Information Protection Security Controls for Classified Data (IPSC)

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the information protection security controls for classified information and should be used by those who are planning, developing, or implementing information processing services using data classification.

Table of Contents

1. Introduction to Information Classification ... 3
1.1. Purpose of the IPSC ... 3
1.2. Description of Data Classification ... 3
1.3. Assigning Data Classifications ... 3
1.4. Downgrading Data Classifications ... 4
1.5. Classification levels ... 4
1.6. Data Classification during Acquisition and Development or Major Changes ... 5
1.7. Data Classification in Supplier Agreements ... 5
1.8. Labelling and Handling Classified Data ... 5
1.9. Use of Cryptography ... 5
1.10. Note on Compliance with Acts ... 5
1.11. Glossary ... 6
2. Access Control (Logical) ... 6
2.1. Management of User Identities and Access ... 6
2.2. User Identification ... 6
2.3. Authentication ... 7
2.4. Account Passwords ... 8
2.5. User Access Control ... 9
2.6. Service Accounts ... 9
2.7. Auditing ... 9
2.8. Appropriate Use Banner ... 10
3. Electronic — Storage ... 10
3.1. Location of Information ... 10
3.2. Device Configuration ... 12
3.3. Anti-Virus Software ... 12
3.4. Security Patching ... 12
3.5. Backups ... 12
3.6. Email ... 13
3.7. Transportation of electronic media on removable storage ... 13
4. Information Transfer ... 14
4.1. Agreements on Information Transfer ... 14
4.2. Transfer within the Electronic Security Perimeter ... 14
4.3. Transfer across the Electronic Security Perimeter ... 14

5. Network Zones 15
5.1. High-level Overview of Internal Zones 15
5.2. Enterprise Edge Network 17
5.3. Integrated Service Network 17
5.4. Core Network 17
5.5. Management Network 17
5.6. Wireless 17
6. Physical Security Controls 18
6.1. Data Centers 18
6.1.1. Access Control (Physical) 18
6.1.2. Perimeter Security 18
6.1.3. Wiring Closets 19
6.1.4. Utility Controls 19
6.1.5. Environmental Controls 19
6.2. Work Areas where Sensitive Information is Processed 19
6.2.1. Access to Work Areas where Sensitive Information is Processes 19
6.2.2. File Security (Physical/Paper) 19
6.3. Physical Transportation of Information 20
7. Retention / Disposal / Redeployment — Deploying Computers 20
7.1. Redeploying Computers 20
7.2. Disposal of Electronic Information on Storage Media 21
8. Cloud Computing Security 21
8.1. Policy Summary 21

Appendix 22
Network / Application Login Banner 22
Email Disclaimer 22

1. Introduction to Information Classification

1.1. Purpose of the IPSC

This document brings together all of the security controls relating to data classification at the Government of Saskatchewan ("GoS") into a single consolidated location. This is not the entirety of the GoS information security policy, standards, and specifications framework but, rather, a view of it intended to be useful for personnel developing or implementing information processing services that use data classification. Where strict clarity and accuracy is required, always refer to the authoritative documentation, if applicable, referenced and linked to in each section of this document. All documentation maintained by the Information Security Branch can be found on the *IT Security Services TaskRoom* web page.

1.2. Description of Data Classification

A data classification scheme is a model of security categories that information can be assigned to, where each category has different levels of criticality and/or financial value, which in turn drives the requirements for confidentiality, integrity, and availability.

Data classifications are used to provide people who deal with sensitive information a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security controls that apply to all information within the category facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

The Government of Saskatchewan uses a positive-classification model, where information is by default considered to be non-sensitive unless classified otherwise. The general rule when assigning a security classification to an identified information asset is to classify it at the lowest reasonable level (after taking criticality and asset value into account) in order to avoid unnecessary protection costs.

In determining the level of sensitivity, Information Owners must consider that, in some cases, aggregated information can be more sensitive than a smaller subset or individual record. For a simple example, having a list of home phone numbers does not create personally identifiable information unless it is combined with the associated names.

1.3. Assigning Data Classifications

Information Owners have the responsibility and decision-making authority for information throughout its life cycle including regulating its use and protection through the assignment of a classification.

- For a high-level definition of Information Owners and their responsibilities, see the "Information Owner" section in the *Organization of Information Security Policy*.
- To help understand the value of information and apply the appropriate security controls, Information Owners should use *A Guide for Information Protection Classification*.
- To determine and communicate the classification of information for an IT project or application, Information Owners should complete a *Statement of Sensitivity*. The Statement of Sensitivity also informs other information security activities including, though not necessarily limited to, refining security requirements, threat/risk assessments, and privacy impact assessments.
- The "Information Classification" section of the *Asset Management Security Standards* defines how information that has been classified is inventoried.

1.4. Downgrading Data Classifications

The data classification of information assets can change over time. For example, a particular piece of information may cease to be sensitive after the drafting stage is complete and it has been released to the public. These situations need to be considered as over-classification can lead to the use of unnecessary security controls (and their associated costs), while under-classification can endanger the secure achievement of government objectives.

Information should have a data classification only for the period of time that it requires protection, after which it should be downgraded or declassified. This ensures that information that requires security classification receive the attention they need, which contributes to the overall security of the information security program.

1.5. Classification levels

A Guide for Information Protection Classification should be used to help understand the value of information and the correct data classification level.

The table below outlines a summary of the classification levels in use at the Government of Saskatchewan.

	Description
Public	**Public Sector Security Classification Guideline**: Unclassified, public information. Internal communications. **Saskatchewan's Information Protection Classification**: Will not result in injury to individuals, governments or private sector institutions.
Class C	**Public Sector Security Classification Guideline**: Low sensitivity. Information that is only sensitive outside the government and is generally available to employees and approved non-employees. **Saskatchewan's Information Protection Classification**: Could reasonably be expected to cause significant injury to individuals or enterprises within limited: financial losses, impact in services/performance levels, and reputation.
Class B	**Public Sector Security Classification Guideline**: Medium sensitivity. Information that is sensitive within the government and is intended for use only by specific groups of employees. **Saskatchewan's Information Protection Classification**: Could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government, financial loss, legal action, damage to partnerships, relationships and reputations.
Class A	**Public Sector Security Classification Guideline**: High sensitivity. Information that is extremely sensitive, of highest value to the government and intended for use by named individuals (positions) only. Documents that can be used to create an identity. **Saskatchewan's Information Protection Classification**: Could reasonably be expected to cause extremely serious personal or enterprise injury, including: significant financial loss, loss of life or public safety, social hardship, major political or economic impact.

1.6. Data Classification during Acquisition and Development or Major Changes

To support the requirements of the *System Acquisition, Development and Maintenance Security Policy* when developing, acquiring, or making major changes to an information system, Information Owners and Service Owners must:

- prepare a *Statement of Sensitivity* to determine the confidentiality, integrity, and availability requirements of the system;
- apply security controls based on a Threat and Risk Assessment;
- document the roles and responsibilities related to information system security management;
- document specific procedures and standards used to mitigate risks and safeguard the information systems; and
- document communication procedures for security-related events and incidents.

1.7. Data Classification in Supplier Agreements

To support the requirements of the *Supplier Relationships Security Standards*:

- security controls must be implemented before a supplier is allowed to access the government's information assets, with control details provided in the *Supplier Relationship Security Standards* referenced above; and
- agreements must be established to document both parties' obligations to fulfil relevant information security requirements, with terms provided in the *Supplier Relationship Security Standards* referenced above.

1.8. Labelling and Handling Classified Data

The "Information Classification" section of the *Asset Management Security Standards* defines how information with a data classification is labelled and handled.

1.9. Use of Cryptography

The IPSC does not generally contain specific details on compliant cryptographic implementation. Always refer to the most current version of policy, standards, and specifications document as listed below:

- *Cryptography Security Policy*;
- *Cryptography Security Standards*;
- *Cryptography Security Specifications*.

1.10. Note on Compliance with Acts

In addition to the requirements in the IPSC, GoS is also required to maintain compliance with external requirements, including:

- *Archives and Public Records Management Act*;
- *Freedom of Information and Protection of Privacy Act*; and
- *Saskatchewan Records Management Policy, Guidelines, and Tools*.

1.11. Glossary

For the definitions of any security-specific or GoS-specific terms, refer to the *Information Security Glossary*. A few terms occur frequently in the IPSC and have their definitions repeated here for convenience:

- **Electronic Security Perimeter**: An electronic security perimeter is the logical or physical demarcation point between networks of differing security protection requirements, ownership or governance. The Government of Saskatchewan Electronic Security Perimeter specifically is the logical group of managed computing assets with access to the Government of Saskatchewan managed network, including by managed VPN.
- **Network Workstation**: A computer running a general-purpose end-user operating system, such as Microsoft Windows 10, connected directly to the GoS network and leveraging GoS central IT infrastructure.
- **Personal Health Information**: Defined in the *Health Information Protection Act.*
- **Personal Information**: Defined in the Freedom of Information Protection of Privacy Act.

2. Access Control (Logical)

2.1. Management of User Identities and Access

As per the *Access Control Security Policy*, to ensure authorized users access appropriate resources and to prevent unauthorized access to systems and services, there must be a formal user registration and de-registration process and a provisioning system to manage user identities and access.

2.2. User Identification

User identification is how a user is recognized or identified by a device or a system, using a unique symbol or character string for each specific user.

	Requirements
Public	Anonymous access is permitted.
Class C **Class B** **Class A**	User identification requirements for all other classes: • a unique system/network user ID, identifiable to the employee; • inactive ID's and access control lists are updated and/or unused user ID's disabled immediately upon termination of employee; • all users must be authorized by ministry Service Approvers before access permissions are granted to government assets; • guest and shared accounts must not be enabled; • administrator account must be following the naming conventions as developed by the AMA team; and • any service-based or administrative account not in use must be disabled or removed.

2.3. Authentication

Authentication is the act of verifying the identity of a user or device to the network or an application, often as a prerequisite to allowing access to resources in an information system.

	Description
Public	*If* authentication is used, such as for the purpose of retaining user personalization or configuration, then the authentication used: • should accommodate authentication information passing in a secure manner from endpoint to authentication source; • must support an electronic credential for the handing of non-sensitive information and must use either: o a simple password; or o an assertion from another authentication service that uses any credential strength and authentication method and that is deemed by the relying party to be an authorized and trusted service.
Class C	User authentication requirements for Class C: • all users and devices must be authorized and use encrypted authentication; • single-factor encrypted authentication must be used for local and remote network access; • multi-factor authentication (MFA) may be used; If MFA is used, it should support an electronic credential intended to achieve a medium credential strength and should use either: o A password that follows the requirements specified in Section 3.2, Password Standards, within the *Access Control Security Standards* document; o An assertion from another authentication service that uses a comparable or higher credential strength and authentication method (Class C to A); or o A software or hardware based MFA system approved by the Information Technology Division that may or may not conform to the higher credential strength (Class B or A) standards • must accommodate authentication information passing in a secure manner from endpoint to authentication source; and • network accounts must be disabled after 3 invalid login attempts and manually enabled by the service desk.
Class B	User authentication requirements for Class B: • all users and devices must be authorized and use encrypted authentication; • single-factor encrypted authentication for local and remote network access, multi-factor authentication may also be used, and if used must support an electronic credential intended to achieve a high credential strength and that must use either: o A password that follows the requirements specified in Section 3.2, Password Standards, within the *Access Control Security Standards* document; o An assertion from another authentication service that uses a comparable or higher credential strength and authentication method (Class B to A); or o A software or hardware based multifactor authentication system approved by the Information Technology Division and using a key and cryptographic mechanism validated at FIPS 140-2 Level 1 at a minimum and requires the use of either (a) a password or biometric by the individual to activate the cryptographic mechanism; or (b) a password in combination with the cryptographic mechanism in the same authentication protocol; and follows the requirements specified in Section 3.2, Password Standards, within the *Access Control Security Standards* document; • authentication between the application front-end and the authentication source must be in a secure manner; • single-factor authentication for local network access is permitted; • two-factor encrypted authentication *(see Class A for details)* is required for access from outside the GoS Electronic Security Perimeter; and • network accounts must be disabled after 3 invalid login attempts and manually enabled by the service desk.

	Description
Class A	User authentication requirements for Class A: • all users and devices must be authorized, and use encrypted multi-factor authentication (MFA) for access by both users and for support and administration purposes, that: o achieves a very high credential strength; o uses a cryptographic token using a key and cryptographic mechanism validated at FIPS 140-2 Level 1 at a minimum, and that is approved by the Information Technology Division; o requires the use of either (a) a password or biometric by the individual to activate the cryptographic mechanism; or (b) a password in combination with the cryptographic mechanism in the same authentication protocol; and o follows the requirements specified in Section 3.2, Password Standards, within the *Access Control Security Standards* document. • authentication between the application front-end and the authentication source must be in a secure manner; • remote access from outside of the GoS Electronic Security Perimeter is not permitted; and • network accounts must be disabled after 3 invalid login attempts and manually enabled by the service desk.

2.4. Account Passwords

	Description
Public	If authentication is implemented, then the authentication requirements as outlined in Class C must be implemented.
Class C **Class B** **Class A**	Password requirements for all other classes: • Passwords must be a minimum 8 characters; • Use of a complex password (alphanumeric characters, special characters, upper and lowercase letters and non-dictionary words) is required; • Passwords must not contain the user ID as part of the password; • Passwords must be set to expire within a maximum of 90 days; • Passwords must be stored and transmitted in an encrypted format; • Passwords must be changed at first login; • Password history: last 7 passwords may not be reused • All user accounts must have a password; • Password changes and resets require challenge/response to user identity.

Where challenge/response method is mentioned to validate a user's identity, it consists of a user being required to provide a question (challenge) and a secret answer (response) upon account creation. When a password reset is requested for a specific user account, the user would be required to provide the response in answer to the challenge before the password reset would occur. A self-serve password change/reset, which validates the user identity, may also be used.

2.5. User Access Control

User access controls are means to ensure that access to any information system resource is authorized and restricted based on business and security requirements.

	Description
Public	No Access Controls requirements for Public.
Class C **Class B** **Class A**	Access Control requirements for all other classes: • directory and file level security are required (file level security is directed by the Information Owner or ministry through the use of a Service Request); • user access must be approved by ministry personnel authorized by Information Owners as reflected in job duties; • user access permissions including user ID's must be reviewed regularly; • computers must be logged off the network or application at the end of a shift; and • computers must be locked by the user when away from the computer and a locking screen saver must be automatically invoked after 20 minutes of computer inactivity.

2.6. Service Accounts

Service accounts are required for servers providing services to GoS affecting all levels of data classification. As the stability of these accounts impacts the availability of services they may fall outside of the standard account definition. Minimum security specifications that recognize the difference from user accounts are provided in the *Access Control Specifications* for local Windows service accounts, Group Managed and Managed service accounts for Windows, Unix service accounts, and Unix sudo privileged access.

2.7. Auditing

Auditing refers to independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established standards, policies and operational procedures. This is often accomplished through the use of audit logs which are a chronological record of system activities and includes records of system accesses and operations performed in a given period.

	Description
Public	No Auditing requirements for Public.
Class C	Auditing requirements for Class C: • all successful and failed network access authentication attempts are logged and audited, at a level sufficient to permit security auditing; • file and directory permissions are reported to ministries on an as-requested basis for Information Owners to review; • all changes or additions of user ID's must be documented; • all changes to file and directory permissions are documented in the service request processing toolchain; and • access to system audit logs is limited only to authorized users.

	Description
Class B	Auditing requirements for Class B: • all successful and failed network access authentication attempts are logged and audited, at a level sufficient to permit security auditing; • file and directory permissions are reported to ministries on an as-requested basis for Information Owners to review; • all changes or additions of user ID's must be documented; • all changes to file and directory permissions are documented in the service request processing toolchain; and • access to system audit logs is limited only to authorized users.
Class A	Auditing requirements for Class A: • all access and modifications to information must be logged at a level sufficient to permit security auditing; • all successful and failed network access authentication attempts must be logged at a level sufficient to permit security auditing; • file and directory permissions reported to ministries on an as-requested basis for Information Owners to review; • all changes to file and directory permissions must be logged at a level sufficient to permit security auditing; • all changes or additions of user ID's must be documented; and • access to system audit logs is limited only to authorized users.

2.8. Appropriate Use Banner

	Description
Public	No Appropriate Use banner requirements for Public.
Class C	For web sites containing Class C information, Security, Privacy and Disclaimer Policies must be present.
Class B **Class A**	Network and/or application login or sign-on banner is required for remote access – see Appendix for example.

3. Electronic — Storage

3.1. Location of Information

The tables below outline the requirements for the location of information storage depending on the classification level.

	Description
Public	Information storage requirements for Public: • systems classified as Public are not permitted to contain personal information; • all Public data as-rest, including data backups, **should** be stored in Canada at all times (data sovereignty requirements may exist and should be confirmed with the Information Owner); • all system architecture housing Public data **should** ensure that all GoS data remains separate from the data of other customers; • approved server storage devices must be located in a secure room; • network workstations may house Public information; • mobile devices may house Public information as per the *Mobile Wireless Device Policy*; and • removable storage devices may house Public information as per the Government of Saskatchewan Removable Media Policy.

	Description
Class C	Information storage requirements for Class C: • any Class C systems containing Personally Identifiable Information (PII) **must** ensure that: o all data at-rest, including data backups, **must** remain in Canada at all times; o to the extent possible and feasible, all data in-transit, including data backups, **must** remain in Canada at all times. • all Class C data at-rest, including data backups, **should** be stored in Canada at all times (data sovereignty requirements may exist and should be confirmed with the Information Owner); • all system architecture housing Class C data **must** ensure that all GoS data remains separate from the data of other customers; • network workstations may house Class C information; • mobile devices may house Class C information as per the *Mobile Wireless Device Policy*; • removable storage devices containing Class C information must be in compliance with the Government of Saskatchewan Removable Media Policy.
Class B	Information storage requirements for Class B: • any Class B systems containing Personally Identifiable Information (PII) **must** ensure that: o all data at-rest, including data backups, **must** remain in Canada at all times; o to the extent possible and feasible, all data in-transit, including data backups, **must** remain in Canada at all times. • all Class B data at-rest, including data backups, **should** be stored in Canada at all times (data sovereignty requirements may exist and should be confirmed with the Information Owner); • all data at-rest and in-transit, and which is located outside of the GoS electronic security perimeter, including data backups, **must** be encrypted end-to-end at all times; • all system architecture housing Class B data **must** ensure that all GoS data remains separate from the data of other customers; • network workstations may house Class B information in an approved and supported, secure, containerized system; • mobile devices may house Class B information as per the *Mobile Wireless Device Policy*; and • removable storage devices containing Class B information must be in compliance with the Government of Saskatchewan Removable Media Policy.
Class A	Information storage requirements for Class A: • any Class A systems containing Personally Identifiable Information (PII) **must** ensure that: o all data at-rest, including data backups, **must** remain in Canada at all times; o to the extent possible and feasible, all data in-transit, including data backups, **must** remain in Canada at all times. • all data at-rest, including data backups, **should** be stored in Canada at all times (data sovereignty requirements may exist and should be confirmed with the Information Owner); • all data at-rest and in-transit, including data backups, **must** be encrypted end-to-end at all times; • all system architecture housing Class A data **must** ensure that all GoS data remains separate from the data of other customers; • network workstations and mobile devices **must not** house any Class A information outside of an approved and supported, secure, containerized system unless explicitly approved by the Ministry's Permanent Head and the Ministry of Central Services Deputy Minister: o if so, it must be encrypted and compliant with the *Mobile Wireless Device Policy*; and • removable storage devices **must not** house any Class A information unless explicitly approved by the Ministry's Permanent Head and the Deputy Minister of the Ministry of Central Services: o if so, it must be encrypted and must be in compliance with the Government of Saskatchewan Removable Media Policy.

3.2. Device Configuration

	Description
Public	Servers must be hardened according to applicable Government policies, standards and specifications. Specifically, but not exclusively, all server configuration ports must be disabled if not in use.
Class C **Class B** **Class A**	Device configuration requirements for all other classes: • only authorized devices are allowed on the network; • information technology equipment (servers, workstations, mobile devices, PDAs, etc.) must be hardened according to applicable Government policies, standards and specifications; specifically, but not exclusively, all server configuration ports must be disabled if not in use; and • workstations must be configured to prevent installation of unauthorized software and/or configuration.

Authorized software or hardware is a standard service catalogue item, or a custom IT solution (hardware or software) provided by Central Services and is compliant with Government of Saskatchewan policies and standards or an approved exception using the Risk Management Decision Item (RMDI) process.

3.3. Anti-Virus Software

	Description
Public	Up-to-date anti-virus software with current signatures configured for on-access scanning is required.
Class C **Class B** **Class A**	Anti-virus requirements for all other classes: • up-to date anti-virus and anti-spyware detection software is required; • it must be centrally administered and installed on all computing devices (where technologically feasible) with current signatures and configured, where appropriate, for on access scanning and automatic deployment of signature files; and • anti-virus software and signature updates must be tested before being deployed.

3.4. Security Patching

	Description
All Classes	Security patches for operating systems, applications, and server and network firmware must be tested and deployed where applicable in compliance with the approved IT Division of Central Services Change Management Process.

3.5. Backups

	Description
Public	Current image of public websites must be maintained to permit rapid restoration.
Class C/B/A	Requirements for backups: • backup media must be in encrypted format; • backup media must be transported and stored securely offsite; and • information backup strategy must be in accordance with internal business requirements and restorations, as well as records management requirements; • contracts to provide backups must include confidentiality/privacy clauses; • all secure offsite facilities must be accessible 24/7; • all data at-rest, including data backups, must meet the requirements of the Electronic — Storage section.

3.6. Email

	Description
Public	No Email requirements for Public.
Class C	Email requirements for Class C: • all email sent must incorporate standard email disclaimer as specified in Section 9.2, Email Disclaimer, within this document; • email proxy/filter must be used that prevents a direct connection of the email server to the Internet and blocks malicious attachments; and • email containing Personal and Personal Health information must be encrypted using a method approved by the Information Security Branch and must not be sent outside of the GoS Electronic Security Perimeter.
Class B	Email requirements for Class B: • all email sent must incorporate standard email disclaimer as specified in Section 9.2, Email Disclaimer, within this document; • an email proxy/filter that prevents a direct connection of the email server to the Internet and blocks malicious attachments must be used; • email containing Personal and Personal Health information must be encrypted using a method approved by the Information Security Branch and must not be sent outside of the GoS Electronic Security Perimeter, and • email containing Class B information sent outside of government must use a secure encryption method approved by the Information Security Branch (which currently includes the FIPS 140-2 standard).
Class A	Email requirements for Class A: • all email sent must incorporate standard email disclaimer as specified in Section 9.2, Email Disclaimer, within this document; • email proxy/filter must be used that prevents a direct connection of the email server to the Internet and blocks malicious attachments; • email containing Personal and Personal Health information must be encrypted using a method approved by the Information Security Branch and must **not** be sent outside of the GoS Electronic Security Perimeter; • Email containing Class A information must **not** be sent outside of the GoS Electronic Security Perimeter and, when sent within the GoS Electronic Security perimeter, must be encrypted using a method approved by the Information Security Branch .

3.7. Transportation of electronic media on removable storage

	Description
Public/ Class C	Transportation requirements for Class C and Public: • Use of regular envelopes and/or interoffice envelopes is permitted.
Class B	Transportation requirements for Class B: • Tamper evident packaging (e.g. double-sealed envelope with inside envelope signed to reveal evidence of tampering is required.
Class A	Transportation requirements for Class A: • tamper evident packaging (e.g. double-sealed envelope with inside envelope signed to reveal evidence of tampering is required; • transfer must be performed with business authorized staff or courier using a locked case tagged with forwarding or return office address; and • files or devices must not be left unattended in non-secured areas.

4. Information Transfer

Where authentication credentials are mentioned in this section, they always require a secure encryption method approved by the Information Security Branch (which currently includes the FIPS 140-2 standard). See Section 2.3, Authentication, within this document for additional information.

4.1. Agreements on Information Transfer

The *Information Transfer Security Policy* mandates requirements for electronic transfer of information across the electronic security perimeter of the Government of Saskatchewan network of all classifications of data, summarized as:

- Data Classification is required;
- responsibility for security lies with the sender; and
- compliant formal agreements on the information transfer must be in place (requirements for which are defined in the *Communications and Network Security Standards)*.

4.2. Transfer within the Electronic Security Perimeter

	Description
Public **Class C**	Requirements for Public: • transfer within the GoS Electronic Security Perimeter is permitted; and • no encryption of transmissions is mandated within the Electronic Security Perimeter.
Class B	Requirements for Class B: • transfer within the GoS Electronic Security Perimeter is permitted; and • all data at-rest and in-transit must be encrypted end-to-end at all times using a secure encryption method approved by the Information Security Branch (which currently includes the FIPS 140-2 standard).
Class A	Requirements for Class A: • transfer within the GoS Electronic Security Perimeter is permitted; and • all data at-rest and in-transit must be encrypted end-to-end at all times using a secure encryption method approved by the Information Security Branch (which currently includes the FIPS 140-2 standard).

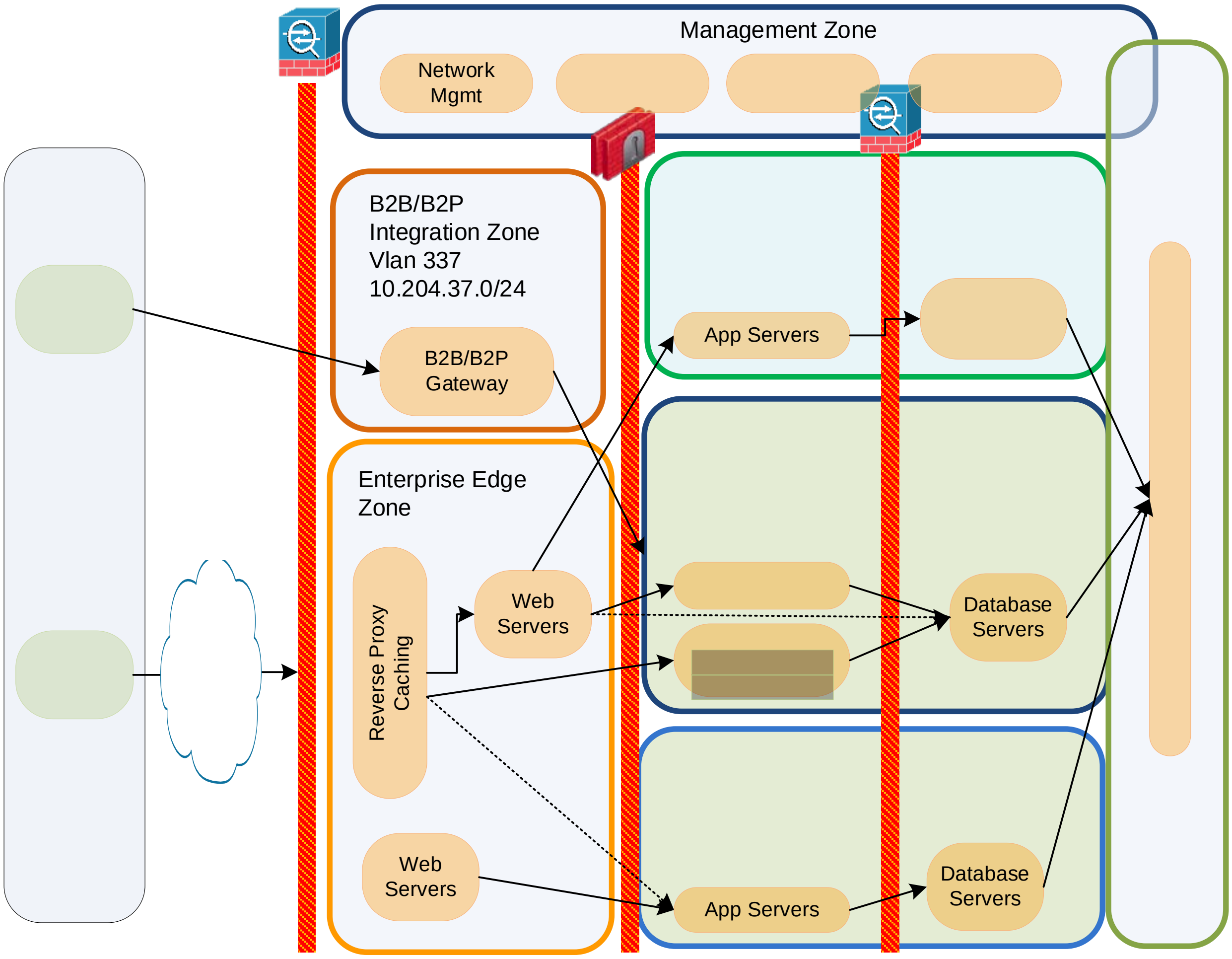
4.3. Transfer across the Electronic Security Perimeter

	Description
Public	Requirements for Public: • transfer across the GoS Electronic Security Perimeter is permitted; and • no encryption of transmissions is mandated for data.
Class C	Requirements for Class C: • transfer across the GoS Electronic Security Perimeter is permitted; and • Class C data transmissions containing Personal or Personal Health information require a secure encryption method approved by the Information Security Branch (which currently includes the FIPS 140-2 standard); otherwise, encryption of data is not required.

	Description
Class B	Requirements for Class B: • transfer across the GoS Electronic Security Perimeter is permitted; and • Class B data transmissions require a secure encryption method approved by the Information Security Branch (which currently includes the FIPS 140-2 standard).
Class A	Requirements for Class A: • transfer outside of GoS Electronic Security Perimeter is **not** permitted.

5. Network Zones

5.1. High-level Overview of Internal Zones

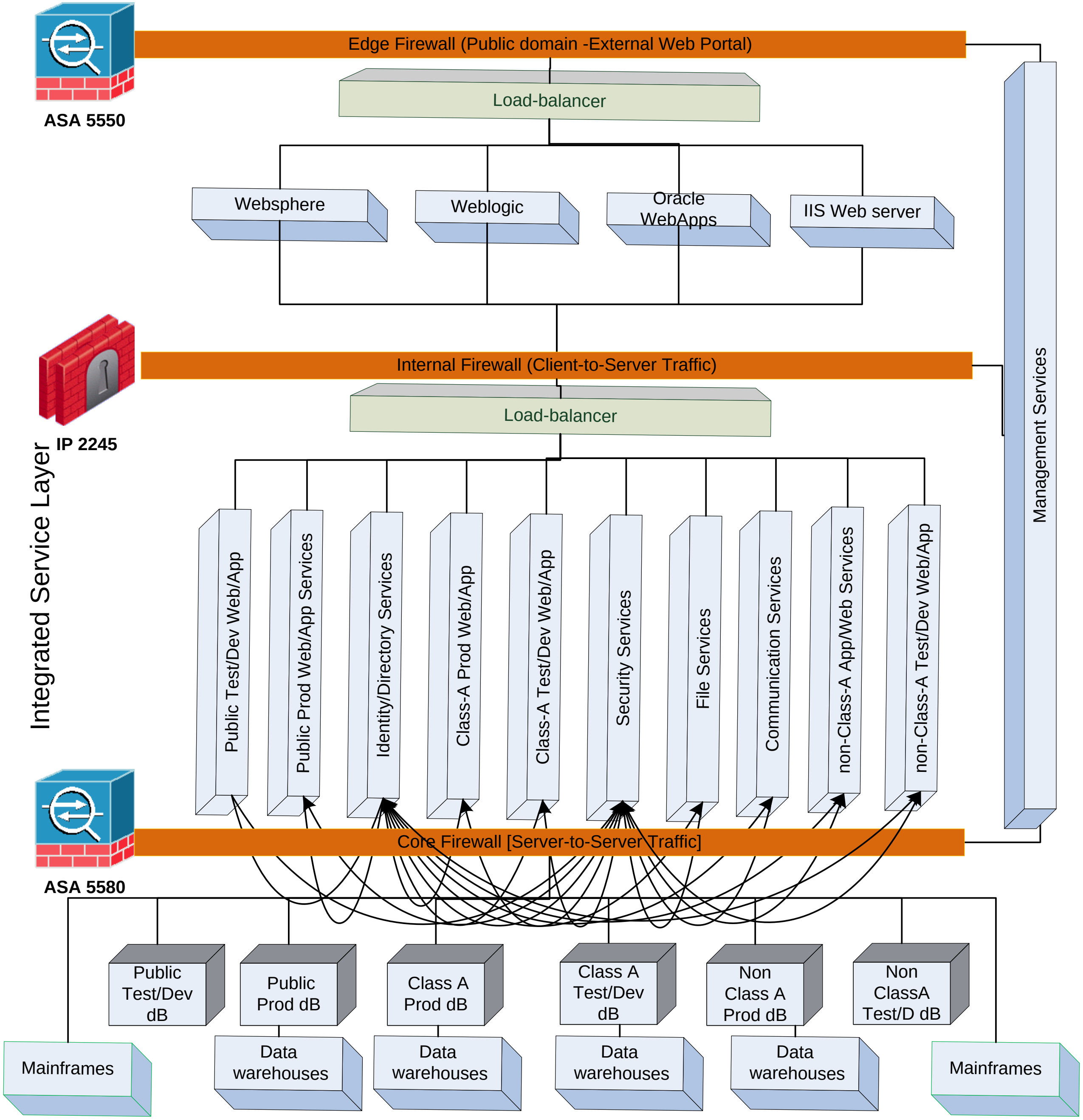


This is a high-level view of how the internal zones of the GoS datacenter are designed:

- **Public Internet Perimeter Zone** – Access to services hosted on the Enterprise Edge only.
- **Enterprise Edge Perimeter Zone** – This area isolates the GoS-internal network from the Internet/public domain. It hosts services for public domain. Servers Include: Public domain web portals, Weblogic, Websphere servers as well as proxy servers for internal servers.
- **B2B/B2P Integration Zone** – Provides partner access and integration. Hosts B2B or B2P Gateways/servers.

- **Internal Network Perimeter "Integrated Service" Zone** – This area hosts enterprise portals and application servers. Remote access VPN authentication required for telecommuters to use services hosted on the internal network.
- **Management Zone** – Provides management access to network devices/applications: Network Management, Server Support, Application/Developer, Service Desk/AMA.
- **Internal Core Network Perimeter Zone** – This is the network core, it provides another layer of security to critical network services. No direct access to the Internet.

The following diagram illustrates the traffic flow between different network service areas or sub-zones:



5.2. Enterprise Edge Network

- Class A servers cannot offer any direct services to remote users outside of the GoS Electronic Security Perimeter. If remote access is required, VPN through either the Enterprise Edge or B2P/B2B Integration zones (depending on whether it is an individual user or a business partner) must be used to extend the GoS Electronic Security Perimeter.
- Specifically, but not exclusively, site-to-site VPNs must terminate at the B2B/B2P zone and provide access only to either a server located in that zone or to a gateway located in that zone that permits access to other zones only after enforcing user-level access control (i.e., a "jump box").

5.3. Integrated Service Network

Servers must be housed in the appropriate application zones for their Classification within the Integrated Service Network.

5.4. Core Network

- No direct access to Class A or B data will be allowed without being routed through an authorized intermediary;
- Test and Dev zones must not have access to Production Zones;
- Database servers must be housed in the appropriate database zones within the Core Network.

5.5. Management Network

Privileged administrative access to logical zones can only be initiated from the Management Network. Specifically, but not exclusively, the Storage Subsystem configuration capability is exposed *only* to the Management Network. The Management Network must not host any services accessible from other zones. The Management Network may host services that poll (egress method) but not services that that are accessed directly (ingress method).

5.6. Wireless

As per the *Wireless Networking Security Policy*, only the official GoS Central Services ITD supported wireless service may be used to connect wirelessly directly to the GoS network. Individuals and ministries must not independently deploy access points. ITD will work with any ministry wishing to establish or expand WLAN networking in their area.

6. Physical Security Controls

The summarized controls in this section support the requirements of the *Physical and Environmental Security Policy* and *Physical and Environmental Standards* for data centers and work areas.

6.1. Data Centers

6.1.1. Access Control (Physical)

	Description
All Classes	Access control requirements for data centers housing all classes of data: • all employees and other authorized personnel must wear visible identification; • access is permitted for authorized individuals only; o visitors must only be allowed access for specific and authorized purposes, must wear visible identification badges or tags of a different colour than personnel, and must be escorted by authorized personnel at all times; o external party support personnel may be granted access only when required and their access must be authorized and monitored; • individual access authentication via access card/key fob is required to enter Computer Data Centers; o proper access card/key fob control must be maintained i.e. log for all access tokens issued/returned; o an audit log of all access and attempted access (including by authorized visitors) is maintained and made available to GoS upon request; and o access rights must be regularly reviewed, updated, and revoked when necessary; • personnel must notify security when they encounter unescorted visitors or anyone not wearing visible identification.

6.1.2. Perimeter Security

	Description
Public **Class C**	Perimeter security requirements data centers that house only Public and Class C data: • automatic locking door closers; • the room should be without windows; • the door is solid with non-removable pin hinges; and • floor to ceiling walls.
Class B **Class A**	Perimeter security requirements for data centers that house Class B and A data: • automatic locking door closers; • the room should be without windows; • the door is solid with non-removable pin hinges; • floor to ceiling walls; • data centers must be physically separate GoS information processing facilities from those managed by external parties; • monitored alarm capability (physical intrusion detection), including tamper and intrusion alarms; and • wireless access to data processing not permitted.

6.1.3. Wiring Closets

	Description
All Classes	Requirements for wiring closets for all classes: • access is limited to authorized users only; and • single factor access to room (i.e. keys) permissible; and • key control must be maintained (i.e. log of keys issued and returned).

6.1.4. Utility Controls

	Description
All Classes	Environmental controls requirements for data centers housing all classes of data: • backup emergency power supply/UPS to prevent interruption of service are required; and • environmental controls (fire, water, humidifier controls, if appropriate) are required.

6.1.5. Environmental Controls

	Description
All Classes	Data centers must incorporate, to the extent possible and feasible, physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural and man-made disaster. Consideration must also be given to any security threats presented by neighbouring premises or streets. In addition to building code and fire regulations: • combustible or hazardous materials must be stored at a safe distance from the secure area; • bulk supplies, e.g. stationary, must not be stored in a secure area; • fallback equipment and backup media must be located off-site at a safe distance to avoid damage from a disaster affecting the main site; and • environmental alarm systems, fire suppression and firefighting systems must be installed.

6.2. Work Areas where Sensitive Information is Processed

6.2.1. Access to Work Areas where Sensitive Information is Processes

	Description
All Classes	Requirements for access to work areas for all classes: • physical perimeter security to office spaces should be based on threat and risk assessment and recommended controls outlined by Central Services, Protective Services Pranch.

6.2.2. File Security (Physical/Paper)

	Description
Public **Class C**	Requirements for Public or Class C physical file security: • files may be stored in an open area or within an individual office.

	Description
Class B	Requirements for Class B physical file security: - files containing Class B information may be stored in reception area if locked file cabinets are used and work area secured (either with personnel or physical barriers); and - files may be stored in offices if desk drawers are locked or file cabinets are locked.
Class A	Requirements for Class A physical file security: - files containing Class A information are stored in secure room compliant with the requirements of the *Physical and Environmental Security Standards*; - files must be located in locked file cabinets; and - if the physical file is the sole copy, it must be stored in fire resistant cabinet.

6.3. Physical Transportation of Information

	Description
Public Class C	Requirements for physical transportation of information are that: - regular envelopes and / or interoffice envelopes may be used.
Class B	Requirements for physical transportation of information are that: - tamper-evident packaging is used (e.g. double-sealed envelope with inside envelope signed to reveal tampering).
Class A	Requirements for physical transportation of information are that: - tamper-evident packaging is used (e.g. double-sealed envelope with inside envelope signed to reveal tampering); - the information is transferred with authorized staff or courier using a locked case tagged with forwarding or return office address; and - files or devices are not left unattended in non-secured areas.

7. Retention / Disposal / Redeployment — Deploying Computers

7.1. Redeploying Computers

	Description
All Classes	Within Government: - as part of inventory management, the current location for all computing assets must be tracked; and - all electronic storage media must be sanitized using a secure media eraser, approved by Information Security Branch, according to the Government of Saskatchewan *Electronic Storage Media Disposal Policy*. External to Government: - as part of inventory management, the current location for all computing assets must be tracked; and - all owned electronic storage media must be removed according to the Government of Saskatchewan *Electronic Storage Media Disposal Policy*.

7.2. Disposal of Electronic Information on Storage Media

	Description
All Classes	All electronic media, including removable devices, mobile computing devices or permanent electronic storage media, must be end-of-life'd according to the Government of Saskatchewan *Electronic Storage Media Disposal Policy*.

8. Cloud Computing Security

8.1. Policy Summary

The *Cloud Computing Security Policy* defines the policy for the consideration and use of cloud computing services. It mandates a 4-step framework for cloud computing risk management:

1. **Perform data classification.**

2. **Perform Threat and Risk Assessment (TRA) on the solution:**

   Option 1:
   A review by TRB and a Threat Risk Assessment completed by the Information Security Branch that takes into account:

   - supplier has adequate security policies, standards, and technical controls;
   - supplier adequately separates GoS data from the data of other customers;
   - GoS retains ownership of their data with the ability to easily move data or standardized applications elsewhere, with the supplier as a data custodian;
   - the supplier suitably sanitizes storage media at its end of life;
   - ability to audit the supplier's security or access reputable third-party audits.

   Option 2:
   Suppliers who have achieved ISO/IEC 27001 certified compliance or members of the Canadian Public Sector Community Cloud (under the auspices of the Public Service Chief Information Officer Council) can use a simplified risk management process of a successful review by TRB and a successful ISB review of the supplier's Statement of Applicability and recent external auditor's report

3. **Address threats/risks identified by implementing the proper security controls.**

4. **Continuously monitor and periodically audit services.**

Appendix

Network / Application Login Banner

Approved login banner:

> This System is the property of GOS. Authorized access only. Unauthorized access to this network device is prohibited. Disconnect immediately or risk possible criminal consequences.

Alternate login banner, as reviewed by Justice in 2011:

> This system, and the information within it, is the property of the Government of Saskatchewan. Only AUTHORIZED personnel of the Government of Saskatchewan may use this system. Unauthorized access is prohibited.
>
> Authorized users are subject to the “PSC 1103 Information Technology Acceptable Usage Policy” and “The Freedom of Information and Protection of Privacy Act” and Government of Saskatchewan and ministry specific security policies and procedures. By proceeding to use this system, you indicate that you are an authorized user, you are aware of your security, privacy and acceptable use responsibilities.

Email Disclaimer

Approved email disclaimer, as reviewed by the Ministry of Justice:

> CONFIDENTIALITY NOTICE:
> This e-mail and any file transmitted with it are intended only for the named recipients and may contain legally privileged and/or confidential information. If you are not the intended recipient, please do not disseminate, distribute, or copy this e-mail without the consent of the sender.