Ontario

Government of Ontario

Government of Ontario IT Standard (GO-ITS)

Number 25.18

Physical Security Requirements for Data Centres

Version #: 1.1

Status: Approved

Prepared under the delegated authority of the Management Board of Cabinet

UNCLASSIFIED

© Queen's Printer for Ontario, 2012

Last Review Date: 2012-11-15

Foreword

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

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

Copies of cited standards may be obtained as follows:

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

Internet: http://www.ontario.ca/itstandards/

Summary

The Corporate Policy on Information and Information Technology Security requires that Government 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.

Government of Ontario I&IT operations rely upon data centre facilities for both the provision of service and the security of a managed environment. This document describes the minimum physical requirements for data centre design, construction, and operation to ensure that I&IT assets are appropriately safeguarded.

Version control and change management

Date	Version	Author	Comment
May 8, 2009	1.0	MGS CSB	Editor: Tim Dafoe, CSB
March 12, 2012		Tim Dafoe	General update as per Document History section
November 15, 2012	1.1	Tim Dafoe	Updates approved by Information Technology Executive Leadership Council (ITELC). Approved document version number set to 1.1

Ongoing ownership and responsibility for maintenance and evolution of this document resides with the Corporate Security Branch, Office of the Corporate Chief Information Officer. The Corporate Security Branch will provide advice on the interpretation and application of these security requirements and manage any updates to the document when the need arises.

Contact Information

If you have questions or require further information about this document or the GO-ITS 25 series, please contact the following Corporate Security Branch staff:

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

Table of Contents

1. INTRODUCTION 5
2. REQUIREMENTS 8
2.1. Threat/Risk Assessment (TRA) 8
2.2. Data separation 9
2.3. Zones 9
2.3.1. Public zone 9
2.3.2. Reception zone 9
2.3.3. Operations zone 10
2.3.4. Security zone 10
2.3.5. High security zone 11
2.3.6. Defence in depth requirements 11
2.3.7. Zone control matrix 12
2.4. Constructing new facilities 13
2.5. Leased facilities 13
2.6. Building and fire code compliance 14
2.7. Vendor contracts 14
2.8. Facility site and management 15
2.8.1. Facility location 15
2.8.2. Landscaping 15
2.9. Facility construction 16
2.9.1. Utilities 16
2.9.2. Lighting 16
2.9.3. Roof access 18
2.9.4. Ceilings 18
2.9.5. Windows 19
2.9.6. Doors 19
2.9.7. Fire protection 22
2.9.8. Raised floors 23
2.9.9. Loading docks and receiving 23
2.9.10. Elevators 24
2.9.11. Circulation routes 24
2.9.12. Stairwells 25
2.9.13. Floor loading capacity 25
2.10. Physical access control 26
2.10.1. Perimeter safeguards 26
2.10.2. Guard services 26
2.10.3. Personnel screening 27
2.10.4. Physical access control 27
2.10.5. Identification cards 27
2.10.6. Visitor access 28
2.10.7. Contractor access 29
2.10.8. Electronic access control 29
2.11. Exit routes 30
2.12. Intrusion detection 31
2.13. Server rooms 32
2.14. Cross-over floors 33
2.15. Emergency electrical power 34
2.16. Staff and visitor parking 34
2.17. Maintenance and cleaning services 35
2.18. Garbage removal and recycling 36
3. RESPONSIBILITIES 37
4. ACKNOWLEDGEMENTS 40
5. DEFINITIONS 42
6. APPENDIX A: ADDITIONAL INFORMATION 44

1. INTRODUCTION

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

1.1. Purpose of the standard

This document describes minimum security requirements for the physical design, construction, and operation of data centres for the Government of Ontario. The objective of this document is to ensure that data centre facilities housing Government of Ontario I&IT resources will offer a degree of security adequate to both safeguard sensitive information and support availability requirements.

This document has been produced in consultation with stakeholder groups within the Government of Ontario and the Office of the Ontario Fire Marshall. It has been developed with reference to section 9 (*Physical and environmental security*) from the ISO/IEC 27002:2005 code of practice, in addition to the following documents:

- *Operational Security Standard on Physical Security*, Treasury Board of Canada Secretariat (2004)
- *G1-017 Hardware*, Royal Canadian Mounted Police (1985)
- *G1-018 Doors and Frames,* Royal Canadian Mounted Police (1985)
- *G1-026 Guide to the Application of Physical Security Zones*, Royal Canadian Mounted Police (2005)
- *G1-031 Physical Protection of Computer Servers*, Royal Canadian Mounted Police (2008)

Technical requirements in this document are stated in accordance with ISO/IEC 27002:2005 recommendations, existing GO-ITS 25 standards, and external guidance received by CSB. If access to any of the above documents is required, please consult CSB for assistance.

1.2. 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.

1.3. Application and scope

The GO-ITS 25.18 Physical Security Requirements for Data Centres **must** be understood to apply to:

- All ministries of the Ontario Government;
- Any organization that uses ministry or I&IT Cluster information technology infrastructure; and
- Any third party individuals or organizations that connect to the Government of Ontario integrated network for business purposes, unless exempted in a Memorandum of Understanding.

The intended scope includes managed facilities intended for I&IT asset storage and operation that are:

- Primarily intended to provide for managed environmental conditions and a secure, central operating environment for computer equipment and servers;
- Owned, rented, or leased by the Government of Ontario; and
- Owned, rented, or leased by a third party vendor, including but not limited to outsourcing agreements that result in routine business operations at a central facility, specific project infrastructure, or Disaster Recovery / Business Continuity services with a third party facility component.

As new GO-ITS standards are approved, they are deemed mandatory for all project development and procurement opportunities. When implementing or adopting any GO-ITS standard or GO-ITS standard update, ministries and I&IT Cluster **must** follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management and risk mitigation mechanisms are employed.

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

Use of this standard **must** be accompanied by Threat/Risk Assessment (TRA) activities, to address variations in information sensitivity, identify significant vulnerabilities, determine required additional safeguards, and document risk.

Disaster Recovery (DR) and Business Continuity Planning (BCP) are not within the intended scope of this document. References to DR/BCP activities are intended to provide context when describing data centres operated on behalf of the Government of Ontario, or highlight items which may relate to such planning. It is recommended that alternate guidance be consulted for these items. For more information, please contact the MGS Corporate Security Branch.

For the purpose of this document all references to “information” refer to digital information

[1] Sensitive information as defined per Information Security and Privacy Classification (ISPC) policy (http://intra.ops.myops.gov.on.ca/cms/tiles.nsf/(vwReadResourcesByRefId_Content)/cpd2008.08.18.14.34.52.PSU_res/$File/InformationSecurity&PrivacyClassificationPolicy-Aug05.pdf).

and data.

The MGS Corporate Security Branch should be contacted if application of this standard is not clear relative to a given environment.

1.4. Background

Data centres operated or leased by, or operated on behalf of, the Government of Ontario **must** employ minimum physical safeguards to protect sensitive information. This standard describes the minimum requirements for such facilities.

1.5. Principles

The following guiding principles support, and are stated in accordance with, the Management and Use of Information & Information Technology Directive, the Corporate Policy on Information and Information Technology Security, the ISPC policy, external physical security guidance, ISO/IEC 27002:2005, and GO-ITS 25 series security standards:

- Data centre facilities are intended to provide a secure perimeter for operations, control access to equipment and data, protect against environmental threats, and support the availability requirements of Government business.
- Facilities included within the scope of this document **must** meet the physical security requirements described in this standard.
- Threat/Risk Assessment (TRA) and Security Testing and Evaluation (STE) **must** be used to document the provision of adequate, effective safeguards for all data centre facilities, and demonstrate that identified safeguards are appropriate relative to data sensitivity.
- Any requirements for the use of enhanced safeguards (e.g., as per TRA recommendations and/or the determination that a given facility is associated with an elevated degree of risk) **must** be identified for data centres.
- Readiness (or lack of readiness) for a specific data center, in terms of the ability to store or process sensitive information, **must** be disclosed to client groups that require services prior to any contract for services or service level agreement (SLA).
- The design, construction, and management of data centres **must** be sufficient to permit for secure operation (as expressed in terms of accountability, confidentiality, integrity, availability, and opportunity for audit).
- Data centre staff **must** report all security related events or incidents (as per the roles and responsibilities section of this document) that occur within any facility (e.g., be it leased or owned).

REQUIREMENTS

The following security requirements apply to data centres operated or leased by, or operated on behalf of, the Government of Ontario:

2.1. Threat/Risk Assessment (TRA)

Existing data centre facilities, and those being acquired by lease, purchase, or construction, **must** be subject to a Threat/Risk Assessment (TRA) and Security Testing and Evaluation (STE).

Site architectural drawings and facility operations documents **must** be assessed in any TRA performed, and **must** be included in the acquisition of any data centre facility. These documents form the basis of facility physical security requirements.

A conceptual TRA is valuable once the requirement for a data centre has been identified. A logical TRA will assist in the design and specification of new facilities, once a location has been selected. A physical TRA should be performed for existing (or leased) facilities, and upon construction of new data centres.

Government of Ontario data centre facilities are likely to incur some degree of risk by virtue of their operations. Existing data centres **must** have a new TRA completed when there has been a significant change in a business function (e.g., a change which results in storage or processing or sensitive information), modifications that increase the time critical status of the facility for any reason, or modifications to the facility itself or the environment surrounding it.

Some data centre facilities may require enhanced safeguards if operating risk is to be appropriately mitigated. The following are examples of conditions that would indicate that a given data centre facility requires enhanced safeguards:

- The facility is critical to Government of Ontario I&IT strategy in the sense that continuity of broader operations will rely on the availability of the data centre;
- The facility is or will become part of a documented high availability strategy;
- The degree of information sensitivity or the requirement for integrity assurance associated with processing at an existing facility is intended to markedly increase;
- A TRA has indicated that an elevated degree of risk exists regarding a facility;
- A TRA has indicated that safeguard effectiveness must be increased for a given data centre, due to operational considerations or physical location;
- The facility will support the operation of a high security zone, or is expected to provide for such capacity in the future; and/or
- An existing facility lacks safeguards in a manner that will inherently increase the risk associated with ongoing operations.

The list above is not exhaustive, but provides criteria for determining when a data centre facility should be designed to support and/or operated with enhanced safeguards. These safeguards will typically offer an increased level of effectiveness, and thereby meet requirements for a more robust facility security posture.

Enhanced safeguards can sometimes be applied to a specific security zone.

Any such required additional physical security safeguards **must** be documented via the TRA process. A TRA may recommend safeguards that exceed those described in this document.

2.2. Data separation

To facilitate access control, data centre facilities must be separated into distinct areas depending on operational requirements (e.g., server rooms, wiring closets, call centres, system support areas, service delivery, receiving).

Separating these areas permits for the allowance of access to information and equipment based on authorization and job function, and assists in implementing the segregation of duty principle described in GO-ITS 25.0 General Security Requirements.

Each area separated due to operational function must be assigned to a zone to assist in determining minimum physical safeguards and access control requirements.

2.3. Zones

Data centre managers **must** use a zone model to apply safeguards to areas within the data centre facility, and protect sensitive information as identified by ISPC policy or per TRA recommendations.

The use of zones permits for modular separation of facility areas via physical barriers and other access control methods, permits for greater variation in access levels, and provides for defence in depth. Data centre safeguard requirements in this document are based on the following five zones:

- Public Zone
- Reception Zone
- Operations Zone
- Security Zone
- High Security Zone

A TRA **must** identify existing and required safeguards associated with each zone in the data centre facility.

2.3.1. Public zone

Any public entrance to a physical facility and the immediate environment around it is considered a public zone. It is not always possible to manage these environments directly.

A public zone may include:

- Facility parking lots;
- Grounds surrounding a facility;
- Public corridors or concourses;
- Elevator lobbies in most shared facilities; and
- Any areas of unimpeded public access during posted business hours.

2.3.2. Reception zone

A reception zone is an area where public access intersects with facility staff or operations for administrative reasons or to obtain access.

Typical reception zone areas include:

- Main entrance of a facility or a floor in shared accommodation situations;
- Visitor receiving and waiting areas; and
- Public service desks and kiosks.

Every facility should have a reception zone accessible directly from the public zone that must be traversed to obtain service, be granted facility access, or obtain an escort to proceed to another zone.

The following are mandatory security requirements for a reception zone:

- Access control **must** be in place to restrict further public movement;
- Public/visitor access to the reception zone **must** be limited to specific hours;
- Any required authentication and approval for facility access (e.g., presentation of credentials or validation of authorized access) should take place within the reception zone; and
- Only authorized staff and approved visitors should be granted access to areas beyond the reception zone, with monitoring and logging in place to track such access.

2.3.3. Operations zone

An operations zone is a periodically or informally monitored area within the facility where access is limited to authorized personnel and approved/escorted visitors only. Corridors, storage closets, employee offices, and similar areas are appropriate for inclusion within an operations zone.

The following are mandatory requirements for an operations zone:

- **Must** have a recognizable perimeter;
- **Must** not permit for public access, and employ barriers for this purpose;
- **Must** employ some degree of activity monitoring; and
- **Must** only be accessible via a reception zone, and separated from the reception zone by a wall and locking door (subject to possible exemption as per section 2.3.6. of this document).

2.3.4. Security zone

A security zone is an area within the facility that is monitored continuously, and is accessible to authorized personnel and approved/escorted visitors only. **The secure raised floor portion of a data centre is appropriate for inclusion within a security zone.** Other areas of a facility (e.g., sensitive communications or wiring closets) may also be defined as security zones.

The following are mandatory requirements for a security zone:

- **Must** have a recognizable perimeter;
- **Must** employ robust, reliable high-effectiveness physical barriers to access;
- **Must** be constructed such that all barriers and doors remain continuously closed and locked when not in use;
- **Must** employ activity monitoring with immediate response;
- Access **must** be controlled and recorded at all times; and
- **Must** be located within an operations zone (subject to the possible exemption as per section 2.3.6. of this document).

2.3.5. High security zone

A high security zone is an area within the facility that is monitored continuously, and is accessible only to a specific list of screened[2] and authorized personnel, or approved/escorted visitors accompanied by screened and authorized personnel. A dedicated, sensitive processing environment that must be physically separated from raised floor operations is appropriate for inclusion within a high security zone. Some high security zones may require dual-custody access.

The following are mandatory requirements for a high security zone:

- **Must** have a recognizable perimeter;
- **Must** employ robust, reliable high-effectiveness physical barriers to access;
- **Must** be constructed such that all barriers and doors remain continuously closed and locked when not in use;
- **Must** employ continuous activity monitoring with immediate response;
- All access **must** be continuously controlled, recorded and audited;
- Individuals who require access **must** successfully undergo personnel screening and be added to any list or roster of approved personnel prior to being granted access;
- All approved visitors **must** be accompanied at all times by a screened and authorized individual; and
- **Must** be located within a security zone (subject to possible exemption as per section 2.3.6. of this document).

2.3.6. Defence in depth requirements

Zones should be physically layered to provide for defence in depth protection. It may occur that, given the layout of a particular environment, or given specific operational requirements, such an approach will not be feasible in all instances.

In such cases, the maximum number of zones that may be skipped in the design of a data centre environment **must** be limited to one (1). In such cases, the relevant TRA **must** reflect the skipped zone, and compensating controls **must** be investigated.

[2] This refers to a Government of Ontario personnel security screening result or other formal security clearance that has been deemed appropriate for the environment.

2.3.7. Zone control matrix

The following matrix provides an overview of controls required for each zone for a basic level of operating risk (e.g., for environments that do not require enhanced safeguards):

Functionality and Safeguards	Public Zone	Reception Zone	Operations Zone	Security Zone	High Security Zone
Access Control (Design/Layout)	**N/A**	**NO**	**YES**	**YES**	**YES**
Approved Staff Only (Basic)	**N/A**	**NO**	**YES**	**YES**	**YES**
Approved Staff Only (Limited/List)	**N/A**	**NO**	**NO**	**CONSIDER**	**YES**
Barriers (Basic)	**YES**	**YES**	**YES**	**NO**	**NO**
Barriers (Robust)	**CONSIDER**	**NO**	**NO**	**YES**	**YES**
Contractors (Open)	**N/A**	**YES**	**YES**	**YES**	**NO**
Contractors (Escorted)	**N/A**	**NO**	**NO**	**CONSIDER**	**YES**
Cross-Over Floors	**N/A**	**YES**	**YES**	**NO**	**NO**
Dual Custody Access	**N/A**	**NO**	**NO**	**NO**	**CONSIDER**
Electronic Access Controls	**N/A**	**CONSIDER**	**YES**	**YES**	**YES**
Exterior Entrances	**YES**	**YES**	**AVOID**	**NO**	**NO**
Fire Detection Under Floors	**N/A**	**NO**	**NO**	**YES**	**YES**
Garbage Bins (Large/Outdoor)	**YES**	**NO**	**NO**	**NO**	**NO**
Glass/Glazed Doors	**N/A**	**YES**	**AVOID**	**NO**	**NO**
Locked Door Environment	**N/A**	**NO**	**CONSIDER**	**YES**	**YES**
Lighting	**YES**	**YES**	**YES**	**YES**	**YES**
Lobby/Greeting Area	**YES**	**YES**	**AVOID**	**NO**	**NO**
Maintenance Staff (Open)	**N/A**	**YES**	**YES**	**YES**	**NO**
Maintenance Staff (Escorted)	**N/A**	**NO**	**NO**	**CONSIDER**	**YES**
Monitoring (Basic)	**YES**	**YES**	**YES**	**NO**	**NO**
Monitoring (Continuous)	**N/A**	**CONSIDER**	**CONSIDER**	**YES**	**YES**
Monitoring (Audited)	**N/A**	**NO**	**NO**	**CONSIDER**	**YES**
Parking Areas/Access	**YES**	**NO**	**NO**	**NO**	**NO**
Public Access (Open)	**YES**	**YES**	**NO**	**NO**	**NO**
Public Access (Limited/Escorted)	**N/A**	**CONSIDER**	**YES**	**YES**	**YES**
Raised Floor Server Environment	**N/A**	**NO**	**NO**	**YES**	**YES**
Recognizable Perimeter	**N/A**	**CONSIDER**	**YES**	**YES**	**YES**
Recycled Paper Storage	**NO**	**NO**	**YES**	**NO**	**NO**
Roof Hatch	**N/A**	**YES**	**YES**	**YES**	**NO**
Secure Doors/Locksets	**N/A**	**YES**	**CONSIDER**	**YES**	**YES**
Slab to Slab Walls	**N/A**	**YES**	**CONSIDER**	**YES**	**YES**
Small Server Rooms	**N/A**	**NO**	**YES**	**YES**	**NO**
Two-Factor Authentication	**N/A**	**NO**	**NO**	**CONSIDER**	**YES**
Visible ID Required	**N/A**	**YES**	**YES**	**YES**	**YES**
Visitors Escorted	**N/A**	**NO**	**NO**	**YES**	**YES**
Visitors Reception	**N/A**	**YES**	**NO**	**NO**	**NO**
Windows/Glazing Permissible	**N/A**	**YES**	**YES**	**NO**	**NO**

2.4. Constructing new facilities

Once a location has been selected, a facility that will be constructed for use as a Government of Ontario data centre **must** have a logical TRA completed, based on the intended building architecture and anticipated operational requirements. The results of this TRA should in turn inform the following:

- Physical location, design, and materials for walls, doors, and windows (except for those specifications indicated as mandatory within this document or by regulatory requirement);
- Requirements for ceiling and floor construction for the zones within the facility;
- Requirements for enhanced safeguards;
- Installation, and required degree of efficacy of, access control systems;
- Lighting requirements;
- Robustness and effectiveness of door hardware and locking devices;
- Power supply and utility system requirements;
- Security zone requirements, particularly where security zones will influence the physical layout of the facility, and in instances where a high security zone must be constructed;
- Specifications and requirements for physical key management systems (e.g., a requirement for high security physical keys and locksets); and
- Required facility standoff distance from public easements, with a minimum 10 metre standoff requirement for all new facilities (45 metres for facilities that require enhanced safeguards).

Once a logical TRA has been completed, responsibilities **must** be determined to ensure the implementation of physical security safeguards.

General responsibility for the facility may rest with the Government of Ontario, the facility owner, or a facility management company. Accountability for Government I&IT assets always lies with the Government of Ontario.

2.5. Leased facilities

Prior to leasing an existing facility for data centre use, a physical TRA and required STE **must** be completed to determine if additional physical safeguards are required. Any gaps in physical security requirements **must** be addressed prior to production use of the facility. This requirement holds special significance in instances where a leased data centre will reside in a multi-tenant location, as exterior building security and access control systems may not be directly managed by the Government of Ontario.

Data centre management may accept and assume accountability for some degrees of risk as documented by a relevant TRA (e.g., when additional safeguards have been recommended). In such instances, however, the mandatory safeguards in this standard **must** still be met, and any accepted risk **must** be communicated to facility clients.

Lease agreements **must** address required physical security safeguards required as described in this document and/or determined by a relevant TRA.

Lease agreements **must** also address the following:

- Any additional safeguards required, and the party accountable for the costs;
- Tenant permissions to restrict owner access during specified times or by zone;
- Requirements for entry (e.g., personnel screening, authorization);
- Cleaning services provided for the facility;
- Tenant permission for the installation of locksets and/or doors;
- Tenant permission for the re-keying of locks if locksets cannot be replaced;
- Tenant permission for the installation of electronic access control and/or monitoring controls (e.g., card access, proximity sensors, biometrics, CCTV, lighting, window protection, alarm sensors);
- Connection of data centre fire systems to building controls (including access control);
- Ensuring life safety and access control devices receive emergency power; and
- Ensuring the integrity of all safeguards when physically inaccessible or when main power has been interrupted.

Future developments or changes to a facility should be determined and included in the lease agreement. This includes potential new tenants that may occupy a shared facility and any security restrictions required.

2.6. Building and fire code compliance

The *Ontario Building Code* is applicable to new construction, renovations and alterations for all data centres. All alterations to facilities **must** comply with the Ontario Building Code.

The *Ontario Fire Code* is applicable to existing buildings and covers a wide range of issues including but not limited to:

- Maintenance of exit facilities including door hardware [Subsection 2.7.2. in Division B, *Ontario Fire Code*];
- Maintenance and testing of fire protection/suppression equipment [Part 6 in Division B, *Ontario Fire Code*] and;
- Fire department access to buildings [Section 2.5 in Division B, *Ontario Fire Code*];

All alterations to facilities **must** comply with the Ontario Fire Code. These regulations apply to fire and life safety provisions that are directly associated with both access control systems and facility operations.

Proposed security safeguards **must** not be given priority over fire and building code requirements should any conflict arise between these requirements. Any such conflicts should be resolved with deference to life safety, and documented in a relevant TRA.

Ontario Building and Fire Codes do not presently contain requirements for the testing of electronic access devices. It is important to validate the functionality and correct operation of electronic access controls (e.g., magnetic locking mechanisms) prior to production use of these systems. Such testing **must** be carried out for all Government of Ontario data centre facilities, despite the lack of a code requirement to do so.

2.7. Vendor contracts

All vendor operated facilities housing a Government of Ontario data centre should meet the

general physical security principles described within this standard. Security requirements **must** be included in any related request for proposals in addition to vendor contracts.

2.8. Facility site and management

Appropriate selection of the facility site, and management of the data centre, is critical if I&IT assets are to be protected. Data centres should be located within the province of Ontario.

2.8.1. Facility location

The location of the data center facility should not be located:

- In an area known to be subject to natural disasters (e.g., flooding, earthquakes);
- Within five kilometres of an area or facility with potential for industrial disaster (e.g., highways, railway lines, airports, high pressure pipelines, high voltage power transmission lines, oil refineries, power/electrical generating stations, water storage facilities, chemical plants, military bases, research facilities); or
- In proximity to high profile and/or high-risk installations (e.g., military offices, financial districts, embassies, critical infrastructure, known political or symbolic targets);

Data centre sites are encouraged in areas where:

- The location is readily accessible to authorized employees;
- Fire and emergency services are able to respond quickly to incidents;
- Ready access to electrical power is available from diverse sources (e.g., multiple electrical grids);
- Redundant telecommunication ingress, water supply, and/or other utilities is available;
- Truck deliveries can be made using local roads; and
- Future expansion is possible if increased capacity is required.

2.8.2. Landscaping

Minimum landscaped area

All buildings which comprise the data centre facility should have a perimeter consisting of at least 10 metres of clear landscaped ground, without vehicular access or parking.

Enhanced safeguards

Data centre facilities that require enhanced safeguards **must** employ the following:

- The perimeter distance requirement **must** increase to 45 metres unless access control measures are place to mitigate relevant risk, with any additional standoff requirements or controls identified via the relevant TRA;
- Landscaping barriers of a type or design that will prevent an unauthorized vehicle from closely approaching or being placed adjacent to the facility **must** be placed to enforce the required perimeter distance;

- The layout of landscaping and perimeter barriers **must** not interfere with the ability of fire services to arrive and gain access to the premises in the event of an emergency;
- Landscaping features close to the physical premises **must** not obstruct CCTV or other monitoring; and
- Facility grounds **must** be kept clear at all times of any objects (e.g., maintenance items) that could facilitate unauthorized access or access to the building roof (e.g., tall garbage bins, ladders, or scaffolding).

2.9. Facility construction

2.9.1. Utilities

Safeguards

Utility crews should not be permitted to conduct work within 15 metres of a data centre facility when excavation or work on overhead lines is required, unless planning and management of such tasks has been organized with the assistance of the Government of Ontario.

In the event of an emergency requiring utility crew access to a data centre site, prior agreements should be established with the utility company on procedures appropriate for use in the vicinity of the data centre.

Utility spaces (e.g., mechanical, electrical, and telecommunications rooms) **must** be locked at all times using key locks and managed key control. Access to utility spaces **must** be documented for audit purposes.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards to protect utility rooms **must** employ the following:

- Intrusion detection systems **must** be implemented for utility access/areas;
- Security grade door fastening hardware **must** be used in conjunction with a metal door and frame (RCMP G1-017 level III as a minimum door hardware assembly requirement);
- Automatic door closing and locking devices **must** be used; and
- Any door of this type held or propped open for more than a brief interval should produce an integral alarm sound or result in an alarm signal.

2.9.2. Lighting

Lighting is a valuable and inexpensive deterrent to physical breaches. It improves visibility for checking badges, identifying individuals at entrances, inspecting vehicles, preventing unauthorized entry, and detecting intruders.

Lighting should be chosen according to need and desired effect. The amount of light required to detect the movement of intruders will vary by location and environment. The required light output may also depend on the specific spectrum required.

All lighting should adhere to ANSI/IES (American National Standards Institute and Illumination Engineering Society) recommended illumination levels. Required light output may depend on the specific spectrum required.

Consideration for energy savings should be made for all lighting decisions.

Exterior illumination

The following site areas **must** be provided with night illumination:

- All exterior entrances (including internal corridors or entrances for data centres located within a facility shared with another organization);
- Building/facility perimeter and any associated fence or barrier;
- Exterior building surfaces;
- External common areas (e.g., parking lots, driveways); and
- External access hatches and window openings.

Exterior lighting **must** illuminate surfaces and objects to a height at least 2.45 metres from the ground. Exterior lighting sources may include:

- Existing street lighting;
- Standard exterior lighting (e.g., entrance lighting, yard/grounds lights); and
- Security lighting (e.g., building mounted directional lighting, site perimeter lighting, flood lights, lights with specific spectrum for CCTV applications).

In instances where extensive exterior lighting is required, an environmental impact assessment should be considered if concerns exist regarding potential impact of the lighting proposed. Location of species sensitive to light or proximity to sites such as nature preserves or conservation areas should be determined. Installation of full cut-off lighting fixtures should be considered to reduce the impact of light pollution.

Interior lighting

Interior lighting **must** provide adequate lighting to all surfaces and safe visibility for staff within the facility at all times. All interior areas **must** include lighting that illuminate wall surfaces and equipment to a height at least 2.45 metres from the ground.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Specific colour spectrum lighting should be used for optimal CCTV images;
- Tamper resistant exterior light housings **must** be installed to resist attack;
- Lighting **must** be positioned to prevent shadows near all entrances and the facility perimeter;
- Perimeter lighting **must** be arranged to provide for a degree of overlap in coverage, such that the failure of (or an attack against) a lighting fixture does not result in a complete loss of illumination for the corresponding area;

- Wall mounted exterior fixtures **must** be installed at least 4 metres in height from the ground; and
- Approximately ten percent (10%) of data centre lighting should be powered from an emergency power circuit.

2.9.3. Roof access

Roof access and roof hatches are an avenue of opportunity for attackers.

Safeguards

- Roof access ladders **must** be protected via a locking shroud, or removed;
- Ease of "fence to roof" or similar movement **must** be identified and controlled;
- The number of roof hatches should be kept to a minimum;
- Inner locking devices **must** be installed for all roof hatches;
- Roof hatches should be monitored;
- Roof hatches should be constructed of a robust material (e.g., hardened steel);
- A roof hatch should not be located in a security zone; and
- A roof hatch **must** not be located in a high security zone.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- No external roof access ladders (even if a locking shroud is used);
- Roof hatch and roof areas **must** be monitored electronically;
- Dedicated roof top lighting **must** be present, but should not highlight the location of roof hatches; and
- CCTV **must** be installed to permit monitoring of roof areas and hatches.

2.9.4. Ceilings

Suspended ceilings are vulnerable to attack. Solid slab floor to slab ceiling walls should be used within the data centre. These walls **must** be used in the construction of security and high security zones.

Safeguards

- Solid ceiling construction and slab to slab walls should be used consistently between all areas (or zones) within all data centre facilities;
- Solid ceiling construction and slab to slab walls **must** be used between a public zone and a reception zone;
- Solid ceiling construction and slab to slab walls **must** be used for a security zone or high security zone; and
- Additional safeguards (e.g., monitoring) should be used in situations where existing facility structures do not allow for extended walls, or the space above drop ceiling level is required for air movement.

2.9.5. Windows

Facility planning activities **must** specify any areas that cannot use windows due to security requirements. These requirements may include:

- Deterrence of visual surveillance;
- Deterrence of acoustic or other forms of remote surveillance; and
- Resistance to external unauthorized entry.

If windows must be included in a newly constructed facility or are present in an existing or leased facility, some types of security glazing and synthetic materials can assist in reducing risk. The relevant TRA should determine the required degree of safeguard effectiveness, and document the need for such window materials.

Building code requires that safety glass **must** be used on doors and windows that may pose a hazard if broken. It should be noted that some safety glass intended for fire and safety use will not offer increased impact load over standard glass types, and does not provide a deterrent factor for unauthorized access. Annealed glass should not be used in areas where attack is likely (e.g., exterior window openings) or injury could result.

Safeguards

- Select glazing that will deter attack, with reference to a relevant TRA;
- Windows that can be opened **must** have locking devices installed, remain locked at all times, and be monitored to detect unlocked or open windows;
- Where possible in existing facilities, permanently seal opening windows (in such instances where life safety considerations will not be affected);
- Avoid the inclusion of windows where possible during facility construction;
- Exterior overhead doors **must** not contain windows; and
- A security zone or high security zone **must** not contain any exterior windows.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Ground floor windows **must** be avoided in security and high security zones;
- All 2nd floor windows **must** be at least three (3) metres in height above ground level for any point on the premises;
- Security glazing **must** be used for any exterior facility ground floor windows (with potential application for all windows if recommended by a relevant TRA); and
- Interior security glazing within the facility as per TRA requirements;

2.9.6. Doors

Doors provide entry to facilities and zones, and are therefore a weakness in the robust construction of the data centre.

Exterior doors

Exterior doors should be of metal construction (e.g., hollow steel with internal stiffening or reinforcement). The entire door assembly **must** include a metal frame and security grade hardware (e.g., RCMP G1-017 level II as a minimum standard). Automatic door closing devices **must** be used, and exterior doors **must** reliably lock when closed. If held or propped open for more than a brief interval, exterior doors should have a mechanism to produce an integral alarm sound or result in an alarm signal.

Exterior locksets **must** be of a high security design that will resist manipulation.

Interior doors

Hollow core wood doors should be replaced with hollow metal or Kalamein doors (with a 105 minute fire protection rating)[3]. Hollow core wood doors **must** not be used to protect security or high security zones, or in instances where enhanced safeguards are required.

Impact resistant glazing should be installed in glass doors. Polycarbonate material will resist attack, but care **must** be taken to ensure that the use of such panels does not contravene building and fire safety codes. If impact resistant panels cannot be installed, laminated glass is an acceptable alternative.

Glass doors **must** not be used to protect security or high security zones. Door assemblies in all such environments **must** use metal frames and security grade hardware (e.g., RCMP G1-017 level II as a minimum standard). Locksets **must** be of a high security design that will resist manipulation.

In instances where enhanced safeguards are required, the requirements above **must** be extended to operations zones.

Overhead doors

Overhead doors should be constructed of robust material (e.g., steel), with secure, heavy-duty hinges between sections, and no windows. The steel panels should be reinforced from the inside (e.g., with welded steel vertical supports). Overhead doors with thin wood or plastic panels may permit an intruder to enter a facility once the panel is removed by via impact or other means; this type of overhead door should not be used. If their use cannot be avoided (e.g., in a leased/existing facility), these panels should be augmented by retrofitting expanded metal mesh, steel plates, steel bars, or metal strap reinforcement. Overhead doors that use multiple leaves to operate **must** employ locking mechanisms to ensure individual leaves cannot be lifted or manipulated.

---

[3] *Fire Protection and Prevention Act*, Office of the Ontario Fire Marshall, 1997 (http://www.e-laws.gov.on.ca/html/source/regs/english/2007/elaws_src_regs_r07213_e.htm)

Frames and astragals

Door frames should be of quality construction and design, and be as strong as the door they support. To deter attacks that involve spreading door frames (defeating the lock and bolt), door frames should be blocked and reinforced at the strike area with strong material (e.g., hardened steel).

A full length astragal on reverse-hand doors and double-doors offers resistance to prying and attacks involving the door latch or bolt. Astragals are usually fastened to the door edge with carriage bolts, or welded in place. On a double door, the astragal is usually mounted on the active leaf of outward opening doors. Astragals intended to deter attack **must** be of robust construction and material (e.g., hardened steel). Exposed fasteners or removable screws/bolts used to affix astragals not welded in place **must** not be available to the attacker.

The astragal on outward opening sets of doors that lack a centre mullion should be mounted on the active leaf to ensure the door without the astragal will close first.

Hinges

Hinges **must** face inward on exterior doors, and be of heavy-duty construction. Exterior doors with accessible hinges may provide an intruder with access to a facility via removal of hinge pins. Some security hinge hardware can deter this type of attack; the following describes security grade hinge configuration:

- Hinges are to be installed with secured or non-removable pins to deter attempts to remove hinge pins; and
- A locking pin is to be installed in the hinge plate to deter lifting of the door.

Secure hinge hardware should be deployed for all doors intended for access control purposes, and **must** be used in instances where hinges cannot be reversed on doors that protect security and high security zones.

Double doors

Double doors should have the inactive leaf secured with top and bottom bolts (preferably automatic or edge mounted), unless the doors have a centre mullion. An astragal of robust construction and material (e.g., hardened steel) **must** be installed on all double doors to deter attacks that involve prying back a door latch.

Exit doors

Exit doors typically provide direct access to the exterior of the building or into an exit stairwell in a multi-story building. Exit doors **must** open in the direction of egress for emergency routes, and meet the following requirements:

- Exit doors **must** be located and signed for facility exit purposes only;
- Exit doors **must** be secure from attack from the building exterior; and
- The exit door should be connected with the intrusion detection system, with a monitored alarm activated when opened. This requirement is mandatory for environments that require enhanced safeguards.

2.9.7. Fire protection

A comprehensive fire detection and suppression system is required to ensure that life and property are protected. Fire and life safety protection systems (e.g., fire alarms, heat/smoke detectors, carbon monoxide detection, automated fire suppression, extinguishers, and emergency exit routes) should be professionally designed, installed and maintained.

A comprehensive water and leak detection system is a priority to ensure that equipment and data is protected. Water and leak detection systems should be professionally designed, installed and maintained.

Detection safeguards

The following requirements apply to all data centre fire detection safeguards:

- Heat and smoke detection devices **must** be professionally installed and maintained;
- Heat and smoke detection devices **must** be installed in accordance with NFPA 72 requirements;
- In a security zone or high security zone with a raised floor, heat and smoke detection devices **must** be installed both above and below the floor surface in accordance with the Ontario Building Code;
- Detection devices should be interconnected with the fire suppression system, local alarms, facility management systems, and remote monitoring stations;
- Detection devices should be positioned appropriately relative to airflow to ensure early detection; and
- All detection devices **must** be tested according to a defined schedule.

The Fire Code specifies frequencies of checks, inspections and tests of fire alarm systems. Such validation will likely apply to a building fire alarm system that has been modified to satisfy this standard.

Suppression safeguards

Fire-rated walls should be installed within data centre facilities, in accordance with the *National Building Code of Canada* (NBCC)[4]. For facilities five to six stories in height or less, the resistance rating should be at least 45 minutes in duration. Taller structures should employ a two hour resistance rating for such walls. Facilities with on-site power capability (e.g., diesel power generation) and fuel storage should increase this level to three hours, and sprinklers should be in place (pre-action, pre-action deluge, or wet pipe).

Due to the intended function of a data centre environment, chemical or clean agent suppression (e.g., FM-200, Inergen, ECARO-25, Novec 1230) in equipment areas is

[4] *Structural Fire Protection – Predictive Methods*, National Research Council Centre (http://archive.nrc-cnrc.gc.ca/eng/ibp/irc/bsi/87-fire-protection.html)

preferable. The ability to manually trigger such suppression should be provided within areas protected by chemical suppression (via pull stations). Appropriate signage for safety purposes **must** be erected in areas protected by chemical fire suppression.

Portable fire extinguishers should also be provided throughout the data centre facility.

All suppression systems **must** be maintained on a pre-defined schedule.

2.9.8. Raised floors

Raised floors are used for data centre I&IT operations areas. These environments are typically part of a security zone.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards should employ the following:

- Unauthorized removal of floor panels in a high security zone should activate a monitored alarm; and
- Access to the area below the raised floor should be approved by facility and/or program management prior to work activities.

2.9.9. Loading docks and receiving

Loading docks, receiving areas, and mail rooms are potential vectors for attack; the risk associated with their operation **must** be identified and mitigated.

Safeguards

- Shipping and receiving areas **must** be correctly integrated into the zone design of the facility, and cannot be part of a security or high security zone;
- Overhead doors **must** be securely closed via integral locking or with padlocks that can be accessed only from inside the facility;
- Doors should be heavy-duty sectional or vertical lift doors, with a steel outer casing on both the inside and outside, or a reinforced panel design;
- Mail rooms should be located at separate facilities where possible, to reduce the risk associated with packages from hostile individuals or organizations; and
- If a mail room must exist within the same facility, the relevant TRA **must** explicitly address the mail room, identify any risk, and document both existing and required safeguards.

Enhanced safeguards

Data centre facilities that require enhanced safeguards **must** employ the following:

- Deliveries **must** be arranged in advance and validated upon arrival before access to a loading dock or receiving area is permitted; and
- Vehicles approaching and/or entering the loading dock or receiving area of a facility that requires enhanced safeguards should be subject to vehicle

undercarriage inspection and related techniques where appropriate, and within the bounds of legal authority.

2.9.10. Elevators

The following safeguards apply to elevator location and operation:

Safeguards

- Passenger and freight elevators should be located in a public zone or reception zone at ground level;
- Elevators to data centre areas in a shared facility **must** be considered a public zone; and
- In a shared facility and/or multiple floor facility, ingress points should require traversal of a reception zone accessible from the elevator lobby.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Elevator interiors **must** be subject to monitoring (e.g., CCTV);
- Operation of elevators **must** be controlled by an access control system either 24 hours a day, or during periods where access is restricted (e.g., during evenings); and
- Elevators **must** only stop on those floors where access has been authorized.

2.9.11. Circulation routes

A circulation route is the path used by employees to move within the facility, for example, when:

- Entering a facility;
- Exiting a facility;
- Emergency evacuation of a facility; and
- Entering or exiting zones.

Circulation routes are necessarily influenced by facility layout, access control needs, and life safety requirements. Circulation routes may be optimized to balance these priorities if considered during facility design. Entrances, exit points, and corridors can be placed to minimize risk and avoid potentially expensive additional safeguards.

Additional safeguards and access control requirements intended to influence circulation routes may be recommended by the relevant facility and/or data centre TRA.

Safeguards

- All ingress from a public zone to an operations zones **must** pass through a reception zone;
- A reception zone **must** be controlled by data centre and/or facilities management, an appropriately assigned Government of Ontario security function, or a third party engaged under contract to provide such services;

- An operation zone **must** not permit for public access during routine operations;
- Exit routes intended for egress from a public zone **must** be located/configured as public zones themselves;
- With the exception of cross-over floors, all exit doors that comprise emergency egress routes from controlled areas should be equipped with automated door closing mechanisms, be of sufficient door and hardware construction to deter attack when closed, and make use of “hold open” alarms;
- Where possible, dedicated emergency egress routes should be constructed or designated; and
- Signage in emergency egress areas should indicate the intended direction of traffic;

2.9.12. Stairwells

Stairwells are, in most shared facility environments, considered public zones (due to emergency egress requirements in federal and provincial building codes).

Safeguards

- Where possible, stairwells required for emergency egress should be dedicated to this purpose, and appropriately signed;
- Stairwells intended for regular use and/or emergency egress **must** comply with the Ontario Building/Ontario Fire Code requirements as applicable; and
- Stairwells **must** not allow for access to controlled areas (e.g., security or high security zones) in a manner that bypasses intended access control, nor may they permit for bypass of reception zones.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Stairwells **must** only be used for emergency exit in a facility with elevators;
- Stairwell doors **must** be secured with magnetic locks, and monitored;
- Stairwells and related corridors **must** be monitored (e.g., CCTV); and
- Perimeter exterior doors from a stairwell **must** be monitored (e.g., CCTV).

2.9.13. Floor loading capacity

Safeguards

The maximum weight bearing capacity or floor loading capacity of the data centre systems / storage area (e.g., a raised floor security zone) **must** be determined, posted, and provided to any group planning expansion or development within the facility.

2.10. Physical access control

2.10.1. Perimeter safeguards

Safeguards

- Minimum building/facility standoff or clear ground distance of 10 metres from public easements and vehicle traffic **must** be enforced;
- All windows **must** be configured as per the recommendations in document;
- All doors **must** be configured as per the recommendations in document; and
- Roof access doors **must** be secured as per the recommendations in this document.

Enhanced safeguards

Data centre facilities that require enhanced safeguards **must** employ the following:

- Fencing (e.g., chain link or welded steel mesh) with a minimum height of 2.2 metres should be erected around the entirety of the facility perimeter;
- Fencing should be placed such that surveillance of the perimeter can be conducted, and that “fence to roof” access is prevented;
- Consistent illumination of the perimeter and/or fence should be provided, such that perimeter monitoring can identify potential or ongoing attack;
- Gates for employee/pedestrian and vehicle access to the facility should be of a design that can be locked if required;
- No signage should identify the ownership or role of the facility;
- Parking areas and vehicle lanes **must** be located 45 metres or more from facility exterior walls, unless other forms of access control are enforced;
- Monitoring of the facility perimeter and grounds **must** be conducted (e.g., via CCTV);
- Fencing of roof areas **must** be installed for areas where an adjacent roof is closer than four metres to a facility structure;
- Exterior windows **must** have monitored intrusion alarms;
- Utilities, electrical power, and communications circuits **must** enter the facility underground, preferably via redundant/discrete ingress points; and
- Facility air intakes should be identified and protected in a manner that will deter the placement of pollutants or irritants.

2.10.2. Guard services

The results of a TRA may identify a requirement for guard services. The following are functions that may be provided:

- Enforce procedures within the facility;
- Assist with the identification of authorized personnel;
- Support life safety obligations and processes;
- Monitor alarms, CCTV, and conduct patrols;
- Monitor the reception zone to control facility access;
- Respond to alarms and security incidents; and
- Prepare incident reports.

2.10.3. Personnel screening

Access to specific zones within data centres (e.g., a high security zone) **must** be limited to those who have obtained a successful screening result following an approved personnel screening process. For more information on the specific screening process for a given program, consultation with the relevant program area(s) is recommended. Staff **must** complete any required personnel screening process prior to being granted access to an area where a successful screening result is mandatory.

Vendors and visitors who have not completed the personnel screening process **must** be escorted by authorized staff in controlled areas of the facility, and not left unattended.

All employees who require access to a high security area **must** first obtain a valid personnel screening result.

2.10.4. Physical access control

Access to controlled areas **must** be restricted in accordance with the principle of least privilege outlined in GO-ITS 25.0 General Security Requirements.

The use of turnstiles should be considered for reception areas that lead to security and high security zones. These devices are effective both for deterring typical “door surfing” attacks upon entry, and the removal of equipment upon exit.

Access control systems **must** be monitored to detect and respond to violations of data centre procedures and security policies.

Access to security zones should require the use of two factor authentication (e.g., the requirement to use a PIN in conjunction with a proximity card). Access to a high security zone **must** require the use of two factor authentication. Dual custody systems should be considered for use when controlling access to a high security zone.

2.10.5. Identification cards

The only zone where identification cards are not required is a public zone. The use of identification cards **must** be instituted for all other zones. Staff who request access to the data centre should have their identification examined upon arrival to the reception zone.

Safeguards

- Identification cards **must** be worn at all times by staff and long-term contractors who require access to or will be operating in the data centre environment;
- Identification cards **must** have a photo of the cardholder, and should have an expiration date;
- Identification card distribution and return **must** be centrally managed;
- The identification card database **must** be regularly consulted for the purpose of identifying identification cards that have expired;
- Expired cards and associated access capabilities **must** be immediately revoked;

- The expiration date for long-term contractor identification should never extend past the end of the contract term; and
- Managers **must** retrieve identification cards for their supervised employees upon the last day of employment or long-term contract.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Identification may be requested from employees when access to a security or high security zone is attempted, despite the assumption that their credentials were validated upon entrance to the facility; and
- If visual validation of identification is to be employed, unique identification should be issued to those individuals with authorized access to a high security area.

2.10.6. Visitor access

The presence of visitors in data centres is often necessary to permit for vendor support and repair of equipment. Visitor access privileges can also be abused or exploited by attackers.

Safeguards

- **All visitors to the facility must announce themselves at the reception zone, provide photo identification, and sign in;**
- **The employee who receives the visitor must enter the reception zone and approve the visitor before access is granted;**
- **The visitor must be provided with a visitor badge that is worn in a manner as to be visible at all times;**
- **The employee responsible for a visitor must not leave the visitor unattended in a security or high security zone, and is accountable for the visitor at all times;**
- **The visitor badge must be returned to the reception zone when the visitor returns to the reception zone;**
- **Visitor badges must be serialized, and tracked (e.g., the badge number assigned to a specific visitor on a given day must be recorded);**
- **The visitor log must also track the date of the visit, arrival time, exit time, and the staff member responsible for the visitor while on the premises;**
- **Visitor logs must be retained for a period of two years;**
- **The loss or failure to return a visitor badge must be reported to facility security; and**
- **Lost visitor badges and any accompanying access card/privileges must be revoked immediately.**

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Visitors should surrender photo identification prior to being escorted from the reception zone (with personal identification returned upon surrender of the assigned visitor badge, once the visit is complete); and
- Visitors may be required to surrender personal belongings and electronic devices prior to being escorted from the reception zone.

2.10.7. Contractor access

Building contractors may require facilities access, sometimes after typical business hours. Contractors **must** not be excluded from access control requirements.

Safeguards

The following safeguards are intended to reduce risk associated with contractor access:

- Work access after regular business hours **must** be arranged prior to arrival;
- Standard visitor procedures **must** be followed at all times;
- Company affiliation and work orders (or notification of site visits from facility management) **must** be provided and validated prior to contractor movement beyond the reception zone; and
- Access **must** not be granted to contractors who arrive without making prior arrangement and obtaining authorization.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Contractors **must** obtain a successful personnel screening result prior to being authorized to conduct work in controlled areas;
- While on site contractors **must** be escorted and monitored at all times;
- The contractor work area should be isolated from controlled zones with temporary barriers and safeguards, if existing controls between zones are likely to be affected by planned work;
- If contract work results in a conduit or other gap between two zones due to an error, the incident **must** be immediately reported to facility security, and compensating controls **must** be instituted.

2.10.8. Electronic access control

In addition to traditional lock and key safeguards, electronic access control **must** be used in data centre environments where monitoring and audit requirements apply, as these systems simplify the generation of activity logs.

Any deployed electronic access control system **must** be monitored for events and faults.

Safeguards

The following safeguards are recommended:

- Electronic access cards **must** only be provided once authorization has been provided, in accordance with GO-ITS 25.0 General Security Requirements;
- Access card holders **must** acknowledge receipt of their cards, understand their responsibilities, and safeguard them from loss or theft;
- The ability to limit access by time of day and location should be explored to reduce the opportunity for unauthorized movement;
- All systems associated with electronic access control **must** have accurate local time, obtained in a manner consistent with the guidance in GO-ITS 25.0 General Security Requirements;
- Systems which maintain the state of the access control infrastructure (e.g., users, privileges, etc.) **must** be centrally managed (with data backed-up);
- Two factor authentication models (e.g., physical card and PIN) should be used for access to security zones;
- Two factor authentication models (e.g., physical card and PIN) **must** be used for access to high security zones;
- Loss or theft of any electronic access card or device **must** be immediately reported to facility security, and the card or device promptly disabled;
- All access cards or devices **must** be accounted for in inventory with issue and expected return dates;
- Data retention practices and privacy impact **must** be documented;
- Access privileges **must** be revoked upon termination or other events as described in GO-ITS 25.0 General Security Requirements; and
- Access to different zones **must** be explicitly configured on a per-user basis, according to employee roles and degree of authorization.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

2.10.8.1. Electronic card access

- Access card or device systems should be enhanced with measures such as turnstiles to deter instances of “door surfing”;
- Two factor authentication models (e.g., physical card and PIN) **must** be used for access to security and high security zones; and
- Emergency/generator power should be configured to supply power to electronic access control systems in the event of a power outage, with deference to life safety considerations.

2.11. Exit routes

Access control systems must not interfere with the requirements for safe exit routes in the event of an emergency. However, the design and operation of an exit route must not contravene zone specifications or minimum security requirements. In the event that a compromise must be made in the design or operation of the facility as to the use of exit routes, life safety considerations should be given priority.

Safeguards

- **Exterior emergency exits must not be used unless in the event of an emergency;**
- **An exit route should not allow a person, without authorization, access to a controlled area as a means for exit;**
- **All emergency exits must swing in the direction of the exit and trigger a monitored alarm when opened;**
- Regular exit routes should employ signage and directional indication to guide employees to exit via operations or reception zones (where life safety considerations permit) to limit the number of sensitive zone interfaces; and
- Access to and design of exit routes **must** comply with Ontario Building Code safety regulations.

2.12. Intrusion detection

2.12.1. Perimeter intrusion detection

The required degree of intrusion detection safeguards will be influenced by the zone being monitored and the degree of risk associated with the facility.

Intrusion detection systems perform the following functions:

- Providing alerts for real time attempted and successful unauthorized access;
- 24/7 monitoring of facility access;
- Providing alerts and access tracking and history logs; and
- Providing photo images for identification of unauthorized access.

Safeguards

Intrusion detection systems should be implemented in conjunction with monitoring capabilities (e.g., CCTV) to increase detection/response capabilities. Alarms **must** be monitored if response time is to be reduced. Alarm and CCTV monitoring areas **must** themselves be considered security zones, and operated in an appropriate manner.

Monitoring of electronic card access **must** be implemented where magnetic door locks are used to restrict access.

2.12.2. Closed circuit television (CCTV)

The effectiveness of CCTV deployment depends on the system design, quality of equipment, degree of monitoring, response time to alarms, and maintenance of the system. In order to prevent security incidents and/or unauthorized access, a timely response to events detected via CCTV is essential.

CCTV system design **must** be a product of facility planning, and make reference to the data centre zone and perimeter security design. The use of video analytics should be considered when CCTV is deployed for activity monitoring purposes.

The use of (or reliance upon) CCTV as a deterrent measure should be carefully considered, as some attackers cannot be effectively deterred by surveillance or

detection measures alone. Any assessment of CCTV effectiveness should be weighed against specific anticipated threat agents. The relevant TRA should document and present any related findings to assist in setting the parameters for CCTV operation.

Safeguards

- CCTV systems **must** provide 24/7 monitoring and recording and produce quality output in all lighting conditions (e.g., additional lighting and/or IR capability for use in darkness, if required);
- Exterior CCTV systems **must** be weather-resistant;
- CCTV back-end systems should provide the ability to include codes or timestamps to assist in event correlation;
- Colour cameras should be installed for more accurate identification of individuals, articles of clothing, and equipment;
- Cameras **must** be located at all exterior doors, and within the reception zone;
- System **must** be assessed daily to ensure all functions are operational;
- CCTV recordings (magnetic tape or digital media) **must** be scheduled for regular and frequent back-up, and protected against modification;
- CCTV operation in public areas should include appropriate signage to indicate the collection of personal information (e.g., facial likeness), and provide contact information for an appropriate information and privacy authority; and
- CCTV operations **must** be centrally managed, and operated in accordance with all applicable local regulation and legislation.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Cameras **must** be located at entrances to security and high security zones;
- Exterior cameras **must** be protected from attack by secure/reinforced housings; and
- Security and high security areas that are monitored by facility employees (or using CCTV that can be accessed in the event of an alarm) should make use of PTZ (pan/tilt/zoom) CCTV devices to provide for enhanced visibility, particularly when equipment layout may obscure line of sight.

2.13. Server rooms

Raised floor rooms for the operation of computer servers are the most critical component of the data centre facility, but some small server rooms may exist within the facility that are not part of the raised floor environment.

Safeguards

- **Must** be located in an operations or security zone;
- Electronic access control **must** be installed;
- Access **must** be provided only to authorized users;
- Security locking devices (magnetic/electronic) door locks **must** be installed;
- Intrusion detection monitoring **must** be conducted 24/7; and

- Access **must** be authorized in accordance with the requirements stated in GO-ITS 25.0 General Security Principles.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- Small server rooms **must** be designated at security zones;
- Access control and CCTV monitoring of server room entrances and interiors **must** be conducted as per security zone requirements;
- Walls **must** meet enhanced safeguard requirements described in sections 2.9.4 and 2.9.7 of this document;
- Room construction should include fire resistant materials; and
- Servers intended to store or process aggregated sensitive information, or for operation of programs where a relevant TRA has indicated a high integrity and/or availability value, **must** be migrated to a managed raised floor environment.

2.14. Cross-over floors

Any facility more than six stories in height will require the use of cross-over floors (due to federal building code requirements). Building regulations for cross-over floors may not support access control requirements. Some types of zones are not appropriate for floors with a cross-over requirement. Cross-over floors should be identified by the relevant facility TRA, and considered when facility security planning is conducted.

Doors leading from stairwells to crossover floors **must** be unlocked, or support an automatic magnetic lock release in the event of an emergency. Stairwell doors to building floors **must** not be locked if they are more than two floors (up or down) from the nearest unlocked floor exit, and available floors **must** provide more than one exit route. Consult relevant building codes for information regarding master key requirements for floor entry from a stairwell designated as an emergency route.

Safeguards

- **For new construction, the layout of stairwells relative to public and reception zones should be of a design that allows unlocked emergency doors to not open into operations zones;**
- **Monitored and/or audible alarms should be used to alert employees and facility security to access from unlocked emergency doors to operations zones (in cases where this layout cannot be avoided);**
- **Security and high security zones must not be located on cross-over floors; and**
- Doors from stairwell to cross-over floor areas **must** be marked as exit routes where applicable, to guide employee movement during emergencies.

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- **For new construction, the layout of stairwells relative to public and reception zones must be of a design that allows unlocked emergency doors to not open into operations zones; and**
- **Monitored and/or audible alarms must be used to alert employees and facility security to access from unlocked emergency doors.**

2.15. Emergency electrical power

Electrical power is critical to data centre operation. Emergency power **must** be adequate to meet availability requirements and service level agreements.

Safeguards

- **Basic facility services (elevators, emergency lighting, HVAC) must be provided by adequate emergency power supply;**
- **Adequate emergency electrical power may vary, and such variance should be identified during system specification;**
- **Security systems (e.g., access control, monitoring) must be provided with adequate emergency power for as long as basic facility services are functional;**
- **Battery powered emergency lighting should be available throughout the data centre;**
- **Testing of emergency power must be included in any applicable data centre disaster recovery (DR) and business continuity planning (BCP) exercises;**
- **Multiple electrical power grids should be used for data centre power, to provide for redundancy in the event one power grid fails;**
- **Data centre facilities should have backup generator capabilities; and**
- **To prepare for the event of extended power outages, data centre facilities and/or operations staff should negotiate and maintain contracts which guarantee the supply of fuel for a backup generator.**

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- **All security systems (e.g., access control, monitoring) must have an uninterrupted emergency power supply, regardless of the status of basic facility services;**
- **Multiple power generators should be maintained to enhance redundancy; and**
- **Emergency electrical power must be in place for any area, zone, or equipment deemed time critical.**

2.16. Staff and visitor parking

Safeguards

- **Parking areas should not exit into an operations zone, even if underground;**

- **All visitor routes from parking areas must lead to a reception zone;**
- **After hours access to indoor parking should be controlled; and**
- **Parking areas and related facility entrances should be monitored (e.g., CCTV).**

Enhanced safeguards

Data centre facilities that require enhanced safeguards **must** employ the following:

- **Electronic access control must be provided to access a gated parking area;**
- **Electronic access control must be provided to gain any facility/perimeter access;**
- **Outdoor parking areas should be separately fenced from the facility;**
- **Parking areas must be monitored (e.g., CCTV or employee patrol); and**
- **Enhanced lighting to ensure adequate viewing (consistent with lighting requirements for facilities requiring enhanced safeguards in this document).**

2.17. Maintenance and cleaning services

Maintenance personnel **must** follow the same security and access control procedures as data centre employees. The following safeguards apply to all third party maintenance personnel:

Safeguards

- **All routine maintenance should be conducted during standard business hours;**
- **All maintenance staff must be subject to all access control procedures;**
- **Maintenance staff must be escorted at all times when in a high security zone;**
- **All maintenance staff must present photo identification upon request; supplied identification cards for use within the facility must be worn at all times and be in plain view;**
- **Contracts with maintenance providers must indicate mandatory compliance with facility security policies and procedures;**
- **Vendors should be able to provide current and past lists of their employees working at a given data centre facility, accompanied by a photograph; and**
- **Vendors should be able to provide past schedule details for employees upon request, if required (e.g., for investigation purposes following an incident).**

Enhanced safeguards

Data centre facilities (or zones) that require enhanced safeguards **must** employ the following:

- **Maintenance staff working in a security zone must be escorted at all times; and**
- **A current list of maintenance staff authorized by name to enter the facility should be maintained in all reception zones, including information photographs, vendor affiliation, work order or contract number, and anticipated end date for authorized access (if applicable).**

2.18. Garbage removal and recycling

Safeguards

- **Large garbage removal bins that do not contain recycled paper must be located in a public zone (i.e., outdoors);**
- **Recycling (included recycled paper) being held for processing (i.e., by a third party document destruction company) must be kept in an operations zone, protected by access control and monitoring;**
- **Monitoring of refuse/garbage areas (i.e., CCTV) should be conducted to detect attempts to obtain discarded information; and**
- **Food or drink is not permitted in server rooms or raised floor environments to avoid damage to equipment and reduce the requirement for garbage collection in these areas.**

3. RESPONSIBILITIES

ITS Data Centre Operations / OPS Facility Services

ITS / OPS staff assigned to data centre operations roles are, for the specific data centres placed under their respective authority, responsible for:

- Compliance with the requirements in this standard, and ensuring that data centre security safeguards meet these requirements;
- Informing management of all physical security incidents, suspected breaches, information security incidents, or faults in facility security systems (i.e.., a failed access control device);
- Assisting in responding to reports of security concerns or incidents;
- Supporting security incident reporting and management procedures;
- Assisting in efforts to prevent, detect, and respond to security incidents via safeguards, incident handling, and security management;
- Following physical security procedures and best practices;
- Ensuring that recommended safeguards identified by relevant Threat/Risk Assessments and/or audits deployed;
- Conducting periodic reviews of data centre security posture;
- Ensuring that all third party service providers comply with this standard and other related government policies;
- Ensuring that security requirements are documented in contracts and agreements with contractors/consultants, and any third party service providers;
- Ensuring that staff and contractors/consultants using the data centre facility are aware of, and adequately trained in, their responsibilities as set out in this document (and other standards);
- Ensuring that Business Continuity Planning and a Disaster Recovery capacity is in place for the data centre facility itself, and consulting additional/related BCP/DR guidance; and
- Negotiating and managing supply of electricity, fuel, etc. for instances of power loss.

Data Centre Clients / Users / Staff

Data Centre clients, users, and staff are responsible for:

- Operating in a manner consistent with this document, and;
- Reporting security concerns or incidents to facility management, ITS operational security, and the IT Service Desk.

Program Managers

Program Managers are responsible for:

- Ensuring that their applications are housed in appropriate data centres, given the security requirements, Threat/Risk Assessment (TRA) findings, and data classification associated with their applications;
- Complying with this standard when accessing their equipment in a data centre;

- Ensuring that TRAs are completed, and recommendations for additional safeguards are evaluated and/or deployed;
- Ensuring that Disaster Recovery (DR) and Business Continuity Planning (BCP) activities have been appropriately conducted for their equipment and programs;
- Ensuring visitors or vendor/maintenance staff associated with their programs are properly escorted in accordance with this standard; and
- Ensuring any temporary visitor badges associated with their facility visits are returned to Operations Security.

Chief Information Officers

The Chief Information Officers are responsible for:

- Being aware of data centre operations and any potential facility security impact regarding applications under their custodianship; and
- Ensuring that recommended safeguards identified by relevant TRAs and/or audits are evaluated and/or deployed.

Corporate Security Branch

The Corporate Security Branch (CSB) is responsible for:

- Maintaining this standard and all other applicable IT security standards, policies, procedures and related guidance on behalf of the Government of Ontario;
- Monitoring industry best practice regarding physical safeguards, specifications, and techniques;
- Liaising with physical security authorities at other levels of government, and
- Conducting Threat/Risk Assessments for data centre physical facilities.

Ontario Realty Corporation (ORC)

The Ontario Realty Corporation is responsible for:

- Negotiating leases on behalf of the OPS and ensuring that site surveys and TRAs have been conducted prior to entering into a lease agreement;
- Ensuring that property owner makes any changes as stipulated in lease agreements and/or a relevant TRA; and
- Ensuring that any requirements related to time sensitive services and/or utilities are addressed through lease agreements (e.g., timeliness of repairs, SLAs).

Ontario Internal Audit

The Ontario Internal Audit Division is responsible for:

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

4. ACKNOWLEDGEMENTS

4.1 Editors

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

4.2 Contributors

Full Name	Cluster, Ministry and/or Area
Raj Mistry	MGS Corporate Security Branch

4.3 Consultations

The following individuals were consulted:

Charlotte Ward, MGS CSB

Pat Antliff, MGS CSB

Mano Pancharatnam, MGS CSB

Jim Patterson, MGS CSB

Andrea Howat, MGS Facilities Management

4.4 Reviewers

The following individuals and/or groups have reviewed this standard:

John Lorenc	Manager, IPC, MGS CSB
Mathew Smith	Physical Security, ITS
Krystyna Paterson	Section Manager, Office of the Ontario Fire Marshall
Chris Riddell	Strategic Account Manager, Sungard
Fraser Duff	Security Architect, Health Services I&IT Cluster
David Wilkins	Security Architect, Health Services I&IT Cluster

Edwin Lang	Technology Architect, Health Services I&IT Cluster
Colin Easton	Technology/Security Architect, Corporate Architecture Branch
Production/Server Support	Health Services I&IT Cluster
Review Team	Ontario Internal Audit

5. DEFINITIONS

Access: Entry to an electronic network or physical facility provided to employees and other authorized individuals on or outside government premises.

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

Authorize: To grant permission to access resources according to a predefined approval scheme.

Astragal: A strip of material secured to a door that is intended to deter attacks that rely upon manipulation of a latch or bolt.

Availability: The degree of readiness expected of information systems and IT resources to deliver an appropriate and timely level of service, regardless of circumstances.

CCTV: Closed-circuit Television (CCTV) is the use of video cameras and equipment to produce and transmit a video signal for limited use and viewing, often for security/surveillance purposes.

Confidentiality: The result of safeguards enforcing access to information consistent with the sensitivity of information, competitive position, and legislative requirements (e.g., FIPPA, PIPEDA, PHIPA).

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

Glazing: The transparent component of a window that passes light; can be constructed in numerous ways from various materials (e.g., glass, plastic, ceramic etc.).

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

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

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

NFPA: National Fire Protection Association (United States).

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: A specific program or service within a Ministry.

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

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

Risk: A potential opportunity or threat that may impact on an organization’s ability to meet its business objectives.

Safeguard: A protective and precautionary measure to prevent a security threat from causing impact and/or a security incident from happening.

Sensitive Information: Information that if released without authorization would cause harm, embarrassment, or unfair economic advantage, such as a breach of confidentiality of personal information, unauthorized modification of financial data, or a release of pre-budget information and strategic planning documents (or as determined by ISPC).

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.

Zone: A formally identified area within a facility with specific security requirements, minimum safeguards, defined interface points, and interface requirements.

6. APPENDIX A: ADDITIONAL 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

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)**
	No impact to existing GO-ITS	

Impacts to Existing Environments

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

Application(s) or Infrastructure impacted	Describe Impact	Recommended Action (or page number where details can be found)
Data Centres	Adherence to these security requirements will reduce the risks to Government I&IT resources. Some of the physical safeguards in this document and operational requirements will increase the complexity of data center layouts, and costs for operating facilities. To ensure cost and impact is kept reasonable with regard to security needs, this document recommends linking context-sensitive Threat/Risk Assessment (TRA) results and the construction and/or operation of data centres. This effort was conducted in consultation with TRA subject matter experts within the Corporate Security Branch (CSB). This should permit for a balance of considerations and application of the safeguards most appropriate for a given facility. The use of security zones will limit the application of some safeguards to specific areas. Facilities that do not support all zones may not require all safeguards indicated in this standard. Considered use of security and high security zones should limit the number of facilities and areas where robust measures are required, reducing cost and complexity. Where possible, some safeguards have been indicated as applying to new construction. Some techniques have been separately indicated as appropriate for existing facilities. The impact in terms of operations, cost, and complexity should be reduced by applying only those processes and safeguards best suited for each type of environment. Potential for privacy impact has been noted in some areas of this document, with guidance for addressing possible issues (e.g., disclosure of activity monitoring in a public area, and documentation of data retention).	Compliance with these requirements

References

ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management* (2005)

GO-ITS 25.0 *General Security Requirements*, Corporate Security Branch, Ministry of Government Services (2008)

Information Security and Privacy Classification Policy, Officer of the Corporate Chief Privacy Officer, Ministry of Government Services (2005)

Operational Security Standard on Physical Security, Treasury Board of Canada Secretariat (2004)

G1-017 Hardware, Royal Canadian Mounted Police (1985)

G1-018 Doors and Frames, Royal Canadian Mounted Police (1985)

G1-026 Guide to the Application of Physical Security Zones, Royal Canadian Mounted Police (2005)

G1-031 Physical Protection of Computer Servers, Royal Canadian Mounted Police (2008)

Document History

Drafted, June 2008

Revised, March 2009

- Revised linkage to TRA process and ISPC requirements
- Reviewed document with stakeholders (per sections 4.3 and 4.4) and incorporated input
- Enhanced linkage to external guidance and standards (e.g., ISO/IEC, GoC)
- Developed concept of enhanced safeguards
- Incorporated initial input from CSB TRA and Security Design groups
- For review and approval by IT Standards Council and Architecture Review Board
- Revised original/draft version of zone control/safeguard/functions matrix

Approved by IT Standards Council, March 2009

Revised, April 2009

- Simplified wording in scope section regarding data centre definition (pg. 6)
- Simplified wording regarding contact with CSB if standard is not clear (pg. 6)
- Made wording more clear regarding minimum standard applicability (pg. 6)
- Made wording regarding DR/BCP scope more clear (pg. 6)
- Made wording more clear regarding minimum standard applicability (pg. 8)
- Made wording more clear regarding electronic access control testing (pg. 14)
- Indicated preference for facility location in Ontario (pg. 15)
- Enhanced and expanded facility location to address additional threats (pg. 15)
- Enhanced facility location wording with reference to fire/emergency services (pg. 15)
- Enhanced wording to include “hold open” alarms (pg. 16)
- Narrowed exterior door requirements for metal doors and frames (pg. 19)
- Enhanced wording to include “hold open” alarms (pg. 19)
- All secure zone requirements when enhanced safeguards required (pg. 20)
- Enhanced wording to include a metal door frame requirement (pg. 20)
- Enhanced wording for astragal requirements without centre mullion (pg. 21)
- Enhanced wording to include signage requirement for chemical suppression (pg. 23)
- Enhanced wording to include “hold open” alarms (pg. 25)
- Made wording more clear regarding privacy impact and documentation (p. 30)
- Enhanced wording to make managed environment requirement more clear (p. 33)
- Made wording more clear as to negotiation of generator support (p. 34)
- Made wording more clear for Data Center / Facility Management event reporting (p. 37)
- Enhanced wording for Data Center / Facility Management BCP, DR guidance (p. 37)
- Enhanced wording for Data Center / Facility Management electricity, fuel role (p. 37)
- Enhanced wording for Program Manager TRA, BCP, and DR responsibilities (p. 38)
- Updated list of consulted individuals and reviewers (p. 40)

- Added definition for “CCTV” (pg. 42)
- Enhanced wording of “safeguard” and “sensitivity” definitions (pg. 43)
- Added information in impact section regarding privacy documentation (pg. 45)

Revised, May 2009

- Errata compiled by Internal Audit addressed

Revised, March 2012

- Organizational updates
- Role updates
- Hyperlinks and references updated
- Minor errata addressed

Revised, November 2012

- Hyperlink updated
- Approval information updated

Copyright

© Queen's Printer for Ontario 2012