Supplied Access.....	10
Storage and Transmission	10
Multiple Platform Passwords.....	10
3. Roles and Responsibilities.....	10
Users	10
Program Managers	11
Corporate Security Branch.....	11
I&IT Cluster Security Officers.....	11
I&IT Cluster System Administration	12
Appendix A: Additional Information.....	14
Version Control	14
Type of Standard	15
Publication	15
Appendix B: Acknowledgements.....	16
Development Team.....	16
Reviewers	16
Errata.....	17
Copyright.....	18

1. Introduction

Summary

- The protection of information and information technology is the responsibility of all members of the Ontario Public Service.
- Information and information technology must be protected by passwords.
- Passwords are character strings used to verify the identity of a user.
- Passwords themselves are highly sensitivity information and must be protected accordingly.
- Passwords must be created, used, maintained, stored, protected and deleted in accordance with this standard.
- Users must be aware of the risks to information through improper password usage and maintenance.
- Managers must help and instruct staff to know and adhere to this standard.
- Password owners are accountable for any access to information technology gained through the use of their password.
- Users must not disclose their passwords to anyone else.
- Users must know whom to contact for assistance with their password.
- Users must immediately change any disclosed passwords.
- Users must know how and when to report a password breach.
- Users must know and adhere to all the requirements of this standard.
- Systems administrators must implement this standard.
- Management must make available the technical tools required for all staff to adhere to this standard.
- Reasonable, compensating controls must be used if compliance with this standard is not immediately possible.

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 responsibilities of the Ministry of Government Services to coordinate the standardization of information technology within 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.

Purpose

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

This document sets out security requirements for password management and use within the government of Ontario. The objective of this document is to ensure that the management and use of passwords to access government information and information technology does not result in unacceptable risks to those resources.

Versioning and/or Change Management

This document is owned by Corporate Security Branch, which is responsible for updating it and for providing advice on how to apply it.

Application and Scope

These requirements apply to:

- all ministries of the government of Ontario and any organization that uses a ministry's or I&IT cluster's information technology infrastructure; and
- all agencies that use a ministry's information and information technology infrastructure.

The scope of this standard extends to all information and information technology regardless of the computer system or platform.

While other methods of user verification exist, (e.g. biometrics and artefacts, such as Smartcards), they are not within the scope of this document. This standard regulates the use of passwords, which are defined as confidential authentication information in the form of a string of characters, used as proof of identity. However, all approved methods and tokens of access to government of Ontario information and information technology

are considered highly sensitive and must be protected in accordance with the Information Security and Privacy Classification Policy.¹

To ensure minimal impact to business functions, this standard should be applied as part of an I&IT Security Plan, as required by the I&IT Security Directive.² Assistance for creating a plan is provided in the I&IT Security Plan Guideline.³ Assistance with implementing a plan is available through the Cluster Security Officer assigned to each ministry cluster. Plans should take into account all applicable restrictions and establish reasonable timelines for compliance. Compensating controls must be used if compliance with this standard is not immediately possible.

Contact Information

	Contact 1	Contact 2
<i>Name</i>	Lynette Craig, Security Policy Advisor	David Chan, Business Manager, Security Policy and Administration
<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>	416-327-2399	416-327-2325
<i>E-mail</i>	Lynette.Craig@mgs.gov.on.ca	David.Chan@mgs.gov.on.ca

¹ <http://intra.security.gov.on.ca>

² <http://intra.security.gov.on.ca>

³ <http://intra.security.gov.on.ca>

Background

Access controls must prevent intruders from impersonating legitimate users. Therefore, it is necessary to verify that users are who they claim to be. Passwords are the most common way to provide identity verification for users of information technology at the government of Ontario.

Passwords are administered by many different people across different computer platforms and need to be structured to a standard. This standard seeks to provide adequate structure for the use and maintenance of passwords while ensuring that users are able to enter passwords with minimal inconvenience.

Passwords must themselves be treated as highly sensitive information. Sensitive information must be safeguarded in accordance with the Information Security & Privacy Classification Policy (ISPC).⁴ The ISPC Policy states that all high sensitivity information must be encrypted while in storage and transmission. Encrypting passwords is a very effective way to prevent their detection by unauthorized persons. High sensitivity information is described as information, which, if disclosed without authorization, could reasonably be expected to cause loss of life or public safety, extremely serious personal or enterprise injury, major political or economic impact, sabotage/terrorism, significant financial loss and social hardship. Also included, is all medical and financial information about identifiable individuals.

Protection of passwords also depends on the continuous efforts of users to maintain them in strict confidence. Therefore, each password owner is accountable for any access to systems gained through the use of a their password.

This standard requires that passwords be a minimum of 6 characters in length. A minimum password length is required to protect against systematic bombardment of a logon id, using an extensive list of common words, to gain unauthorized access. The longer and more complex the password composition, the longer the list of password guesses must be. For example, a six character, alphanumeric password would exhaust 1.8 billion illegal access attempts. A password of 8 characters would take over 2.6 trillion illegal access attempts and may require advanced computing capabilities. Therefore, users who are authorized to access highly sensitive information may wish to use a slightly longer password than the minimum required.

Those who have difficulty remembering passwords may want to use passphrases. For instance, a memorable street address, that is not the user's own residence or business address, will meet the requirements for password length and composition and may be easily remembered without being written down, (e.g. 24SussexDrive).

⁴ <http://intra.security.gov.on.ca>

Principles

This standard supports the I&IT Security Directive⁵, Operating Procedures on Usage of IT Resources, Information Security & Privacy Classification Policy and Operating Procedures, and the GO-ITS-25 Security Standards.

- Information and information systems and resources are valuable and integral assets for the delivery of all government of Ontario programs; therefore, they require protection through approved user verification.
- Passwords, certificates or tokens that allow access to government of Ontario information systems containing sensitive data are themselves sensitive information assets.
- All users are individually accountable for their access and use of I&IT resources; therefore, individual accountability requires individual identification.
- Access controls cannot be effective if it is possible for intruders to impersonate legitimate users.
- Access controls must be commensurate with the business needs and the strategy and goals of the government of Ontario.

⁵ <http://intra.security.gov.on.ca>

2. Requirements

General

- All authorized access to information and information technology must first be subject to an approved verification process. At a minimum, that process must be the entry of an approved, unique login identification and password combination.
- All users are responsible for any access gained by the use of their password.
- The strength and complexity of a password must be commensurate with the business requirement for confidentiality, integrity and availability of the information and information systems and resources involved.
- In all instances where the technology will allow it, passphrases should be used, (e.g.,24 SussexDrive) instead of a single password.
- Screensavers must require password re-entry.

Creating Passwords

- Initial passwords must be communicated to the user directly in person, by telephone or by encrypted email.
- Initial passwords must be set to expire within 5 days.
- The password owner, on first login, must change the initial password.
- A mechanism should be in place to force the user to change the initial password and thereafter on a regular and consistent schedule. If the use of software for this function is not possible, then the administrator must manually instruct the password change and verify that it has been successfully completed.
- Passwords must be chosen so that they are easy enough to remember but not easily guessed by someone else.
- A mechanism must be in place to ensure that passwords are not any single word that can be found in an English dictionary.
- Passwords must not include easily identifiable personal information about the owner, (for example, names of family members, pets, birthdays, anniversaries or hobbies.)
- Passwords must not be any words, phrases or acronyms that are part of the broadly recognized Ontario Public Service culture.
- Passwords must contain at least one digit and at least one letter.
- Passwords must contain at least 6 characters.
- Passwords must not be the same as all or part of a user's login id, actual last or given names, or a commonly know nickname.

- Passwords must not be the word “password” or the word “welcome” or be based on them.
- Passwords must not be blank. The use of NULL passwords is prohibited.
- A mechanism must be in place to ensure that passwords are not reused by the same user within a span of 12 consecutive months.

Maintaining Passwords

- Regular users must change their passwords at least once every 90 days.
- System administrators must change their passwords at least once every 30 days.
- Password changes must not involve the use of easily recognized patterns (e.g. changing “compop10” to “compop11” and so on).
- Software that prohibits the use of recognizable patterns should be used wherever possible.
- Applications that require two factor identity authentication will be exempt from the maximum refresh cycles (i.e. the maximum length of time before the password must be changed), for user and administrator passwords. These applications must establish unique password refresh cycles based on system requirements.
- Documented procedures must be in place in the event of password loss, change or emergency modification.

Sharing or Disclosing

- Passwords must not be shared with anyone else.
- Authentication must be individual users not groups of users.
- Passwords must be changed immediately if they have been compromised or it is even suspected that they have been compromised.
- Access to backup media that contains passwords must be limited to authorized personnel.
- Passwords must not be displayed while being entered but may be represented on the screen by a special character such as an asterisk.
- Password memorizing software must not be installed. Where password memorizing software, such as Autocomplete, is part of any authorized, proprietary software, it must be disabled.

Administering Passwords

- To ensure that no one person can commit fraud and erase all trace of their actions, systems administrators with global rights must be a separate function from the function that creates and maintains user passwords.
- Administration and use of passwords must be consistent, uniform and documented in the I&IT Security Plan⁶ for the system on which they are used.
- A mechanism must be in place that provides the briefest possible explanation for the denial of access in the event that a password does not conform to rules for creation and/or change. The message should provide contact information for user assistance. (e.g. “password incorrect – call systems administrator”).
- Default vendor passwords that accompany software must be changed immediately following installation of the software.
- Access must be denied after the fifth, consecutive, incorrect password entry attempt. Users must contact their help desk or system administrator before the system will allow any further password entry attempts.
- Logon ids associated with passwords that have expired for 45 days must be deleted unless an important business reason exists to maintain it.
- Access denials due to the maximum incorrect password attempts must be recorded in an audit or system log. The log must be reviewed, and if necessary, investigated in accordance with approved monitoring and escalation procedures.
- A pre-arranged method of absolute identification, such as a code word, must be supplied by all users to the help desk personnel so that a password change can be performed for any user who is not visually identifiable, (e.g. a telephone request for password change).
- Guest passwords must be disabled.
- Controls must be in place to ensure that emergency passwords are changed after each use.
- Details of why, how and when the emergency password was used must be submitted to the appropriate management level.

Auditing Passwords

- User passwords must be tested for strength on a periodic and random basis.
- Passwords identified as weak or passwords that do not comply with this standard must be corrected immediately.
- Software that captures passwords must not be allowed on any system.
- Auditing methods must be deployed when a new system is implemented to identify poor passwords.

⁶ <http://intra.security.gov.on.ca>

Vendor Supplied Access

- Any non-system accounts that by default do not have a password must be secured with an appropriate password immediately.

Storage and Transmission

- Passwords must be encrypted in storage and in transmission.
- Passwords stored in files must not indicate the system that they are used for unless that information is encrypted also.
- Passwords must not be hard-coded into operating programs, applications or stored in batch files.
- Passwords must not be embedded in any automated logon process, stored in a macro or function key.
- Passwords must not be retrievable from an authentication process.
- Cryptographic keys must be stored in a secure manner using the approved encryption methods available within the Ontario Public Service.
- Unencrypted passwords or credentials information must not be cached.
- Passwords must not be stored on the hard drive but must be entered each time the application is accessed.

Multiple Platform Passwords

- Users who have access to multiple systems where their logon ids are identical, must use different passwords for each logon id on each system.
- Remote access passwords must be different from the regular system access password.

3. Roles and Responsibilities

Users

All Users are responsible for:

- Adopting security measures as outlined in this standard to protect their logon ids and passwords from unauthorized access;
- Ensuring they have taken the approved education provided for the proper use and maintenance of passwords.

- Knowing whom to call to report and/or change forgotten or compromised passwords.
- Understanding and performing their responsibilities to the government information and information technology to which they are granted access.
- Protecting their passwords and reporting any compromise of the password to their manager and the Help Desk.

Program Managers

Program Managers are responsible for:

- Authorizing and approving employee and contractor access privileges.
- Ensuring employees and contractors are individually accountable for using information systems and for following government directives, policies, standards, procedures, guidelines and best practices.
- Reporting any security breaches or suspected security incidents as instructed by the I&IT Cluster Security Officer.
- Ensuring employees and contractors are educated in the proper use and maintenance of passwords including how to report and/or change forgotten or compromised passwords.
- Ensuring users are able to enter their secret passwords with minimal inconvenience.
- Ensuring the use of passwords is immediately revoked when access is no longer required or no longer granted.

Corporate Security Branch

The Corporate Security Branch is responsible for:

- Monitoring as required, to ensure compliance with this standard.
- Updating this standard, as and when required.
- Approving encryption software to be used as a standard throughout the Ontario Public Service.
- Assisting with interpretation of this standard and any other associated policies and procedures.

I&IT Cluster Security Officers

The Cluster Security Officers are responsible for:

- Working with client Program Managers to investigate excessive password misuse or non-normal activity.
- Assessing password policy needs.

- Liaising between the cluster and Corporate Security Branch for password security issues, policies, education, and measures to implement this policy.
- Assisting in the identification, design and implementation of measures to implement this policy.
- Monitoring and auditing the implementation and adherence to these standards on a regular basis.
- Assisting Program Managers to include password requirements in the creation of their I&IT Security Plans.

I&IT Cluster System Administration

The I&IT Cluster System Administrator is responsible for:

- Establishing default passwords in accordance with these standards for new users and for resetting passwords for users whose passwords have been forgotten or compromised.
- Implementing system technical controls to comply with the password security requirements.
- Providing Help Desk service for password reset.
- Supporting security incident procedures.
- Documenting password loss, change and emergency use procedures.
- Providing user security awareness training.
- Ensuring on a regular basis, that network security measures are in place and monitored for unauthorized access attempts.
- Practicing a higher standard of care in maintaining confidentiality and password security due to their higher level of user privileges.
- Reporting password breaches to the appropriate I&IT Cluster Security Officers.

Terms and Definitions

Accountability

The obligation to answer for the 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.

Password Owner

The individual authorized to use a password and responsible for its use to gain access to information technology.

Responsibility:

The obligation to perform a given task or tasks associated with a specific role.

Sensitive:

Information that if released without authorization, may cause harm or injury, embarrassment, or unfair economic advantage as defined by the Information Security and Privacy Classification Policy and Operating Procedures.

Appendix A: Additional Information

Version Control

Date	Version	Author	Comment
Jan. 25 2005	1.0	Krista Schroeder	Initial draft
May 18, 2005	1.1	Lynette Craig	Updated based on Policy Section Review and author change
May 25, 2005	1.2	Lynette Craig	Updated based on CSB Management Review
June 10, 2005	1.3	Lynette Craig	Updated based on Corporate Security Branch – Security Design Section Review
June 29, 2005	1.4	Lynette Craig	Updated based on Cluster Security Officer Review
August 16, 2005	1.5	Lynette Craig	Updated based on Corporate Security Branch Management Review
Dec. 2, 2005	1.6	Lynette Craig	Updated based on email review by Standards Council
Jan. 3.2006	1.7	Lynette Craig	Updated based on requirements of Corporate Security Management to shorten and add summary page.
Feb. 2, 2006	1.8	Lynette Craig	Updated based on presentation review by Standards Council
Feb. 6, 2006	1.9	Lynette Craig	Updated based on requirements of CSB Management review of content.

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

This standard should be restricted to publishing on the Internal (Intranet) IT Standards web site.

Check One	Publish as Internal or External
<input checked="" type="checkbox"/>	Internal Standard
<input type="checkbox"/>	External Standard

Appendix B: Acknowledgements

Development Team

Name	Cluster/Ministry	Branch
Lynette Craig	MGS	Corporate Security Branch

Reviewers

Check	Area	Date: (month/year)
<input type="checkbox"/>	Technical Standards Unit, Corporate Architecture and Standards Branch	
<input type="checkbox"/>	Corporate Architecture Branch (CAB Architects),	
<input type="checkbox"/>	Infrastructure Development Branch & iSERV, OCCSD	
<input checked="" type="checkbox"/>	Corporate Security Branch	July 26/05
<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 type="checkbox"/>	- Security Architecture Working Group (SAWG)	
<input type="checkbox"/>	Cluster ACT/ARB (for Cluster standards promoted to Corporate standards)	
<input type="checkbox"/>	IT Executive Leadership Council (ITELC)	
<input type="checkbox"/>	ITSC members	Jan.18/06
<input type="checkbox"/>	ITSC Wireless Working Group	
<input checked="" type="checkbox"/>	Cluster Security Officers	June 29/05
<input type="checkbox"/>	Network Office, iSERV	
<input type="checkbox"/>	Network Management Committee	

Errata

Presented to ITSC: January 18, 2006

Updated February 2, 2006

1. Added "Background" section to provide clarity of the concept of password strength and complexity being **commensurate** with business requirements as used in the following standard:
 - "The strength and complexity of a password must be commensurate with the business requirement for confidentiality, integrity and availability of the information and information systems and resources involved."

Background section explains the difference in protections between 6 and 8 character passwords. Reference is made to the Information Security and Privacy Classification (ISPC) Policy requirements for the protection of high sensitivity information. A recommendation is made to use a slightly longer password if more protection is required.
2. Provided footnotes with the URLs for the I&IT Security Directive and the I&IT Security Plan Guideline.
3. Background section includes recommendation to use passphrases instead of passwords to help users remember them, (e.g., memorable street addresses.)
4. Added under "Application and Scope" section,
 - a recommendation for implementation as part of an I&IT Security Plan as required by the I&IT Security Directive
 - direction for systems that may not be able to implement immediately
5. Changed standard statement from:
 - "Passwords must not echo back to the screen when being entered."To:
 - "Passwords must not be displayed while being entered but may be represented on the screen by a special character such as an asterisk."

Updated February 6, 2003

6. Removed redundant statement in Purpose section
7. Changed standard statement under "Creating Passwords" section to remove "of their own creation".
8. Changed standard statement under "Creating Passwords" section to remove "alphanumeric" and insert "contain at least one digit and at least one letter."

9. Removed standard under “Maintaining Passwords”, as it may defeat the purpose of an emergency password, as follows:
 - “Emergency passwords, such as those required for emergency system changes or administration, must be held securely and in blind custody by two trusted staff members”
10. Removed standard under “Sharing or Disclosing” as it may exclude safe, encrypted storage, as follows:
 - “Except in the case of passwords created for emergency administrative use, password owners must never record their passwords.”
11. Removed standards under “Sharing or Disclosing”, as other standards preclude these, as follows:
 - “Verbal discussion of security systems including passwords must not be conducted in public, in non-work areas or in the hearing of personnel who lack appropriate administrative authorization of whose authorization is unknown.”
 - “Security systems and passwords must not be discussed with, or in the hearing of staff or contractors who have or signed a non-disclosure agreement.”
12. Removed standard under “Administering Passwords”, in view of another standard that requires each use of the emergency password be reported, as follows:
 - “The emergency password must be changed immediately after each use....”
13. Removed Human Resources section under “Roles and Responsibilities” as the responsibilities are assigned more appropriately elsewhere.
14. Grammar changes as required.

February 15, 2006

Approved by the IT Standards Council on February 15, 2006

February 28, 2006

Approved by the Architecture Review Board on February 28, 2006

Copyright

© Queen's Printer for Ontario 2006.