Ontario

Government of Ontario

Government of Ontario IT Standard (GO-ITS)

Number 25.11

Security Design Requirements

Version #: 1.2

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

UNCLASSIFIED

Last Review Date: 2015-03-18

Foreword

Government of Ontario Information Technology Standards (GO-ITS) are the official publications on the guidelines, preferred practices, standards and technical reports adopted by the Ontario Public Service under the delegated authority of the Management Board of Cabinet (MBC). These publications support the responsibilities of the Treasury Board Secretariat (TBS) for coordinating standardization of Information & Information Technology (I&IT) in the Government of Ontario. Publications that set new or revised standards provide enterprise architecture guidance, policy guidance and administrative information for their implementation. In particular, GO-ITS describe where the application of a standard is mandatory and specify any qualifications governing the implementation of standards.

All GO-ITS 25 Standards are based on the work of recognized global authorities in information and operational security, both in government and industry.

Copies of cited standards may be obtained as follows:

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

Internet: http://www.ontario.ca/government/information-technology-standards

Summary

The Corporate Policy on Information and Information Technology Security requires that Government of Ontario employees protect information that is received, created, held by, or retained on behalf of, Ontario ministries and agencies. Programs are responsible for the implementation of appropriate safeguards, based on an assessment of the risks involved.

The design of systems and services influences their inherent level of security and assurance. A comprehensive, early, proactive approach to such design is the most effective way to reduce risk, control safeguard costs, and improve the security posture of such systems and services.

This practice is referred to as Security Design.

This document describes security concepts, requirements, and system engineering principles that are useful for designers, implementers, and evaluators. In addition, it documents a comprehensive strategy for the organization of networks and system components.

Version control and change management

Date	Version	Author	Comment
Oct. 13th 2010	1.0	Tim Dafoe, CSB	Approved by ITSC and ARB
Mar. 14th 2012		Tim Dafoe, CSB	Minor update as per document history
Jun, 12th, 2012		Tim Dafoe, CSB	Updated consultation list
Nov, 15th, 2012	1.1	Tim Dafoe, CSB	Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 1.1
Jan. 19th, 2015	1.2	Tim Dafoe, SCS	Updates per ARB rationale (administrative changes, ISO/IEC alignment), document number changed to version 1.2

Ongoing ownership and responsibility for maintenance and evolution of this document resides with the Strategy, Planning, and Enterprise Architecture Branch (SPEAB) of the I&IT Strategy and Cyber Security Division (SCS), or a successor division/branch. SPEAB/SCS will provide advice on the interpretation and application of these security requirements and manage any updates to the document when the need arises.

Contact information

If you have questions or require further information about this document or the GO-ITS 25 series, please contact the following I&IT Security and Cyber Security Division staff:

	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

Table of Contents

1. INTRODUCTION

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

1.1. Purpose of the standard

This document outlines an approach for network organization and describes mandatory requirements for Security Design. The objective of this document is to ensure that Government of Ontario I&IT resources can be adequately protected from threats to security by way of a proactive and comprehensive effort to incorporate safeguards into the design of each project or service.

This document has been produced in consultation with stakeholder groups (primarily from security and architecture centres of excellence) within the Government of Ontario. It makes reference to the ISO/IEC 27002:2013 code of practice and Government of Canada ITSG-22 guidance.

1.2. Document organization

This document is organized as follows:

Section 2.1: Zone concept

Section 2.2: Zone descriptions

Section 2.3: Security Design concepts

Section 2.4: Operational Security Design requirements

Section 2.5: System Security Design requirements

Section 2.6: Network Security Design requirements

1.3. 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.

1.4. Application and scope

GO-ITS 25 security requirements apply to all vendors, ministries, former Schedule I and IV agencies, and third parties (including any information technology system or network that processes ministry and agency information) under contract to the Government of Ontario, unless exempted in a Memorandum of Understanding. For the purposes of this document all references to "information" refer to digital information and data.

For security involving sensitive information[1], if it becomes known that sensitive information is deemed to be at serious risk, immediate remedial action **must** be taken to mitigate the risk by applying appropriate tools, controls, methods, and procedures as per the relevant GO-ITS security document.

As new GO-ITS standards are approved, they are deemed mandatory for all project development and procurement opportunities.

GO-ITS 25.11 Security Design Requirements **must** be understood to apply to:

- All entities identified above and/or which use the Government of Ontario Integrated Network; and
- All networks and/or information systems that store or process data for which the Government of Ontario is accountable.

The Strategy, Planning, and Enterprise Architecture Branch (SPEAB) of the I&IT Strategy and Cyber Security Division (SCS), or a successor division/branch, maintains this document and should be contacted if application of this standard is not clear relative to a given environment, program, or application.

1.5. Background

The Management and Use of Information & Information Technology (I&IT) Directive[2] states that projects must "implement security controls" to safeguard sensitive information. The Corporate Policy on Information and Information Technology (I&IT) Security requires that "programs must identify security requirements that must be included in the program design".

Security Design supports and provides tools to accomplish these objectives.

---

[1] As determined via the OPS Information Security and Privacy Classification (ISPC) policy (http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.18.14.34.52.PSU_res/$File/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf) and/or a TRA.

[2] The Management and Use of Information & Information Technology (I&IT) Directive can be found here: http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.04.11.09.46.33.J6N_res/$File/ManagementOfITDir.pdf

1.6. Principles and caveats

The following statements support, and are stated in accordance with, Management and Use of Information & Information Technology (I&IT) Directive, the Corporate Policy on Information and Information Technology (I&IT), and ISPC policy:

- The goal of Security Design is to reduce the risk posed to Government of Ontario I&IT assets, and safeguard the channels required for successful electronic service delivery.
- Security Design can assist in the assurance of data confidentiality, ensuring that information is only available to those who have been authorized to access it.
- Security Design can assist in the assurance of data integrity, ensuring that data remains in its original form when such safeguards are required, such that it cannot be modified either maliciously or in error.
- Security Design can assist in the assurance of system availability, ensuring that authorized users have access to assets and information whenever required, and that systems are resilient.
- The successful application of Security Design concepts requires that program areas successfully conduct data classification in accordance with the ISPC policy.
- Security Design is a proactive means by which to increase the level of security assurance offered by a given project; such efforts should be incorporated into the earliest project planning stages.
- Security Design can reduce the cost associated with technical security safeguards by building security functionality and a defensive posture into new projects at the earliest opportunity.
- Security Design can assist in reuse of common security process, applications, and services to support common business needs.
- Appropriate, effective use of the Security Design concepts and requirements described in this document requires a clear understanding of the assets that must be protected, and assessment of security requirements must occur early in the project cycle.
- The application of Security Design concepts and requirements do not preclude the use of assessment and evaluation techniques such as a Threat Risk Assessment (TRA), Privacy Impact Assessment (PIA), Business Impact Assessment (BIA), and Security Testing and Evaluation (STE).
- Secure development of applications is a complex and critical effort that requires guidance outside the scope of this standard; this document primarily concerns network design, management, and system specifications.
- Performance and service level obligations should be considered when adopting secure design techniques, to ensure adequate system capabilities and identify optimal safeguards for a particular environment.

2. REQUIREMENTS

The Security Design requirements in this section apply to all systems, projects, and services within the scope of this document.

2.1. Zone concept

Services consist of components that perform specific functions, often with a requirement to interoperate and communicate in network environments.

A Zone is a designated network environment with clearly defined boundaries and identified interface points. Each Zone provides access to services within that boundary, while also representing a uniform level of security. Zones can be layered to provide for increasing levels of security (e.g., defence in depth). Deployed safeguards, such as policy enforcement devices and monitoring, provide a first line of defence against threats that may originate from both outside and within a given Zone.

The use of Zones is an accepted method to enforce boundaries between systems and organizational units. They can also help in situations where differentials in information classification or risk have been identified.

Example:

> When a typical web application is deployed, a presentation system will accept queries from unmanaged networks, passing them in parsed form to an application or business logic server. In cases, a database host may also be queried. Several types of access and data are thus required for each transaction. These individual components can be placed within different Zones. With proper safeguards, this mode of deployment can reduce the likelihood that a malicious query or external threat agent reaches an application server or database without detection.

Appropriate use of Zones is intended to:

- Support interoperability, by standardizing security concepts and safeguards;
- Set minimum management and security requirements for network environments;
- Provide for a consistent level of protection for similar components or resources;
- Reduce contact between sensitive network environments and threat agents;
- Define and document the interface points between networks; and
- Ensure more costly safeguards are deployed only where necessary.

Zones defined for use within the Government of Ontario include:

- ***Unmanaged Zone***
- ***Access Zone***
- ***Operations Zone***

- ***Presentation Zone***
- ***Logic Zone***
- ***Data Zone***
- ***Storage Zone***
- ***Management Zone***
- ***Security Zone***
- ***Extranet Zone***

A Zone of one type can always be connected to a Zone of the same type, but there are some restrictions regarding the direct connections that may exist between different Zones; these restrictions are described in section 2.2.10 of this document.

2.1.1. Zone interface requirements

The following requirements are necessary for secure separation of Zones:

- All interface points for a given Zone **must** be clearly defined and documented;
- The number of interface points **must** be kept to a minimum; and
- Traffic from one Zone **must** not be extended to a Zone with a markedly different security posture/level without compensating controls or additional safeguards.

2.1.2. Zone interface technology requirements

Zone interface points **must** meet technology and configuration requirements:

- All communication **must** be examined and controlled by either:
  - Technology that meets the requirements described in GO-ITS 25.6 Security Requirements for Firewalls, or:
  - Other technology endorsed by the I&IT Strategy and Cyber Security Division (e.g., via TRA and ST&E processes) for this purpose[3];
- Traffic flow provisions for one Zone **must** not expose other Zones to undue risk;
- Electronic data transit between protected Zones **must** be impossible unless the interface point is crossed;
- Rules **must** be configured (in accordance with the principles described in GO-ITS 25.0 General Security Requirements and the configuration details in GO-ITS 25.6 Security Requirements for Firewalls) to provide access control, control traffic flow, and enforce security policies;
- In particular, the interface point **must** restrict traffic flow to protect the Zone from known variations of attack traffic, and in accordance with control requirements for that Zone;

[3] Technology may be endorsed for specific environments, and additional safeguards may be required.

- A single hardware device, or a single logical instance of other technology, should not be used as an interface point for multiple Zones, particularly where differentials in security levels exist, as a compromise of the device or related network equipment could result in access to many Zones;
- A single device or logical instance **must** not be used as described above in the case of a Security Zone; and
- Environments that rely on multiple devices in series for control over interface points (e.g., for successive Zones) should vary the type of deployed platform or technology where possible.

2.1.3. Network devices in Zones

Other network devices contribute to the overall security posture of Zones. Network routers and switches can enhance the security and management capabilities within a Zone. However, due to differences in change control, product security evaluation (e.g., Common Criteria), and potential variance in configuration standards, they **must** not be considered direct replacements for technology endorsed in section 2.1.2 (e.g., for the purposes of boundary control and policy enforcement).

Network devices within Zones, and particularly those associated with the interface point for a given Zone, **must** comply with GO-ITS 25.1 Security Requirements for Routers and Switches.

2.2. Zone descriptions

The Zones defined for use in the Government of Ontario are as follows:

2.2.1. Unmanaged Zone

2.2.1.1. Definition

An *unmanaged* network refers to a network where users, devices, applications and risk cannot be determined with any accuracy whatsoever. The Internet is an example of an unmanaged network; the number of both hosts and users are vast, potential sources of traffic are geographically diverse, and hostile traffic is common. An Unmanaged Zone describes any such network environment.

Smaller, closed networks where no overarching administrative control is exercised can also be considered “unmanaged”.

2.2.1.2. Control requirements

Unmanaged networks, by definition, are not centrally controlled. They represent a known source of hostile traffic that **must** be managed within other Zones. It is not possible to control the traffic within an Unmanaged Zone.

2.2.1.3. System security requirements

Government of Ontario systems and services **must** never be located in an Unmanaged Zone.

An exception to this requirement is the use of mobile devices supplied by the Government of Ontario, and intended for use by an end-user, on public data networks (e.g., Internet, PSTN, wireless data). Such use **must** however be conducted in accordance with the requirements described in GO-ITS 25.0 General Security Requirements, GO-ITS 25.5 Security Requirements for Wireless LANs, GO-ITS 25.7 Security Requirements for Remote Access Services, GO-ITS 25.10 Security Requirements for Mobile Devices, and ISPC policy.

2.2.2. Access Zone

2.2.2.1. Definition

An Access Zone describes the managed network access layer that exists when a network edge or border terminates at an Unmanaged Zone, and an interface point has been defined. The Zone created by this interface point denotes the edge of the Access Zone.

Systems located in an Internet *de-militarized zone* (DMZ) made accessible from an Unmanaged Zone (e.g., public services) should be understood to be located in an Access Zone.

2.2.2.2. Control requirements

An Access Zone is the first opportunity to manage external client traffic and reduce exposure for subsequent Zones.

The following controls **must** be implemented within an Access Zone:

- Internal hosting services (e.g., Intranet) **must** not be operated in this Zone;
- High Sensitivity information **must** not be stored (e.g., bulk long-term storage) in this Zone;
- High Sensitivity information may be presented to clients from DMZ hosts in this Zone, but **must** be communicated via cryptographic means compliant with GO-ITS 25.12 Use of Cryptography, protected by strong authentication (e.g., two-factor), and securely purged from DMZ systems once successfully presented;
- Traffic received from an Unmanaged Zone **must** be controlled in a way that limits potential inbound connections, and only those network protocols supported by subsequent Zones are supported and permitted;
- The Access Zone **must** enforce network paths that are consistent with the security goals for subsequent Zones, and resist attempts to manipulate the enforced path (e.g., abuse of dynamic switching or routing protocols);
- Interactive sessions (e.g., connections to a system where session state is maintained and an individual can directly issue system commands or access information) **must** be authenticated via strong authentication (e.g., two-factor), and protected via cryptography of a type and strength indicated within GO-ITS 25.12 Use of Cryptography for this purpose;

- The Access Zone must be flexible, such that a response to changing conditions in bordering Unmanaged Zones can be undertaken if required;
- All traffic received from an Unmanaged Zone not intended for receipt by a Access Zone server with a public interface should be dropped; and
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.2.3. System security requirements

Network devices present in the Access Zone:

- **Must** be hardened to a robust specification (in accordance with GO-ITS 25.1 Security Requirements for Routers and Switches, and industry best practice) to withstand sustained attack originating from an Unmanaged Zone;
- **Must** be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- **Must** be subject to ongoing monitoring and evaluation;
- **Must** conceal the network topology and configuration detail from threat agents located in an Unmanaged Zone;
- **Must** operate as few network services as possible, to minimize system complexity and attack surface; and
- **Must** not unnecessarily support protocols that could reduce the Zone security posture (e.g., network protocols that are not required to operate the system, but may provide access or a vulnerability to an attacker).

Systems present in the Access Zone:

- **Must** be hardened to a robust specification (in accordance with GO-ITS 25.8 Security Requirements for Servers, program area build requirements, and industry best practices) to withstand sustained attack originating from an Unmanaged Zone;
- **Must** be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- **Must** be subject to ongoing monitoring and evaluation;
- **Must** be protected from malware;
- **Must** have a system configuration (e.g., according to a build book) that includes reducing (where feasible) the amount of executable and or interpretable code present, to reduce the available attack surface;
- **Must** process the data required to handle transactions only, and for a minimal period of time (e.g., avoid storage);

- **Must** never simply forward intact, unprocessed client queries or traffic (e.g., raw client input from an Unmanaged Zone) to any other Zone, unless that Zone is also an Access Zone; and
- Should, where possible and where benefit exists, forward parsed queries to hosts located in subsequent Zones via network port numbers that differ from those on which the request was initially received.

2.2.3. Presentation Zone

2.2.3.1. Definition

A Presentation Zone is the environment presented to clients, users, and requesting entities within the organization (including partner groups connected via an external network). The Presentation Zone contains systems (e.g., Intranet hosts) that present data to and receive data from client systems.

The systems and services in the Presentation Zone are regularly exposed to client input and are susceptible to attack. These systems may process transactions, but do not typically process or store data.

2.2.3.2. Control requirements

The following controls **must** be implemented within the Presentation Zone:

- High Sensitivity information **must** not be stored (e.g., bulk long-term storage) in this Zone;
- High Sensitivity information may be presented to clients from this Zone, but **must** be communicated via cryptographic means compliant with GO-ITS 25.12 Use of Cryptography, protected via a robust means of authentication (e.g., two-factor), and securely purged from Presentation Zone systems once successfully presented;
- Traffic received from client systems **must** be controlled in a way that limits potential inbound connections, such that only those network protocols required to orchestrate sessions and/or complete transactions with the connecting client are permitted;
- All traffic entering the Zone not intended for receipt by a Presentation Zone server should be dropped;
- Interactive sessions (e.g., connections to a system where session state is maintained and an individual can directly issue system commands or access information) **must** be authenticated via strong authentication (e.g., two-factor), and protected via cryptography of a type and strength indicated within GO-ITS 25.12 Use of Cryptography for this purpose; and
- Activity monitoring and logging **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.3.3. System security requirements

All systems located within the Presentation Zone:

- **Must** be hardened to a robust specification (in accordance with GO-ITS 25.8 Security Requirements for Servers, program area build requirements, and industry best practices) to withstand potential attack from client systems;
- **Must** be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- **Must** be subject to ongoing monitoring and evaluation;
- **Must** be protected from malware;
- **Must** have a system build (e.g., according to a build book) that includes reducing (where feasible) the amount of executable and or interpretable code present, to reduce the available attack surface;
- **Must** process the data required to handle transactions only, and for a minimal period of time (e.g., avoid storage);
- **Must** never simply forward intact, unprocessed client queries or traffic (e.g., raw client input) to any other Zone, unless that Zone is a Presentation Zone or a DMZ located in an Access Zone; and
- Should, where possible and where benefit exists, forward parsed queries to hosts located in subsequent Zones via network port numbers that differ from those on which the request was initially received.

2.2.4. Logic Zone

2.2.4.1. Definition

A Logic Zone contains systems that execute business rules according to functional requirements, and receive requests or transactions from other systems. These systems may also issue queries of their own (e.g., to obtain information from a database).

Services within a Logic Zone **must** be hardened and protected. Compromised Presentation Zone systems may pose a threat to other systems if they are used as an intermediate attack platform.

Session management for applications and services should be orchestrated within this Zone.

2.2.4.2. Control requirements

The following controls **must** be implemented within the Logic Zone:

- Traffic received from a Presentation Zone **must** be reliably controlled such that only those protocols required for presenting data to clients are available;
- Queries issued from an Access Zone or Presentation Zone **must** never reach systems located within the Logic Zone without being mediated and parsed first (e.g., to validate input, detect attack, and/or perform bounds checking);

- Requests sent to the Logic Zone **must** be validated and pre-processed in a manner that reduces the likelihood of a malicious command or string being issued to a system within the Zone;
- Malicious queries or data should be identified, and when identified, dropped, with a resulting alarm (with review); and
- Activity monitoring and logging **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.4.3. System security requirements

All systems located within the Logic Zone:

- **Must** be hardened, in a manner appropriate for the deployed platform, against attack and misuse;
- **Must** be protected from malware;
- **Must** be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- **Must** be subject to ongoing monitoring and evaluation;
- **Must** issue requests to other Zones (i.e., a Data Zone) via a unique interface point;
- **Must** never directly issue database commands (i.e., SQL commands) from an interactive user to the Data Zone;
- **Must** process and interpret queries in a manner which includes access control and format validation, to ensure only authorized queries and information will be parsed; and
- **Must** maintain local business logic and application code in binary form only (unless reliance on scripting or similar technology makes this requirement unfeasible); and
- Should, where possible and where benefit exists, issue outbound queries to other Zones (i.e., a Data Zone) via network port numbers that differ from those on which the request was initially received.

2.2.5. Data Zone

2.2.5.1. Definition

The Data Zone is intended to safeguard organized information made available via systems such as database servers. This includes long-term storage of large amounts of information. Due to the access and organization requirements for data on these systems, the requirements for this Zone vary from those of a Storage Zone.

Application execution environments should not be included within the Data Zone.

Appropriately safeguarded High Sensitivity information (even when in bulk or aggregate form) may be stored in this Zone. Depending on the relevant TRA, OPS personnel security screening may be required to gain authorized access to a Data Zone.

This Zone may also include systems with high availability and integrity requirements.

2.2.5.2. Control requirements

The following controls **must** be implemented within the Data Zone:

- Traffic received from an Logic Zone **must** be reliably controlled such that only those protocols required for performing database queries are available;
- The Logic Zone **must** be the only Zone capable of issuing a query to servers located within a Data Zone, except for instances where additional safeguards have been implemented (as per section 2.2.12); and
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.5.3. System security requirements

All systems located within the Data Zone **must:**

- Be hardened, in a manner appropriate for the deployed platform, against attack and misuse;
- Be protected from malware;
- Be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- Be subject to ongoing monitoring and evaluation;
- Not accept queries or connections from any anonymous or unknown source of traffic, and process requests only from known hosts;
- Be protected by safeguards suitable for sensitive information (if present), in accordance with ISPC requirements;
- Never receive or process database commands (e.g., SQL) received directly from interactive users via the Logic Zone; and
- Use a unique account and access control for ODBC connections, and never rely upon the default SA account (or similar default administrative account, unless vendor/product constraints preclude this requirement).

2.2.6. Operations Zone

2.2.6.1. Definition

An Operations Zone is a general-purpose network intended for end-user computing and daily tasks. Operations Zones include typical office networks (e.g., OPS desktop computing).

2.2.6.2. Control requirements

The following controls **must** be implemented within the Operations Zone:

- High Sensitivity information **must** not be electronically stored (e.g., aggregate or bulk long-term storage) in this Zone;
- Traffic received from other Zones **must** be reliably controlled such that only those protocols required for managing systems and providing connectivity are permitted; and
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.6.3. System security requirements

All systems located within the Operations Zone **must:**

- Be hardened against attack and misuse (in a manner suitable for the system in question, be it a client desktop, server, or appliance such as an IP phone or multi-function device); and
- Be protected from malware.

2.2.7. Storage Zone

2.2.7.1. Definition

Systems intended to provide bulk and/or long-term storage of data, or provide for a backup service, are components found within a Storage Zone. This Zone contains systems that provide a layer of abstraction for dedicated storage hardware (e.g., tape libraries). SAN deployments are also considered Storage Zone components.

High Sensitivity information may be stored in this Zone. Depending on the relevant TRA, OPS personnel security screening may be required to gain authorized access to a Storage Zone.

This Zone may include systems with high availability and integrity requirements. A backup service within this Zone, for example, will have implications for Disaster Recovery and Business Continuity plans.

2.2.7.2. Control requirements

The following controls **must** be implemented within the Storage Zone:

- No traffic should spontaneously originate from the Storage Zone (with the exception of authorized management and monitoring traffic);
- Only authorized hosts and networks are permitted to issue connections or queries to the Storage Zone;
- Traffic received from other Zones **must** be reliably controlled such that only those protocols required for managing systems and providing connectivity are permitted;
- Interactive sessions to systems within an Storage Zone **must** only be permitted from a Management Zone, or, when in conjunction with additional safeguards, an Operations Zone;
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors); and
- No traffic should be transferred by proxy, routed, or otherwise passed from the Storage Zone to Zones where such traffic would not be permitted via a direct connection.

2.2.7.3. System security requirements

All systems located within the Storage Zone **must:**

- Provide protection for High Sensitivity information, if applicable (e.g., through the use of access control techniques, and cryptography that meets the requirements described in GO-ITS 25.12);
- Be hardened, in a manner appropriate for the deployed platform, against attack and misuse;
- Be protected from malware;
- Be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- Be subject to ongoing monitoring and evaluation;
- Be subject to Disaster Recovery and Business Continuity planning requirements;
- Deny queries or connection from any anonymous or unknown source of traffic, accepting requests only from authorized hosts; and
- Operate only those applications required to perform required storage and backup duties, to reduce the attack surface of Storage Zone hosts.

2.2.8. Management Zone

2.2.8.1. Definition

The Management Zone is intended as a secure network environment from which to operate and monitor systems located in other Zones. Systems within this Zone are typically used to monitoring server health, storage capacity, security events, and system logs. Such a network provides the ability to manage hosts from a central and documented location.

Due to the level of access afforded to the Management Zone, it is critical that it be secure from attack and ingress access from other Zones.

Depending on the relevant TRA, OPS personnel security screening may be required to gain authorized access to a Management Zone.

2.2.8.2. Control requirements

The following controls **must** be implemented within the Management Zone:

- The traffic within the Management Zone **must** not be observable from other networks or Zones;
- Traffic received by the Management Zone **must** be reliably and stringently controlled to reduce the likelihood of unauthorized access;
- The Management Zone **must** be the only Zone capable of issuing interactive sessions and/or administrative queries to systems within the Storage Zone and Security Zone, and is the preferred location for enterprise administration activity;
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors);
- The Management Zone should offer protection for High Sensitivity information, if applicable (e.g., through the use of access control techniques, and cryptography that meets the requirements described in GO-ITS 25.12);
- The only means by which to gain access to a Management Zone **must** be local console access, or a Virtual Private Network connection which uses both strong authentication (e.g., two-factor) and approved cryptography;
- Be subject to Disaster Recovery and Business Continuity planning requirements;
- Strong authentication **must** be used for interactive sessions between any system within a Management Zone and any other Zone;
- There **must** be no direct network path between an Unmanaged Zone, Access Zone, or Presentation Zone and a Management Zone; and

- This Zone **must** deny/drop all spontaneous inbound traffic with the exception of expected management traffic from known hosts (e.g., Event Log data, UNIX *syslog* data, SNMP traps, e-mail notifications).

2.2.8.3. System security requirements

All systems located within the Management Zone **must:**

- Be hardened to a robust specification, appropriate for the deployed platform, to withstand sustained attack;
- Be protected from malware;
- Be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- Be subject to ongoing monitoring and evaluation;
- Be subject to audit; and
- Deny queries or connection from any anonymous or unknown source of traffic, accepting requests only from authorized hosts.

2.2.9. Security Zone

2.2.9.1. Definition

A Security Zone is intended as a special-purpose network where security devices and systems are operated. Systems within a Security Zone may process and store High Sensitivity information, and have exceptional integrity and/or availability requirements; a backup service within this Zone, for example, will have implications for Disaster Recovery and Business Continuity plans.

The systems within a Security Zone may be logically or physically isolated from one another, or other Zones.

A Security Zone is also intended to protect sensitive cryptographic material, PKI certificate authorities, services with forensic requirements, and related systems. Life safety systems and mechanisms may also be located within a Security Zone.

Depending on the relevant TRA, OPS personnel security screening may be required to gain authorized access to a Security Zone. This TRA may further indicate that employee Position TRAs are required when specifying roles and defining employee access for a Security Zone. A Disaster Recovery and Business Continuity plan may be required for any systems in a Security Zone.

2.2.9.2. Control requirements

The following controls **must** be implemented within a Security Zone:

- The traffic within the Security Zone **must** not be observable from other networks or Zones;

- Traffic to and from this Zone should be controlled by both type and volume;
- Operational systems required for security system maintenance **must** be located within the Security Zone;
- No interactive sessions are permitted to enter a Security Zone from another Zone that is not itself a Security Zone or Management Zone;
- No traffic is permitted to cross a Security Zone interface point unless it has been generated in response to a request originating within the Security Zone, or originates from a known host within a Security Zone or Management Zone;
- No traffic is permitted to cross a Security Zone interface point unless it has been authorized, the data or session is authenticated, and the information is subject to monitoring and review; and
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.9.3. System security requirements

All systems located within a Security Zone **must:**

- Be hardened to a robust specification, appropriate for the deployed platform, to withstand sustained attack;
- Be protected from malware;
- Be subject to security processes such as Threat Risk Assessment (TRA) and Security Testing and Evaluation (STE) prior to deployment;
- Be subject to ongoing monitoring and evaluation;
- Be subject to audit; and
- Require strong (e.g., two-factor) authentication for any system access of any kind.

2.2.10. Extranet Zone

2.2.10.1. Definition

The Government of Ontario has many agreements with agencies, partners, and vendors that require extranet access. This access is managed via contracts, memoranda of understanding, and security policies. The Extranet Zone therefore does not meet the definition of an Unmanaged Zone, particularly when conducted via dedicated circuits instead of public networks. This Zone can be viewed as a logical (but safeguarded) extension of the Government network.

An Extranet Zone supports this type of external connection.

Because this Zone can include systems the Government of Ontario does not directly manage, there exists an increased degree of risk that **must** be addressed.

2.2.10.2. Control requirements

It is recommended that the requirements and practices for this Zone be developed as agreements are made, and enforced in concert with Extranet Zone partners.

The following requirements are mandatory for the Extranet Zone:

- No Extranet Zone agreement can remove the requirement for boundary control and policy enforcement at the Zone interface point; and
- Activity monitoring, logging, and review **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements (e.g., via Intrusion Detection or Intrusion Prevention sensors).

2.2.10.3. System security requirements

Extranet systems are not necessarily managed by the Government of Ontario. However, the systems within an Extranet Zone (e.g., by means of contracts or a memorandum of understanding where possible) should:

- Be subject to audit;
- Be hardened, in a manner appropriate for the deployed platform, against attack and misuse; and
- Be protected from malware.

2.2.11. Zone integration rules

The permissible connections between Zones are an important part of the Zone strategy; they serve to reduce exposure of sensitive systems and information, particularly when an elevated degree of risk may exist.

2.2.11.1. Network connectivity

The following requirements are mandatory:

- Virtual Private Network tunnels **must** terminate at Zone interface points to permit inspection and monitoring;
- Traffic from Virtual Private Network tunnels (including those used internally) **must** be visible to firewalls acting as Zone interface points, to permit for the management of traffic and protocols issued to a Zone; and
- Virtual Private Networks are not a replacement for authorization and authentication services; any requirement for these services (e.g., as identified by a TRA) **must** be independently provided within a Zone.

2.2.12. Server and component placement

The following table describes direct destination traffic permitted between Zones. A Zone can communicate with another Zone of the same type, unless a TRA or other security finding for a specific Zone recommends against it.

Source of Connection	Acceptable Destination Zone(s)
Unmanaged Zone	Access Zone
Access Zone	Presentation Zone Logic Zone (with additional safeguards, in some situations – see 2.2.13) Operations Zone
Operations Zone	Access Zone Presentation Zone Logic Zone Data Zone (with additional safeguards) Storage Zone (with additional safeguards) Security Zone (with additional safeguards) Management Zone (with additional safeguards)
Presentation Zone	Access Zone Logic Zone Storage Zone Management Zone
Logic Zone	Presentation Zone Data Zone Storage Zone Management Zone
Data Zone	Logic Zone Storage Zone Management Zone
Storage Zone	Access Zone Presentation Zone Logic Zone Data Zone Operations Zone Management Zone

Security Zone	Storage Zone Management Zone
Extranet Zone	Access Zone Presentation Zone Logic Zone
Management Zone	Access Zone Presentation Zone Logic Zone Data Zone Operations Zone Security Zone Storage Zone

Possible additional safeguards for Operation Zone communications with the Data Zone, Storage Zone, and Security Zone include (but are not limited to) the following:

- Dedicated Operation Zone segments for communications;
- VPN communications with approved cryptography;
- Strong authentication (e.g., two-factor) and/or secure protocols;
- Dedicated equipment (e.g., not used for general purpose computing); and/or
- Additional safeguards recommended by a relevant TRA.

2.2.13. Placement of services with multiple components

Server Type	Acceptable Deployment Zone
Public DMZ Web Server	Access Zone (in a DMZ)
Public Network Services	Access Zone (in a DMZ)
Intranet Web Server	Presentation Zone
Web/Application Server	Presentation Zone
Web/Application/Database Server	Presentation Zone
Application or Business Logic Server	Logic Zone
Application/Database Server	Logic Zone
Database Server	Data Zone

Servers with mixed functions (e.g., a web server running an application, or an application with an internal database, etc.) may introduce vulnerabilities to a Zone, and negate the value of separating components. As such, servers **must** be placed in the Zone corresponding to the component most exposed to client input and/or unmanaged traffic.

Deployed systems that rely on web server software to serve or manage applications (e.g., a content management front-end) may be located within the Logic Zone, but additional safeguards may be required.

Projects with a business requirement to operate multiple functions on a single server, or deploy varying types of servers in a single Zone, should review relevant TRA findings to determine if elevated risk has resulted due to non-standard component placement. Such risk may require mitigation.

When non-standard placement occurs, some shared facilities which rely on the security inherent in a Zone for their own placement may be unavailable.

2.2.14. Placement of services by sensitivity

Information contained in traffic that traverses Zones **must** be classified according to sensitivity (i.e., according to ISPC). When deciding which controls to employ in order to mitigate the risk posed to data, systems, and applications, the source (e.g., originating Zone) of queries should also be considered, particularly with reference to information sensitivity.

2.3. Security Design Concepts

Security Design concepts are presented here as considerations for all program areas planning new systems or services. These concepts, if embraced during design and development efforts, can enhance overall security, deter attack, and make new systems more resilient.

Some Security Design considerations are considered mandatory because they assist in defeating known attacks, or because they offer both broad applicability and considerable value for protecting I&T assets relative to the cost of implementation.

2.3.1. Identity

Identity refers to the attributes that allow a person or system to determine who an individual is as a unique entity. When a system attempts to ascertain identity and make a determination regarding access, the following are examined:

- Who the user is (positive identity);
- Evidence of identity provided by the user (authentication); and
- Permissions for access and granting of rights (authorization).

Before deciding what functions an individual is allowed to perform, identity **must** be established. The degree of assurance required will vary according to the goals of the system, the information to be accessed, and the findings of a PIA, TRA, or similar documentation. In cases where sensitive information is stored or processed, two-factor authentication may be required (especially when recommended by a relevant TRA) to provide adequate assurance.

In some cases, authorization is independent from authentication and identity (e.g., not allowing any user to authenticate to a system after midnight, regardless of their identity). This section explains basic identity requirements and concepts with the assumption that positive identification is required for access.

For systems that will identify a user or evaluate a device or system credential (e.g., a device certificate), the following criteria **must** be employed:

- User or host credentials **must** be unique, and not shared with other users or hosts (e.g., a PKI certificate would be associated with a single user);
- The unique credential **must** be validated by a separate authority (e.g., a PKI Certificate Authority or central directory) where technically feasible;
- Credentials **must** be protected and not readable or easily altered. For example, a hardware token can be made tamper resistant. Passwords **must** be obscured when typed and protected in transit, to reduce the likelihood of interception; and
- Identity credentials **must** remain confidential when processed by authentication and authorization systems.

2.3.2. Privilege

Privileges are rights assigned to user accounts that permit for enhanced abilities within a system or application. Typical rights include the ability to manage user accounts, alter or manage content, write to system files, or perform maintenance.

Privileged user accounts are often required for administrative access to systems and applications. These accounts require a strong degree of identity assurance and must be protected from unauthorized use in accordance with the requirements stated in GO-ITS 25.0. For more information, refer to section 2.5.17 of this document.

2.3.3. Authorization

An authorization process validates that an individual (or process) has the rights to access a resource or data, and assigns appropriate privileges or credentials. A user may be authorized to read the files served by a public web server or FTP site, but is typically not authorized to change the content.

Basic authorization design requirements are as follows:

- Identity **must** be established before authorization takes place, except in instances where a service is explicitly intended for anonymous access;
- The principle of least privilege **must** be observed; and
- Users are authorized in accordance with the “need to know” principle (e.g., based on job requirement). For more information, refer to section 2.3.7 of this document.

Access control systems **must** only permit access to Government of Ontario I&IT systems or networks upon successful identification, authentication, and reference to an authorities file or user profile, unless the service is explicitly intended for anonymous access.

Access to information **must** be protected by default (e.g., a separate action must be required to allow access).

2.3.4. Authentication

Authentication is the process and result of verifying (prior to granting access) that the user presenting credentials is indeed the individual they purport to be. Authentication provides a degree of identity assurance by testing the credentials granted. This degree of assurance varies on the specific implementation, but can often be enhanced.

Three common types of credentials for authentication are:

- Something the user has (e.g., a token or digital certificate)
- Something the user knows (e.g., a password, phrase, PIN)
- Something the user is (e.g., biometric identifiers, such as fingerprints or voice)

A common means to enhance identity assurance is to protect the communications channel the authentication occurs over (to deter interception and replay) and to require multiple credentials (sometimes called “factors”). A *strong* authentication scheme is one that uses such techniques to deter attack and subversion. A two-factor authentication scheme would require that a user present the following:

- Two distinct identifying credentials corresponding to the user, not a group
- The two credentials **must** use different types of authentication

Access to sensitive or classified information, or from an Unmanaged Zone, are typical rationales for increasing the level of assurance associated with authentication.

2.3.5. Default deny

All authentication and security systems **must** deny access by default when a failure to provide correct identity credentials occurs. Life safety systems are common exceptions to this practice, as a denial of access in that context could result in harm to health and safety.

2.3.6. Separation of duties

Separation of Duties can prevent even authorized and authenticated individuals from causing undue system impact, or engaging in malicious activities (e.g., removing information or tampering with audit logs). A typical implementation of this principle would be to prevent user or system administrators with powerful privileged accounts from manipulating activity and audit logs (e.g., for the purposes of engaging in insider attacks or fraud).

The Separation of Duties principle **must** enforced as per the requirements stated in GO-ITS 25.0 General Security Requirements.

In particular, Separation of Duties **must** be enforced for all access to systems and applications processing high sensitivity information.

2.3.7. Need to know

“Need to know” describes the legitimate requirement of a person or organization to know, access, or possess specific sensitive or classified information during the performance of an authorized, assigned role. Information sharing arrangements should be based on the necessity for access to, or knowledge of, only that information required to carry out official duties. Secure systems and access control can support this principle

.

2.3.8. Separation of knowledge

Split knowledge is a condition under which two or more entities separately know or possess components that, individually, convey little or no knowledge of the resulting combination. Separation of data or information into two or more parts requires that each part remain constantly under the control of separate authorized individuals or teams; one individual or team will never have knowledge of the complete piece of data.

Since split knowledge means that two or more individuals are custodians for data that is only useful when combined, it can be a useful isolation technique when applied to access control and authentication (or processes like cryptographic key generation). Split knowledge can also be used within operations groups to share portions of information required to access systems during emergency situations.

2.3.9. Separation of custody

This is a process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions, and no single entity must be able to access or use the materials

This technique can be applied to physical access control. For example, two keys may be turned at the same time to open a secure door, but the keyways are located far enough apart that a single individual cannot turn both at once. Some facilities with secure rooms will employ biometrics using a similar arrangement.

2.3.10. Separation of test, development, and operations facilities

Separation of test, development, and operational systems or networks **must** be performed in accordance with GO-ITS 25.0 General Security Requirements.

2.3.11. Isolation

Isolation provides a means to control and secure data, and is a means to separate critical processing or High Sensitivity information from other production activities. Isolation typically refers to complete physical separation of systems from other environments and hosts (e.g., discrete hardware and dedicated network equipment).

Isolation of critical or sensitive processing environments from general production **must** be conducted as per GO-ITS 25.0 General Security Requirements when it is deemed to be a worthwhile safeguard in a particular environment (e.g., according to a TRA).

2.3.12. Roles and authority

Each automated system access control mechanism **must** provide for an up-to-date authorities file or user profile that lists all of the resources to which each authorized user may have access and what transactions or limits are permitted to each individual.

Authorized users **must** have access profiles defined and controlled so as to restrict the functions that they can perform (e.g., read, write, execute, update, allocate, delete, or create). Time and location may also be used to limit access by users to specific times or from certain locations.

2.3.13. Grouping roles and authority

Authorities **must** be grouped for users who:

- Need access to the same data, files, and directories;

- Have the same authorities (e.g., none, read, read and write); and
- Have the same security clearance and need to know (e.g., can access all files with equal or lower security classification when required for job function).

2.3.14. Enforced network path

Network access control **must** be enforced as per the network security requirements stated in GO-ITS 25.0 General Security Requirements. When designing systems or solutions, the following techniques may be considered:

- The system could require that data traverses a specified path from a specific host to a specific host, where possible;
- Generic allowances of any source IP traffic to any destination IP **must** not be permitted at Zone interface points;
- The minimum number of data ports is to be used for any given type of connection. Opening a broad range of inbound listening ports **must** be avoided unless required by a specific application;
- Where possible, connections should be TCP based; and/or
- If stateless connections are necessary (e.g., UDP-based protocols with no current TCP equivalent), these should be restricted to specialized servers (and not made available from dedicated network devices). Notable examples are DNS servers, which should be dedicated to performing Domain Name Service resolution.

2.4. Operational Security Requirements

2.4.1. Logging and events

Activity, system, and audit/event logging **must** be conducted in accordance with GO-ITS 25.0 General Security Requirements.

2.4.2. Account creation and management

An account **must** be created, changed, suspended or deleted only by an authorized Security Administrator. The ability to create user accounts **must** be controlled according to the need to know, least privilege, and separation of duties principles.

Procedures and tools **must** be in place to permit prompt identification of the individual assigned an account (e.g., based on other information, such as a computer name or DHCP address) without the user being contacted or made aware that an authorized investigation is underway.

Security staff **must** maintain a list of assigned accounts (an original list not produced from systems during an emergency situation) for each user, including the name of the authorizing manager.

The identifying information **must** include name, location, department, telephone number and other information required by the program area. In the case of contract resources, the internal sponsor **must** be identified.

For new services and applications, account management implementations **must** include the following revocation capabilities:

- Accounts **must** be terminated immediately upon request from the responsible program manager;
- Accounts **must** be suspended if invalid sign-on attempts exceed the specified number of attempts;
- Following the issue of a new administrator password or password reset, an account **must** be suspended if not accessed within 24 hours;
- Accounts that have been inactive for 60 days **must** be suspended; and
- If an account is suspended for inactivity, notification **must** be forwarded to the authorizing manager. Upon specific written request from the responsible manager, the account may be retained, but if it remains unused within six months, the account **must** be deleted.

2.4.3. Account distribution

The distribution of user accounts **must** be controlled according to the need to know, least privilege, and separation of duties principles. Distribution **must** also occur in a secure fashion (e.g., resistant to interception or manipulation).

2.4.4. Password distribution

Distribution of passwords **must** be performed in a controlled manner by means of a secure distribution system. The initial password should be generated by an automated service, and issued directly to the user in a manner that no one else can observe the password.

Any advice that a password is being distributed **must** be separate from the actual password. The user **must** be the only person to see the password, and **must** acknowledge its receipt. This process must also be auditable.

If the distribution of a password is the result of a reset, the responsible administrator **must** verify the identity of the user. All password distribution and use must comply with the requirements described in GO-ITS 25.0 General Security Requirements.

2.4.5. Default accounts

All Accounts supplied with a product by a vendor for the purposes of enabling access by administrative or support staff **must** be suspended, deleted or otherwise securely changed prior to implementation, in accordance with GO-ITS 25.0.

At the testing stage, examination of the product **must** include testing for the successful control of default accounts and/or passwords. New passwords assigned to default accounts that cannot be removed **must** be stored in a secure fashion.

2.4.6. Malware controls

The objective of these controls is to protect the integrity of software, systems, and information.

All new systems and services **must** employ controls to protect against the introduction or propagation of malicious content (or “malware”).

Malicious code may be present as executable or interpretable content in files, email or web content. All of these should be scanned and verified against known signatures/indicators of malicious code. Attack signatures **must** be monitored on a daily basis, and updated immediately upon release, for detection functions to remain effective. Systems should ideally include mechanisms to detect new or customized malware.

In addition:

- The installation of software **must** be restricted to administrative staff;
- Anti-malware tools **must** be installed, operated, and updated regularly for both clients and servers, as appropriate; and
- Local firewall software **must** limit both incoming and outgoing network connections to pre-defined services and applications.

Software updates **must** only be downloaded from managed sites. Hashed signatures / certificates of origin for the software **must** be provided by the vendor, and **must** be confirmed to be accurate prior to installation. Software updates **must** be implemented promptly, and tested prior to installation if change control requirements apply to the environment.

2.4.7. Credential expiry

After a password has expired, access to all resources **must** be denied until a new password has been selected.

Program Managers **must** immediately notify their Cluster Help Desk when an individual has left their unit and the individual user’s access and privileges **must** be removed from all drives, directories, hardware credentials, and mobile devices to which they had access.

2.4.8. Audit

Audit capabilities **must** be deployed for new systems, in accordance with GO-ITS 25.0 General Security Requirements.

2.4.9. Access control

Designing appropriate controls and deciding which controls to apply is based on the maximum sensitivity of the information in question.

The design and operation of access control systems **must** comply with the guidance published in GO-ITS 25.0 General Security Requirements.

2.4.10. Remote access

Remote, interactive access to Government of Ontario networks **must** require users to authenticate using strong (e.g., two-factor) authentication.

Any dial access to Government of Ontario I&IT assets **must** be managed as per GO-ITS 25.7 Security Requirements for Remote Access Services.

2.4.11. Automated logon

Access to Government of Ontario information, computing systems, and network resources **must** be attained through a secure sign-on process.

Each user **must** be required to formally sign on before being granted access to a network, system or application. This will involve presentation of a valid username and corresponding password and/or other authentication credentials.

2.5. System Security Requirements

2.5.1. User passwords

The most common authentication method used within the OPS is to verify that the user knows a prearranged secret – a valid password.

All use of passwords within the Government of Ontario **must** comply with GO-ITS 25.0 requirements.

In situations where high assurance is required, a combination of authentication methods is appropriate.

2.5.2. System passwords

Where system passwords (e.g., passwords for maintenance or administrative accounts) are used to enhance security by providing secondary authentication for specific features or privileges, the system password **must** not replace the requirement of an individual username and password. Such schemes are common on network devices.

System and user passwords **must** not be the same. When second level passwords are used as part of a new design, the system or device **must** be reviewed to ensure that system passwords are appropriately configured and managed.

2.5.3. Password storage

New deployments should leverage enterprise services for password assignment and management.

Passwords **must** not be written down or printed in hard copy, except as part of a formal process surrounding emergency/fire accounts (see section 2.5.19).

Users **must** not store their passwords in system software to facilitate sign-on.

System and application password files or databases should be stored separately from application data; they **must** also be configured in a secure manner, to prevent unauthorized access (e.g., to deter attacks against hashed entries).

Passwords **must** remain encrypted in storage; systems that need to verify passwords **must** validate against a representation of the passwords. Hash algorithms are typically used to accomplish this (ideally in conjunction with enhanced methods, such as the use of HMACs). This scheme allows passwords to be verified, but does not permit decryption of the stored passwords. A “salt” value of least two UTF-8 encoded characters (e.g., 16 bits) **must** be prepended to each password if a secure hash algorithm is used to deter brute-force and dictionary attacks. Longer salt values are preferable.

If an existing system does not support storing passwords in a hashed form, then the owner **must** ensure that adequate security mechanisms (e.g., access control) are in place to protect and assure the confidentiality of stored passwords. The password or pass phrase that enables decryption **must** be protected in a manner commensurate to the sensitivity of the information protected, and encryption specifications must comply with GO-ITS 25.12 Use of Cryptography.

Self-service password recovery systems **must** be designed in a secure fashion, and meet all requirements for password storage.

2.5.4. Authentication attempts

In the event of repeated consecutive attempts to authenticate with an incorrect password (e.g., in excess of ten attempts), the system **must** prevent further attempts by disabling the account for a predetermined period of time. This time period will vary depending on the security requirements of the system. This activity **must** be recorded by audit logs in accordance with GO-ITS 25.0 General Security Requirements, and preserved for two years in accordance with GO-ITS 25.8 Security Requirements for Servers.

Invalid authentication attempts **must** clear the connection and/or force the user back to the beginning of the sign-on sequence. A security violation alarm **must** be generated following each unsuccessful session and, if applicable, the line or logical channel cleared.

Reactivation **must** require intervention on the part of an administrator.

The system **must** impose a delay between unsuccessful sign-on sessions.

2.5.5. Forced logoff

The resource owner **must** determine the appropriate period of inactivity to invoke a forced interactive session timeout, with reference to the exposure and risk (as identified by a TRA). Users who resume such a session will be required to enter their credentials.

Users **must** be automatically logged off, or optionally, the system **must** suspend the session and re-authenticate the user before allowing further activity, under the following circumstances:

- When inactive terminals have exceeded a defined period of inactivity documented in a local system policy;
- When screen-lock features are not or cannot be implemented, and there is no activity from the terminal for a maximum period of 20 minutes (or less if recommended by the relevant TRA) as per GO-ITS 25.0;
- Following an error or interruption in the communications link between the user and the system; and
- Upon system failure, if the system must fail closed (e.g., if required by a TRA).

When the system is outputting information to a terminal and if the time since the last input exceeds the established log-off limit, then the terminal **must** be logged off on completion of output.

The forced log-off process **must** be uninterruptible once it has been initiated. Any cached local credentials should be expired, if possible.

Whenever a user is logged off in a switched connection, all communications links, lines, channels and screens **must** be cleared or reset as part of the log-off sequence.

2.5.6. Concurrent sessions

An individual account should not be signed on to multiple concurrent interactive sessions on any single system or application, as concurrent sessions can in cases appear to be indicative of a security event, and may merit investigation (particularly when occurring from disparate locations).

Under special circumstances, one or more users may require concurrent session privileges. Exceptions for Administrators may be granted, where warranted, under controlled conditions subject to audit.

2.5.7. Automatic workstation locking

Each workstation **must** be configured with automatic locking functionality that activates when the system is not in use.

2.5.8. Logon messages

Upon successful authentication to any Government of Ontario I&IT system or network, a message **must** be produced that indicates the prohibition of unauthorized access to any

Government of Ontario computing resource or networked computing system. The notice should also include an approved reference to an Acceptable Use Policy.

2.5.9. System banners

A system (e.g., a server that can be remotely accessed) **must** not identify itself in any way prior to successful user identification and authentication. Welcoming messages **must** be avoided (e.g., an invitation to access the resource). Any prompts for a username and password are to be generic in nature, and should not identify the system or type of system being accessed or its purpose.

Greetings, “welcome” banners, or similar phrases **must** not be displayed until the user has been successfully authenticated and access authorized. System banners that warn against unauthorized use (and use approved wording) may be required for some types of systems (e.g., if recommended by a TRA).

2.5.10. User sessions

All of the activity generated by a user from the start of the sign-on process through to conclusion of the log-off process constitutes the user session. Security controls **must** provide reasonable protection against eavesdropping, hijacking, or other interference with a user session.

The state of a user session **must** be set and controlled by the system or application providing services. A user **must** not be able to modify or arbitrarily define the session state.

The service administrator **must** be able to:

- Determine the existence of a given user session; and
- Suspend or terminate any particular session without requiring the cooperation of the user.

Compromised session state information (usually from the network or an unattended workstation, even in encrypted form) **must** not be vulnerable to re-use or replay from or on other systems or at later times. LDAP, Active Directory, and similar traffic may carry identity credentials, and should remain encrypted over unmanaged networks, or be restricted to managed networks.

Possession of copies of the session management software, in source or binary form, **must** not contribute to the ability to compromise any session or to establish unauthorized sessions.

If cryptographic mechanisms are used to help maintain session integrity and confidentiality, the specifications and design **must** comply with the requirements described in GO-ITS 25.12 Use of Cryptography.

2.5.11. User accounts

User identification is required to identify who (or what agent) is requesting access to systems or information. To achieve this, there **must** be:

- A formal user and username registration (and de-registration) process; and
- A unique identifier (e.g., username) assigned to each known user of the system.

Any access control processes involving the management of user accounts and/or passwords **must** comply with the requirements in GO-ITS 25.0 General Security Requirements.

2.5.12. Account types

Five types of accounts commonly seen within the Government of Ontario include:

- Individual accounts (including vendors and contractors);
- Role or functional accounts;
- System accounts;
- Group accounts; and
- Privileged accounts.

The requirements surrounding such accounts are described in the following sections of this document.

2.5.13. Individual account controls

An individual account is one assigned to a single person (employee, customer, third-party service provider employee, vendor, contractor, etc.) and is unique to that individual. This account may be portable and remain with the individual during his/her time of employment or other business relationship with the Government of Ontario (some applications do not permit portability).

An individual is entirely responsible for their individual account. Access to the account **must** not be shared. Users **must** be held accountable for all actions performed on Government of Ontario systems for each account assigned to them.

2.5.14. System account controls

Access control related to system accounts (e.g., maintenance or administrative accounts that do not include elevated privileges, or default accounts that cannot be removed) must be managed in accordance with the requirements described GO-ITS 25.0 General Security Requirements.

System accounts should be individually assigned wherever possible (by means of a uniquely assigned account granted to a specific individual). Access to such accounts **must** not be shared, and the system account **must** not be used for general purpose computing.

Assigned system accounts **must** be securely maintained by the users they are assigned to, and made subject to review/audit.

2.5.15. Vendor and third party account controls

Third Party Service Providers, Vendors, Contractors and their employees **must** only be assigned individual accounts. Individual accounts are assigned to specific personnel who have been granted access to certain facilities. Terms of use for these accounts **must** be detailed in formal agreements, and personnel screening may be required.

Responsibility for ownership and proper usage of these accounts **must** rest with the responsible unit or department sponsoring such access.

Individual accounts for third parties **must** be automatically revoked at the end of the applicable contract, and **must** be reviewed and re-authorized every six months, unless renewal is requested and granted prior to the expiry date.

Third party accounts **must** not be authorized to access production systems without specific security review and approval.

Privileged accounts and the actions associated with them **must** be subject to audit whenever administrator privileges are required for third parties.

2.5.16. Role or functional accounts

Functional accounts, including system accounts are used by automated system processes to perform specific pre-determined activities. (e.g., program start-up, file transfer, batch commands, or system service initialization). Individuals **must** not be able to use functional accounts to authenticate to a system, or perform *ad hoc* tasks.

Functional accounts are associated with a specific system function, or organizational unit. Accountability and responsibility for functional accounts rests with the system administrator of the unit or program area, or the responsible program manager.

2.5.17. Management of privileges and privileged accounts

The allocation and use of privileges (any feature or facility of a multi-user information system that enables the user to override system or application controls) **must** be restricted and controlled. These features and facilities include all privileged accounts and system utilities.

The use of system or network privilege **must** be managed and used in accordance with the access control and administrator password requirements stated in GO-ITS 25.0 General Security Requirements. In addition, the following requirements apply:

- All privileges associated with each system product (e.g., operating system, database management system, etc.) **must** be identified to the network, system and/or security administrator;
- All privileged users **must** be identified to the relevant unit or program area network, system and/or security administrator(s);
- Where a specific application requires the equivalent of a username to log on using administrator privileges, the application account **must** not be the application name;

- The assignment and use of privileged accounts **must** be limited to a minimal number of persons who are directly responsible for system support or administration;
- Privileged accounts **must** be used only as necessary to perform administrative functions. These functions **must** be identified as “key technical positions”, and be staffed appropriately;
- An authorization process and up to date record of all privileges allocated **must** be maintained;
- Separate logs **must** be maintained of all privileged user activity. Such logs **must** not be accessible by individual privileged users;
- Resource owners **must** review the activity logs for privileged users at least monthly;
- Administrative and/or elevated privileges for production systems **must** be formally authorized and reviewed every six months, and terminated immediately when no longer required for business purposes;
- Two-factor authentication **must** be used for privileged accounts in any instance where remote access will cross external organizational boundaries (e.g., a session originating from an Unmanaged Zone); and
- Electronic activity and audit logs **must** record account access and privilege use in accordance with the requirements stated in GO-ITS 25.0 General Security Requirements.

Where supported by the system, users **must** be required to first authenticate to the system using their individual account prior to invoking a privileged ID. This provides for both an enhanced level of accountability and greater protection of systems.

2.5.18. Emergency accounts

Emergency accounts **must** be issued for a limited period of time (e.g., 24 hour period) and on an event-by-event basis.

An emergency account is a type of privileged account that can be granted to production support, operators, or vendors that may require both immediate maintenance access to systems and system privileges exceeding those granted for *ad hoc* tasks.

A UNIX *root* account is the most powerful type of privileged account that can be granted for a UNIX system. Use of root accounts (and accounts with similar privileges) **must** be managed according to any applicable platform specific standard (e.g., GO-ITS 25.8 Security Requirements for Servers), in addition to the requirements described in GO-ITS 25.0 General Security Requirements. For Windows systems, the equivalent privileged default account is *Administrator*.

Separation of duties **must** be maintained. Developers **must** not have fire account or privileged account privileges on production systems.

Passwords for emergency account and administrative accounts **must** be stored in a sealed envelope, and stored under dual-custody control by senior officers within the relevant operations group for the unit or program area.

Each use of a fire account or administrative account during an emergency or incident **must** be authorized, recorded, and reviewed; a new password **must** then be issued and secured for emergency accounts after such use.

2.5.19. Use of privileged system utilities

System utility programs that might be capable of overriding system and application controls **must** be tightly restricted and controlled.

The use of system utilities, audit tools, and other functions **must** be managed and used in accordance with the requirements stated in GO-ITS 25.0 General Security Requirements. In addition, the following requirements apply;

- Unnecessary software utilities and system software **must** be removed;
- Test and development software and systems **must** be rigorously separated from production environments in accordance with the requirements described in GO-ITS 25.0 General Security Requirements;
- System utilities **must** be segregated from application software;
- System utilities **must** be tested and validated, and availability **must** be controlled;
- Procedures for use of the utilities (e.g., who may be authorized, for what purpose, for what duration, and any advance approval requirements) **must** be documented;
- Availability and use of system utilities **must** be limited to the minimum practical number of managed authorized users and **must** follow the procedures documented in the item immediately above;
- All uses **must** be formally authorized, documented and all activities **must** be logged;
- Logs **must** be subject to regular review, and;
- Removal of system utilities when no longer required **must** be verified by the relevant operations management group.

2.5.20. User assistance

A user **must** not to be able to perform any function or receive any automated assistance until authentication has been completed.

2.5.21. Bypass

The sign-on procedure **must** not be bypassed by users, and **must** be implemented in such a manner to preclude such bypass.

2.5.22. Failure modes

Where a TRA or functional specification requires a “fail-closed” mechanism, authorization failure **must** result in a denial of access. The intention is to prevent an unintentional escalation of privileges. In the case of a failure, authorization levels **must**

be less than they would be in the case of success (e.g., no access, or a cessation of operation).

Where a TRA requires a fail-open mechanism (e.g., life and safety systems), a failure in a system will result in access being granted (e.g., via a fire door).

2.5.23. Authentication notices

The system **must** not indicate any special status of the account (e.g., privileged, suspended, etc.) until authentication has been completed.

Each initial time a user successfully signs on to a server that processes or stores data on behalf of the Government of Ontario (and when supported by the technology), a message should be displayed advising the user of the date and time of the last successfully authentication session, as well as the number of unsuccessful attempts since the previous session. This message should be separated from other system messages, such that it may be clearly seen by the user and provide them with a means by which to determine if unauthorized access to an account has occurred.

2.6. Network Requirements

2.6.1. Segregation

Network segregation is a means to accomplish network access control. Segregation simply means reliably dividing a network path into smaller networks where inbound and outbound traffic can be controlled.

Networks should be segregated under the following conditions:

- Interface points between Zones **must** provide for reliable network segregation;
- Hosts that do not conform to the rules for implementation in a given Zone may be segregated from other hosts within that Zone as a compensating control;
- Hosts with different information classifications that reside on the same network segment may be segregated as a compensating control; and
- Hosts that must regularly communicate with a peer in another Zone (e.g., one located within a DMZ in an Access Zone) may be segregated from other hosts as a compensating control.

The use of virtual segregation for networking or processing (e.g., virtual networking, virtual servers, etc. and all similar functionality) **must** be deployed as per GO-ITS 25.0 General Security Requirements.

2.6.2. Network Address Translation (NAT)

One common technique for segregating networks and creating a boundary is Network Address Translation (NAT). This is where the IP address of a source host is changed to a different address (usually an address that cannot route back to the source network without being translated back to the original address).

- NAT techniques should be applied to inbound connections from the Internet to any Government of Ontario host behind a firewall, where possible and where benefit exists; and
- NAT should translate public (Internet routable addresses) to private (internally routable addresses as per RFC 1918) at any Internet gateway where possible.

2.6.3. Port Address Translation (PAT)

Port Address Translation allows an inbound network port to be changed to another port while the traffic itself remains unchanged.

PAT is useful in cases where the same port and protocol traverses multiple Zones since this implies that the same application exists in multiple Zones. For example, if a web server, application server and database were all managed through web interfaces, there would be a web service available in all three Zones. A technical vulnerability within the Presentation Zone web server on such a network could in turn lead to a compromise of all three Zones. By using PAT, each web server could run on a distinct port, potentially mitigating the risk of HTTP-based attacks.

2.6.4. Virtual networking

Virtual network feature sets, such as VLANs and VACLs on ethernet switches, provide a logical means to separate networks and restrict ports on layer-two devices.

VLANs **must** be used in conjunction with firewalls to provide reliable Zone segregation, and in critical environments (i.e., a Security Zone) that require isolation.

2.6.5. Intrusion detection and prevention

Security techniques in the Government of Ontario include the use of Intrusion Detection and/or Prevention Systems, monitoring systems, controls against malware, and auditing.

The Cyber Security Branch is responsible for the implementation, tuning, and monitoring of Intrusion Detection and/or Prevention Systems. The following guidance is provided for IDS/IPS design and operation:

- IDS/IPS **must** exist on an inbound or outbound connection to an unmanaged network (i.e., within an Access Zone that provides access to other Zones);
- IDS/IPS **must** exist for connections to Extranet Zones;
- IDS/IPS should be in place where High Sensitivity information is stored, or traverses a Zone;
- IDS/IPS should be in place at boundaries between Zones where unencrypted traffic flows; and
- IDS/IPS **must** be in place where any VPN connection terminates, or where other types of encrypted sessions terminate and merit inspection (e.g., based on a TRA recommendation).

3. RESPONSIBILITIES

Users

All Government of Ontario employees and staff using I&IT resources are responsible for:

- Complying with directives, policies and agreements when accessing or using Government of Ontario information, equipment and services;
- Understanding information sensitivity and their duty to protective sensitive information as per the ISPC policy and operating procedures;
- Ensuring the security of assigned system accounts and credentials; and
- Reporting any suspected security breaches to the IT Service Desk.

Program managers and project teams

Program managers and project teams are responsible for:

- Ensuring compliance with the requirements in this document;
- Ensuring required security safeguards are in place to protect I&IT assets, including additional safeguards recommended and approved via the PIA and TRA processes;
- Designing services and/or applications in a manner that complies with the Zone requirements described in this document;
- Using the security safeguard information presented in this document as input to program design considerations; and
- Reporting any security exposures or suspected security incidents to the IT Service Desk.

Directors

Directors are responsible for:

- Ensuring that staff members are aware of and adequately trained in their responsibilities as set out in this document;
- Supporting efforts to ensure that security safeguards are deployed to protect Government of Ontario information; and
- Reporting any security exposures or suspected security incidents to the IT Service Desk.

I&IT Clusters

The I&IT Clusters are responsible for:

- Supporting Program Managers and Directors in ensuring that Government information is protected by appropriate security safeguards, and in accordance with both the I&IT Security Directive and ISPC requirements;
- Providing users with instruction and support;
- Ensuring that agreements with service providers address security requirements; and
- Monitoring for compliance with this document.

Infrastructure Technology Services (ITS)

ITS is responsible for:

- Ensuring that agreements that they enter into with service providers will reflect the requirements in this document;
- Operating hosting or other services in a manner that complies with Zone requirements;
- Locating hosted customer equipment and/or applications in a manner that complies with Zone requirements;
- Using the security safeguard information presented in this document to inform network, system, and application design;
- Ensuring that the design of networks, systems, and applications adhere to the security requirements presented in this document;
- Monitoring any services provided for compliance with the requirements in this document;
- Operation of the IT Service Desk, and provision of assistance to clients; and
- Reporting security incidents to the I&IT Strategy and Cyber Security Division.

Network Service Provider

The Network Service Provided is responsible for:

- Operating any provided services in a manner that complies with Zone requirements;
- Using the security safeguard information presented in this document to inform network, system, and application design;
- Ensuring that the design of networks, systems, and applications adhere to the security requirements presented in this document; and
- Ensuring that the logging requirements described in this document and GO-ITS 25.0 are met for managed systems, with all logs maintained in a secure fashion, retained as required, and made available when requested.

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

The I&IT Strategy and Security Division, or a successor division/branch, is responsible for:

- Authorship of security policies and standards for the Government of Ontario, subject to any required approval;
- Providing timely guidance on the deployment and use of security products and services to OCCIO ITS and the I&IT Clusters;
- Updating this document and ensuring that Security Design advice and/or requirements are kept current;
- Assisting in monitoring compliance with security requirements and obligations in conjunction with OCCIO ITS, Network Service Providers, and the I&IT Clusters;
- Maintaining IDS/IPS infrastructure and related capabilities in collaboration with ITS and the Network Service Provider;

- Liaising with security authorities at other levels of Government; and
- Managing security incidents.

Ontario Internal Audit

The Ontario Internal Audit Division is responsible for:

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

4. ACKNOWLEDGEMENTS

4.1 Editors

Full Name	Cluster, Ministry and/or Area
Tim Dafoe	I&IT Strategy & Cyber Security Division

4.2 Contributors

Full Name	Cluster, Ministry and/or Area
Mano Pancharatnam	MGS Corporate Security Branch
Charlotte Ward	MGS Corporate Security Branch

4.3 Consultations

The following individuals were consulted:

Charlotte Ward	MGS Corporate Security Branch
Rob Charuk	OCCIO ITS
Dale Tasker	OCCIO ITS
Hans Wagner	OCCIO ITS
John Ostler	OCCIO ITS
Serguei Doubov	OCCIO ITS
Bill Zeng	MGS Corporate Security Branch
Gilles Fourchet	Children, Youth and Social Services I&IT Cluster
Francois Van Heerden	Children, Youth and Social Services I&IT Cluster
Tony Condello	Children, Youth and Social Services I&IT Cluster
Kit-Mei Chan	Transportation I&IT Cluster
Brady Thompson	OCIPO
Brian Bisaillon	OCIPO

Peter Churchard	OCCTO CAB
Robert Rowntree	Ministry of Health
Terry Danyleyko	Government Services Delivery Cluster

4.4 Reviewers

The following groups have reviewed this standard:

MTO Security/Architecture Staff	Cluster Security Officers Group (Dissolved)
CSC Security/Architecture Staff	Security Architecture Working Group
HSC Security/Architecture Staff	LRC Enterprise Architecture
Ministry of Finance Service Delivery / Strategy	SDLC
.NET COE	

5. APPENDIX A: DEFINITIONS

Access: The ability to enter a physical area or use a resource, which may include viewing, adding, modifying or deleting data, and/or executing applications (running computer programs).

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 stored data (logical access controls).

Authenticate: To establish confidence in the reliability of an assertion (e.g., use of passwords, access cards, or other credentials), and verify the claimed identity of a user prior to granting access.

Authentication: A process of testing assertions to establish a level of confidence (assurance) in their reliability as an indication of identity.

Authorization: The procedural and technical allowance of specific privileges and access.

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 other information, made authentic when digitally signed with the private key of the CA that issued it. Certificate formats are described within the X.509 and RFC 2459 specifications.

Confidentiality: Ensuring that information is accessible only to those authorized to have access. Unauthorized disclosure of the information constitutes a loss of confidentiality. The protection of confidentiality must be consistent with the sensitivity of information and legislative requirements (e.g., FIPPA, PHIPA).

Cryptography: The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, detect unauthorized modification, or prevent its unauthorized use. Cryptography is commonly used to provide confidentiality, integrity, message authentication, identity authentication and digital signatures.

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

Digital signature: A cryptographic technique based on a uniquely related pair of keys where one key is used to create a signature (the private signing key) and the other to check the signature (the public verification key). A digital signature enables the recipient to verify the source (e.g., the signer) of a message or document and confirm its integrity.

Encryption: The transformation of data via cryptography into a form unreadable by anyone not in possession of the required key. It can provide for data confidentiality by keeping the information hidden from any individual or entity for which it was not intended.

Fire Account: A privileged emergency account for a computer system; credentials are recorded and kept secure unless required for emergency maintenance, shutdown, or other duties.

Hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Common names for the output of a hash function include *hash value, hash, message digest and digital fingerprint*. Approved hash functions satisfy the following properties:

- One-way: it is computationally unfeasible to find any input that maps to any pre-specified output, and
- Collision resistant: it is computationally unfeasible to find any two distinct inputs that map to the same output.

Identifier: A bit string that is associated with a person, device or organization. It may be an identifying name, or may be something more abstract (for example, a string consisting of an IP address and timestamp), depending on the application.

Identity: Attributes of an individual determining who the individual is as a unique entity.

Identity authentication: A process that uses a credential(s) to verify the identity of a user who is attempting to access resources and/or services.

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

Information technology assets: 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 property that information has not been modified or deleted in an unauthorized and undetected manner.

Malware: Software and/or program code/instructions inserted into a system, usually covertly, with the intention of compromising one or more of confidentiality, integrity, or availability associated with the system or the data it processes. This includes traditional “virus”, “trojan”, and “worm” software as well as “sniffer”, “logger”, “backdoor”, “trapdoor”, and “rootkit” threats.

Network attached storage (NAS): A server specifically designed for handling files (rather than block data). Network-attached storage is accessible directly on the local area network (LAN) through LAN protocols such as TCP/IP. This is as opposed to storage that is internal to or directly connected to a server (e.g., via parallel SCSI cables) and only accessible from that server.

Password: A string of characters (letters, numbers and other symbols) that are used to authenticate an identity or to verify access authorization.

Pass phrase: A lengthy string of characters intended to provide for significantly increased complexity compared to traditional passwords, in a format users can readily recall from memory.

Privacy: The ability of an individual or group to control personal information and prevent it from being used by people or for purposes other than those they consented to when they provided the information. Organizations must have controls to restrict the collection, use and/or disclosure of personal information to that authorized by the individual or group. In the case of Government organizations, legislative authority is required to collect and use the personal information needed for the delivery of a specific program or service.

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: An estimation of the likelihood and impact of potential events on an organization’s ability to meet its business objectives.

Safeguard: A protective and precautionary measure intended to prevent a threat agent from reducing security or causing harm.

Security: The effort to create managed environments within which agents can only perform authorized actions and gain prescribed access, once appropriately authenticated.

Security Zone: A controlled, managed environment that employs strong physical and logical access controls. Network components must be housed within a single data centre and reliably separated from other parts of the Government of Ontario network by approved network and access controls.

Storage area network (SAN): A specialized network that provides access to high performance and highly available storage subsystems using block storage protocols. The main characteristic of a SAN is that the storage subsystems are generally available to multiple hosts at the same time, which makes them scalable and flexible.

Security Testing and Evaluation (STE): Any collection of processes or assessment models whereby the functional capabilities and security assurance of a given safeguard or system is examined (e.g., vulnerability assessment, penetration testing, code review). STE can be conducted according to formal methodologies, or performed informally for a basic degree of validation (e.g., the security portion of a generic acceptance testing procedure). In the case of physical facilities, STE activities may include audits of physical design, facility construction, access control systems, and compliance with minimum standards.

Threat risk assessment (TRA): A tool to assist Program Managers in fulfilling their responsibilities for security risk management and the development of security plans. A Threat Risk Assessment (TRA) is used to:

- Assess the sensitivity of program assets and information;
- Identify and analyse potential threats and vulnerabilities;
- Assess the level of risk taking into consideration the effectiveness of current security measures; and
- Recommend appropriate measures to protect assets and information from loss, theft, destruction, modification, or misuse.

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

6. APPENDIX B: ACRONYMS

The following abbreviations and acronyms are used in this standard:

BIA: Business Impact Assessment
HMAC: Keyed-Hash Message Authentication Code (specified in FIPS 198)
IDS: Intrusion Detection System
IEC: International Electrotechnical Commission
IPS: Intrusion Prevention System
ISO: International Organization for Standardization
ISPC: Government of Ontario Information Security and Privacy Classification Policy
ITS: Infrastructure Technology Services
MAC: Message Authentication Code
MGS: Ministry of Government Services
OPS: Ontario Public Service (the employees of the Government of Ontario)
PIA: Privacy Impact Assessment
PKI: Public Key Infrastructure
PSTN: Public Switched Telephone Network
RFC: Request for Comments
SAN: Storage Area Network
SCS: I&IT Strategy & Cyber Security Division
STE: Security Testing and Evaluation
TBS: Treasury Board Secretariat
TRA: Threat Risk Assessment
VACL: Virtual Access Control List
VLAN: Virtual Local Area Network
VPN: Virtual Private Network

7. APPENDIX C: 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).
☐	Information Standard – specifications for a data format (e.g. XML schema, metadata, and/or related data models)
☐	Technical Standard - networking and communications specifications, protocols, interfaces (API's) (e.g., standards adopted from recognized standards development organizations such as W3C, OASIS or IETF such as TCP/IP, XML, SOAP, etc.)
☐	Architecture Standard – application patterns, architecture and standards principles governing the design and technology decisions for the development of major enterprise applications
☐	Product Standard – an enterprise-wide product which is mandatory for use such as a single corporate-wide application, which all ministries and agencies use to record and access their HR information.

Publication

Please indicate if this standard should be restricted to publishing on the Internal (Intranet) IT Standards web site or whether it is intended for publishing on the public (Internet) Government of Ontario IT Standards web site.

Check One	Publish as Internal or External
☐	Internal Standard
☑	External Standard

Consultation

Check	Area	Date: (month/year)
☑	Architecture Review Board	Dec. 2014
☐	Strategy, Policy and Planning Branch, ICS	
☑	Controllership Branch, (Corporate Architecture) ICS	
☑	Corporate Security Branch (Cyber Security Branch)	
☑	Information Privacy and Archives	
☐	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)	
☐	Infrastructure Consolidation projects: - Enterprise Email Services - Servers and Data Centres - Desktop Management - Service Management	
☑	SDLC	

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 25.0	Other GO-ITS 25 documents supplement this document (with references throughout), and many concepts are in practice today – GDC project also intends to align with the deployment model described	Comply with GO-ITS requirements

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)
All	Adherence to these security requirements will reduce the risks to Government I&IT resources.	Compliance with these requirements.
All	Implementation of these security requirements will produce impact due to additional complexity and/or increases to the security of service design.	Compliance with these requirements.
All	Implementation of the Zone model will impact corporate architecture.	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 Standards:

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

ISO/IEC Standards:

http://www.iso.org

CSE ITSG-22

http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-eng.pdf

Document History

February 9th, 2010: Final draft for presentation at IT Standards Council (ITSC)

April 7th, 2010: Revised based on ITSC feedback following Feb. 17th, 2010 meeting

- Zone model revised, some Zones renamed
- DMZ alignment changed according to ITS feedback
- Requirements updated according to feedback from OCCTO, MTO

August 9th, 2010:

- Further revisions based on CAB, SDLC, .NET COE, and other ITSC member feedback.

September 23rd, 2010:

- Further revisions based on CAB, GSDC, ITS, ETC, and OCIPO feedback.

October 13th, 2010:

- Further revisions based on OCIPO feedback and CSB adjustments.

October 22nd, 2010:

- Standard endorsed by ITSC.

March 14th, 2012:

- Organizational updates
- Updated hyperlinks and references
- Minor adjustments and errata

March 19th, 2012:

- Document aligned with merging of GO-ITS 25.19 and GO-ITS 25.0

June 12th, 2012:

- Consultation list updated

November 15th, 2012:

- Minor updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 1.1

January 19th, 2015:

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

March 6th, 2015:

- Minor updates as per ARB feedback.

Version 1.2

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

Copyright & Disclaimer