

Subject: Hosting and Software Policies, Standards and Guidelines for MOTI's Intelligent Transportation Systems	
Date: January 24, 2022	Author: Cyber-Physical Systems Team, Information Management Branch Reviewed by: William Zhang, P.Eng.
Bulletin Number: TE-2022-01 Bulletin Type: Requirement	Effective Date: January 24, 2022
Audience	Standards Affected
Ministry Managers, Electrical Services; all holders of the Electrical and Traffic Engineering Manual; all Project Managers; all Design Consultants	Electrical & Traffic Engineering Manual

Policy

ITS servers and the software installed on them must comply with the ITS hosting and software policies, standards and guidelines determined by the Ministry's Information Management Branch (IMB), which in turn reflect and align with those of the Office of the Chief Information Officer for the Provincial Government of B.C.

Details of these policies, standards, and supported software technology roadmaps have been provided as appendices to this document. ITS Designers must consider and accommodate all standards and guidelines summarized and cited herein in the design, development, and delivery of an Intelligent Transportation System's software head-end components. Where a proposed solution cannot align with these factors, or with the detailed standards and guidelines that are provided, approval for exemptions must be sought and granted before the end completion of Phase 3 - Preliminary Design.

Terms and Definitions

The following table provides context and clarity for terms and acronyms used throughout this Technical Bulletin.

Term / Acronym Used	Term Definition / Scope
ITS	Intelligent Transportation System
ITS OT Components	<p>ITS Operational (Industrial) Technology Components are inclusive of firmware, software and associated electronics and instrumentation. Components include:</p> <ul style="list-style-type: none"> • sensors • actuators • electronic signs (DMS, VMS, BOS, etc.) • roadside data processors • controllers (programmable logic controllers, remote terminal units, programmable automation controllers, intelligent electronic devices, etc.) • cameras • media converters, encoders, decoders
ITS IM/IT Components	<p>ITS Information Management / Information Technology Components are inclusive of associated peripherals, firmware, and software. Components include all:</p> <ul style="list-style-type: none"> • servers (virtual and physical) • workstations (virtual and physical) • communications network devices (routers, switches, modems, extenders/repeaters, etc.) • network security devices (security gateways, scanners, firewalls, etc.)
Hosting Infrastructure and Services	<p>Hosting Infrastructure encompasses:</p> <ul style="list-style-type: none"> • all servers (virtual and physical) and associated peripherals, firmware, and software • all tools used to monitor/manage the health of servers and the software installed on them • all corporate tools used to access servers and the software installed on them, e.g., remote access software, authentication services • all computing hardware and associated software used to manage backups and disaster recovery for servers and the software installed on them • all tools used to provide, manage, maintain, and facilitate access to ITS data stores • all tools required to support consumption of corporate services (e.g., email, DNS, NTP, AAA, Security) for servers and the software installed on them • all tools used to manage versioning of the software installed on servers

Term / Acronym Used	Term Definition / Scope
	<ul style="list-style-type: none"> all tools used to facilitate and manage access to/from the internet for software installed on servers all tools used to facilitate and manage interoperability between software installed on servers and other systems/subsystems, software, services, data stores, workstations, and OT <p>Hosting Services encompass:</p> <ul style="list-style-type: none"> Provisioning, delivery, and management of hosting infrastructure ITS software release management and support Authoring the IM/IT documentation related to hosting infrastructure for an ITS and the software installed on ITS servers that IMB considers mandatory or desirable for MOTI's ITS
SCADA	Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to control industrial processes locally or at remote locations
MoTI or Ministry	Ministry of Transportation and Infrastructure
IMB	Information Management Branch, a division of the Ministry
OCIO	Office of the Chief Information Officer

ITS Hosting and Software Standards and Guidelines

1. Hosting Infrastructure and Services

The Ministry provides the hosting infrastructure and services for its ITS. Various server configurations are available; server virtualization is the standard. Storage area network (SAN) storage is available in various speed and resiliency levels. Detailed server specifications will be required from the Designer. Consultation and collaboration with IMB will be necessary to guide this effort and lead times for delivery can be a factor. Managed hosting facilities can be purpose-built at site by exception only.

Physical access to ITS hosting facilities and infrastructure is limited to authorized staff of the Ministry and service providers that have been contracted to manage and maintain these facilities and infrastructure. Remote access to file shares and databases is accommodated via Virtual Private Networks for troubleshooting, however administrator/root access to the servers will not be provided.

Existing OCIO contractual relationships establish the options for supported Infrastructure Software components including:

- Virtualization Technology
- Server Operating Systems
- Database Platforms
- Other Supported Software

The roadmaps for these supported components are updated annually to maintain sufficient currency with vendor releases and these roadmaps will be provided to Designers. Of note however, the Ministry has experience with and a requirement for Designers to use components from within this shortlist.

Virtualization Technology¹:	VMWare
Server Operating System (OS)²:	Windows Server
Database Platform³:	MS SQLServer
SCADA Platform:	Ignition by Inductive Automation
OPC Platform:	KEPServerEX by Kepware

2. ITS Software Development Guidelines & Standards

Software Design - Wherever applicable, ITS software design should be modular and non-monolithic in keeping with current software development best practices. Each module design should provide capabilities to alert to Operational issues associated with the individual component. The Designer should also keep in mind the process involved in updating the software once deployed so that it can be done with minimal impact and downtime.

Designers must consider and align to the “BC Government API Guidelines”⁴ and OCIO’s “Guidelines on the Use of Open Source Software”⁵.

ITS must comply with the Government “Physical Address and Geocoding Standards”⁶, and MoTI’s “Spatial Data Standards”⁷ when relevant to their ITS, and consultations must occur with IMB prior to starting development of any associated system.

It is MoTI's best practice in ITS software design to include a mechanism whereby application software functions can be tested and validated without connection to operational field devices. For example, the ability/capability to use simulation test harnesses and/or run the software in simulation mode.

In addition, it is MoTI's best practice in ITS design to include robust logging and debugging capabilities in application software and in communications between components. These capabilities need to be deployed in such a way that they can be:

- enabled / disabled while system is running, and
- configured to be unimpactful to the hosting infrastructure.

¹ See [Appendix 1](#): OCIO Virtualization Technology Roadmap, March 2019

² See [Appendix 2](#): OCIO Operating System Roadmap, April 2021

³ See [Appendix 3](#): OCIO MSSQL Services Roadmap, March 2020

⁴ See [Appendix 4](#): BC Government API Guidelines – *extracted from source web page* August 31, 2021

⁵ See [Appendix 5](#): OCIO Guidelines on the Use of Open Source Software, Release 1.0, April 2012

⁶ See [Appendix 6](#): Physical Address and Geocoding Standards, Version 1.0, March 15, 2010

⁷ See [Appendix 7](#): Spatial Data Standards, Version 0.6 May 21, 2019

Availability & Recovery - The Designer must consult with MoTI to determine the appropriate ITS Availability and Recovery metrics as per this extract of the IMB's 'Hosting Infrastructure Design Guide'⁸ which describes the availability metrics used by IMB to determine the appropriate hosting infrastructure for an ITS. The Designer must propose a system architecture that meets these stated availability requirements. For example, if the system is expected to remain online during standard maintenance activities such as server OS patching, the design must accommodate single server outages (restarts, reboots) without affecting system availability. Systems must be able to recover automatically in a timeframe that matches the criticality of the system after any hosting or network infrastructure issue such as a brief network outage or virtual server re-allocation to another host node. Critical and Life Safety System architecture must build-in full redundancy and automated failover capabilities and Designers must complete associated Disaster Recovery Planning activities with the IMB as noted in the OCIO Critical System Standard⁹ and comply with the Critical Systems Guidelines¹⁰. SCADA Systems categorized as Critical or Life Safety Systems must support full, redundant local site operation in addition to remote operations from the centralized TMCBC management facility.

Third-Party Components - All application and third-party IM/IT software components used within the ITS must be fully supported by the original software vendor, approved by the IMB, and have an acceptable roadmap for continued product evolution established. It is requested that vendors notify the Ministry if a component or 3rd party module is going to be end of life within the support maintenance agreement timeline. The Ministry expects that all Software Platforms and ITS applications selected will be version N or N-1 when implemented (where N= the current major supported release version, N-1: the previous major release, if still supported by the OCIO and/or original vendor).

Release Management – At minimum, the promotion path for ITS software will be comprised of two MOTI environments:

1. Development (DEV) or Test (TST), whichever is deemed most appropriate for the ITS Software in consultation with IMB and in alignment with the description/purpose for these environments as described in the extracts from the IMB Hosting Infrastructure Design Guide¹¹.

Due to the nature of ITS and their interoperability with operational technology devices on MOTI's field networks, DEV and TST functions are most commonly supported and executed in the same environment and the environment is named based on the primary function that it serves. For example, if an ITS requires a large degree of developer customization and configuration in the Ministry's environment in order to fulfill its function as designed, the environment will be named/labelled Development/DEV. If an ITS requires little to no developer customization and configuration in the Ministry's environment to fulfill its function as designed, the environment name/label will be Test/TST.

⁸ See [Appendix 8](#): Excerpt from Infrastructure Design Guide – Availability V.04 April 23 2020

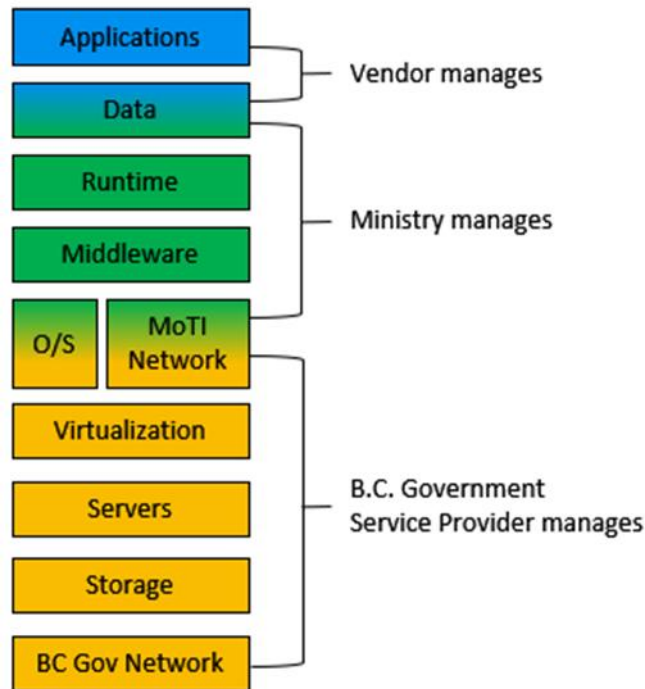
⁹ See [Appendix 9](#): OCIO Critical Systems Standard V3.0, July 2019

¹⁰ See [Appendix 10](#): OCIO Critical Systems Guidelines V3.0, July 2019

¹¹ See [Appendix 11](#): Excerpt from Infrastructure Design Guide – Hosted Environments V.04 April 23 2020

2. Production (PRD) The Software Vendor is required to Factory Acceptance Test (FAT) the ITS software in their own environment before delivering the software to the Ministry. IMB facilitates all releases to Ministry promotion path environments in collaboration with the Designer's Deployment Specialists for the ITS. The Designer must request ITS software releases in advance, which will then be scheduled, approved, coordinated, and communicated to Stakeholders through a structured Change Management process. IMB Change Leads oversee these request and approval processes. If VM snapshots are required in preparation for a release (e.g., prior to a change to support rollback), they must be requested and scheduled in advance with the IMB. For each release, the Designer must provide Release Notes and a Deployment Plan.

Implementation, Maintenance & Support - Responsibilities for the Ministry's ITS Hosting and Software components are spread across three distinct parties, as depicted here.



For example, mandatory standard maintenance patching of Operating Systems is carried out by the Service Providers on a set schedule, with active Ministry participation. Depending on the ITS IM/IT architecture deployed, this can impact ITS availability and performance. Designers should accommodate full remote maintenance capability for all industrial servers located in the field (e.g., AC power cycling via network control relay vs. requiring field maintenance staff performing supporting tasks at roadside). Details of MoTI's Electrical Maintenance Service Agreements with external providers are publicly available and must be considered.

ITS Server & Communication Considerations - ITS server architecture must comply with the OCIO Enterprise IT Security Architecture: Network Security Zone Standards¹² which dictate the security zone to which each ITS component will be allocated based on its purpose and what communications are permitted between designated zones. Whenever possible, standards-based protocols are preferred. Any use of proprietary protocols must be documented in an Interface Control Document (ICD) and submitted to the IMB for approval.

Integration with Corporate Services & Key Ministry Tools - Designers will ensure that new ITS integrate with and leverage established Corporate Services and Ministry Enterprise toolsets (also known as Common Components), and accommodate the recommended protocols in use:

- Active Directory (IDIR) integration for Identity and Access Management
- SiteMinder for public-facing secure Web Access Management
- SMTP protocol for Email Messaging
- Tenable Solutions for Vulnerability, Network, Infrastructure & Application Scanning & Monitoring
- Domain Name System Protocol for Web Addressing

In addition, whenever the ITS is integrated with the Ministry's Advanced Traffic Management System (ATMS), consultation with IMB will be needed to ensure the requirements for interoperability with upstream components are understood and met by the ITS design (e.g., Datawarehouse, DriveBC).

3. Access Control & Information Protection

ITS Access Controls - ITS design must comply with the current OCIO Access Control Security Standard¹³. Largely, the controls are supported through the ITS' integration with the Government's Identity and Access Management Service. Of note however, the following key restrictions must be accommodated:

- All passwords and security tokens must be able to be changed
- All passwords must expire on an established timeframe
- Passwords must meet complexity standards
- Shared password use must be limited to devices that cannot support unique credentials
- Default password use is not permitted for any system component, and devices cannot be deployed while in this state
- Passwords cannot be stored in clear text and cannot be visible during login
- Enhanced auditing of administrative accounts (privileged access) is required

ITS must comply with established OCIO "Database Security Standards for Information Protection"¹⁴.

¹² See [Appendix 12](#): OCIO Enterprise IT Security Architecture: Network Security Zone Standards, Version 2.0, July 20, 2012

¹³ See [Appendix 13](#): OCIO Access Control Security Standard, Version 1.1, August 2020

¹⁴ See [Appendix 14](#): Database Security Standards for Information Protection, Version 1.0, April 4, 2018

ITS IM/IT components must comply with “Cryptographic Standards for Information Protection”¹⁵ specifically regarding required minimum TLS and SSL protocol use.

4. Mandatory IM/IT Documentation Required

In addition to the appropriate deliverables outlined in Section 601.7 of the Electrical & Traffic Engineering Manual containing all relevant IM/IT aspects of solution delivery, the Designer must contribute to the development of content for MoTI IMB’s SDLC deliverables during the project phases identified below, including Deployment Plans and Release Notes identified within Section 2 of this bulletin:

MoTI Engineering Phase	IM/IT (SDLC) Deliverable
Phase 3 Preliminary Design	Preliminary Technical Analysis
Phase 4 – Detailed Design	Technical Design
Phase 5B - Construction	Data Conversion & Migration* (<i>if legacy data is required</i>)
	Conversation Block Diagram
	Conversation Table*
Phase 6 – Integration, Testing & Calibration	Release Notes
	Deployment Plans
Phase 7 – Operations & Maintenance	Disaster Recovery Plan

Additional documentation may be required depending on the size and complexity of the system.

Information Management Branch Contacts:

Felix Candela

A/Director, Cyber Physical Systems
Information Management Branch
Phone: (778) 974-4690
Email: Felix.Candela@gov.bc.ca

Fayaz Kadir

IM/IT Infrastructure Lead, CPS
Information Management Branch
Phone (604) 202-6849
Email: Fayaz.Kadir@gov.bc.ca

ITS Engineering Contacts:

Mark Louttit, P.Eng.

Manager, Electrical and ITS Engineering
Transportation Systems and Road Safety Eng.
Phone: (236) 468-1970
Email: Mark.Louttit@gov.bc.ca

¹⁵ See [Appendix 15](#): Cryptographic Standards for Information Protection, Version 1.7, Sections 2 & 3

Normative References

The following appendices are referred to in this Technical Bulletin in such a way that some or all of their content constitutes requirements of the ITS Hosting and Software Standards and Guidelines described herein. These are dated/versioned references; only the edition cited applies.



Office of the Chief
Information Officer

Virtualization Technology Roadmap

March 2019

Office of the Chief Information Officer
Virtualization Technology Roadmap

Virtualization Enhancements

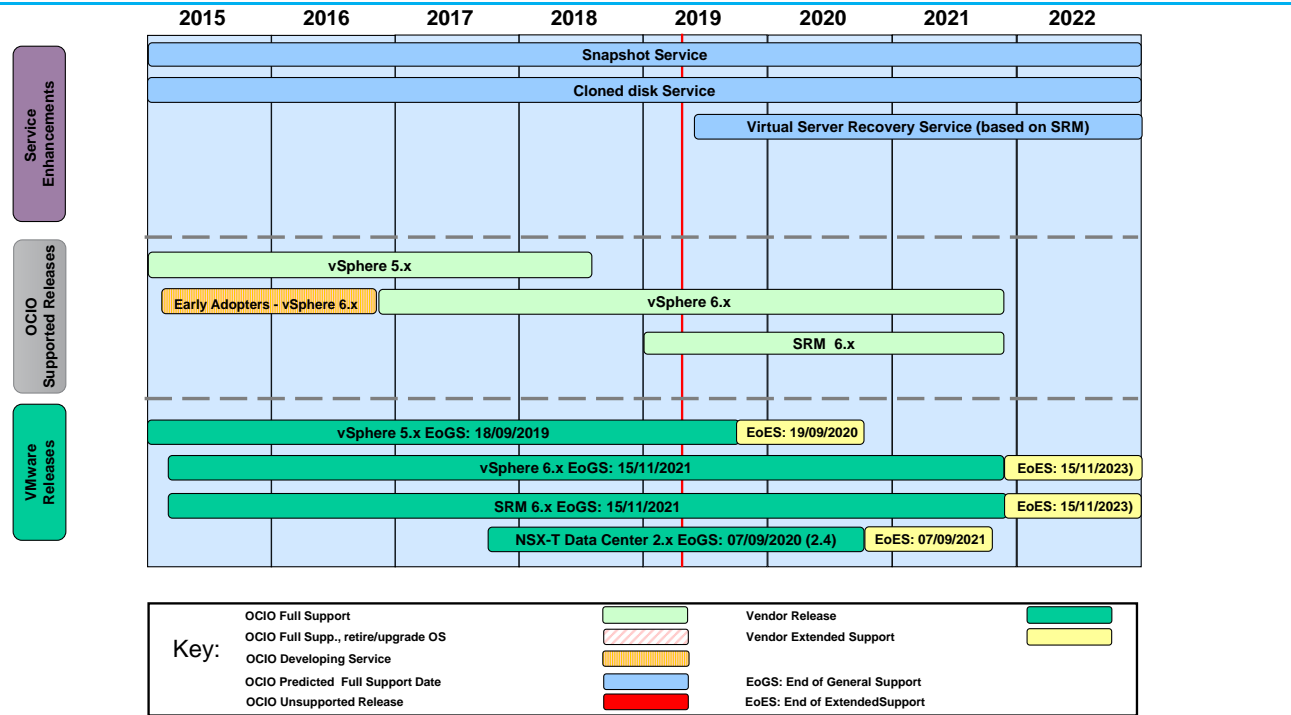
Hardware: New ESXi hosts will arrive in 2019 in Kamloops to continue VMware host refresh

Windows 2019: vSphere environment fully supports the deployment of Windows Server 2019

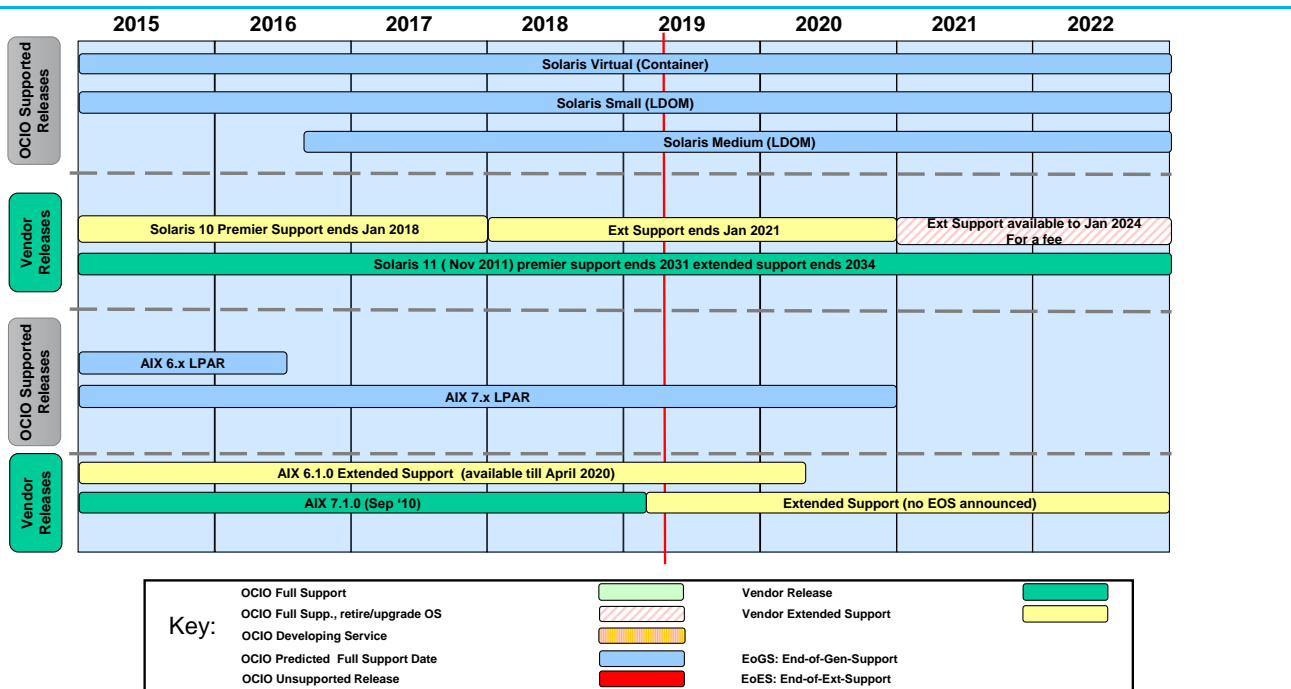
VSRS (Virtual Server Recovery Service): Implemented VMware's SRM solution (VM replication and recovery services)

Automated VM Deployment: Automated VM deployments through VMware VRA/VRO and Infoblox

Large VM Support: The hosting virtualization platform now supports up to 16 vCPUs and 128GB RAM

Virtualization Services Roadmap - VMware

3

Virtualization Services Roadmap – Solaris & AIX

4



Operating Systems Roadmap

April 2021

Office of the Chief Information Officer
Operating Systems Roadmap

Operating Systems Lifecycles

- OS vendors typically follow a standardized release schedule for major changes. For example, Microsoft has established a 4 year lifecycle with annual updates:
 - year 0 – new release,
 - year 1 – service patch 1 rollup,
 - year 2 – feature release,
 - year 3 – service patch 2 rollup
 - year 4 – new release
- Other server operating systems in use (i.e. Solaris, Linux, AIX) have their own specific release lifecycles.
- The goal is to remain current with major OS releases by making an approved build available within six months of release by the vendors. Typically, the release is tested by the Service Provider for several months and then made available for production use to 'early adopters'. Approximately one year after release, all new servers would use 'new' OS, with the old version available on an exception basis.

Operating System Currency

What is N?

Operating system currency is based on an operating system release being designated as the current supported release (designated as N) in the STMS Managed Services environment. Using N as the baseline – other versions can be described:

- N: the version designated as the current supported release. Described in past TIBs as the “default” version
- N-1: the previous major release of the OS – still supported in the Managed Services environment
- N-2, N-3, etc.: older releases of the OS. Retirement phase. Supported based on available vendor support.
- N+1: New releases of the OS being considered for promotion to N.

Major and Minor releases

Operating system versions are described in terms of Major and Minor releases:

- Major release examples: Solaris 11, Windows 2012, RHEL 6
- Minor Release examples: Solaris 11.2, Windows 2012 R2, RHEL 6.7. Minor releases can have mandatory upgrade timeframes to ensure continued vendor support.

3

Operating System Currency

Who decides what N is?

N is decided by the Joint Operations Committee (JOC)






- The Joint Technical Services and Architecture Working Group (JTSAWG) reviews proposed OS release configurations, including new features, as well as security configurations, and approves the technical configuration for the release. JTSAWG passes its technical approval on to JOC with a recommendation for full operational approval and implementation.
- JOC approves the release and advises Joint Service Delivery Management (JSDM)

How is the state of OS Currency Communicated?

- The Annual Operating System roadmap describes the currently supported versions, as well as new versions being considered for adoptions
- Quarterly Compliance reports are produced to identify non-compliant systems (N-2 and greater) is posted to the Enterprise Portal.
- An Annual Operating System Currency reporting is posted to the Enterprise Portal.
- **Client communication:** OCIO submits TIBs describing upcoming changes
- **Client communication:** Hosting Services posts Service Bulletins describing upcoming changes to service

4

Support Legend

OCIO Full Support	
Full vendor support is available	
OCIO support has no restrictions	
OCIO Full Support, retire/upgrade OS	
OCIO support has no restrictions except those imposed by the vendor	
Vendor support is limited (security patches only for example)	
New deployments require an exception from IT AMO	
OCIO Early Adopters Support Date	
Full support is available to a select customers on an exception basis	
OCIO Predicted Full Support Date	
Predicted date for full support based on vendor release dates	
Unsupported Release	
No vendor support available, hence no OCIO support	

5

Things to note

Windows

- Windows 2019 has been declared as N – the default deployment to the data centres – as of June 22nd 2020.
- Windows 2008 reached EOL January 14, 2020. Extended Update Support from Microsoft was made available beyond this EOL date for a rising-rate fee. Support extension is based on Hosting Services' annual review and approval.

RHEL

- RHEL 8 has been declared as N – the default deployment to the data centres – as of June 22nd 2020.
- RHEL 6 reached EOL November 30, 2020.

AIX

- There were currently only 18 AIX servers Active as of June 18, 2020.
- For AIX, the major current version is currently 7.x, with the minor versions currently supported for virtual guests being 7.1 and 7.2. the TLx references refer to patch bundles that are released by IBM on a regular basis – and applied to each minor version shortly after their release.

Solaris

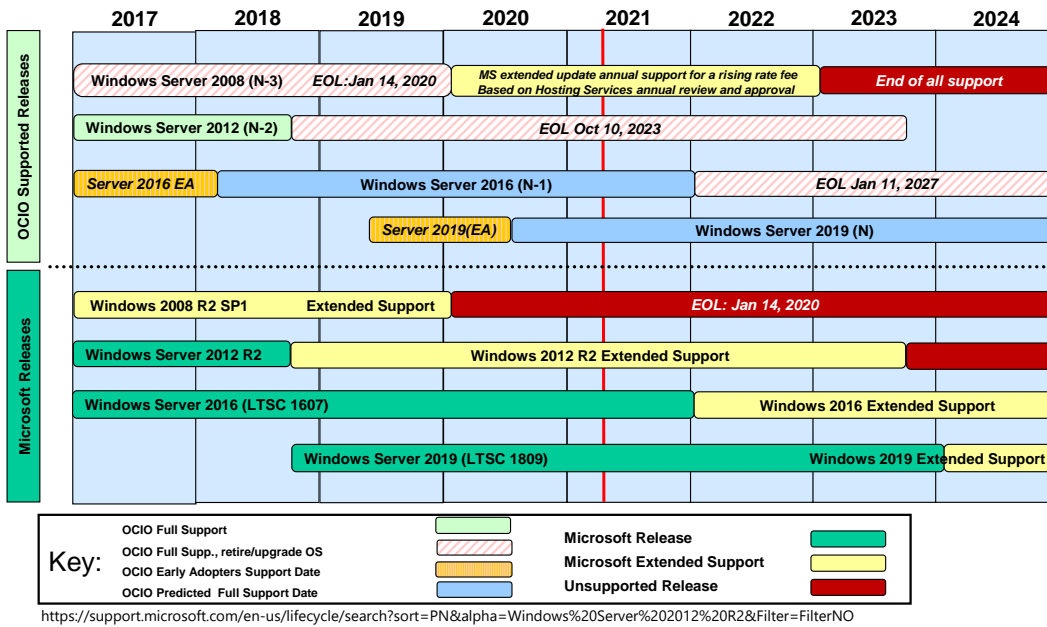
- No new Solaris hosts will be purchased after December 31, 2024.
- Province of BC Extended Support for Solaris 10 ends Jan 24, 2021.
- Extended support for Solaris 10 to Jan 24, 2024 available for a fee.

OpenVMS

- VSI version of OpenVMS started being used as of April 2020.

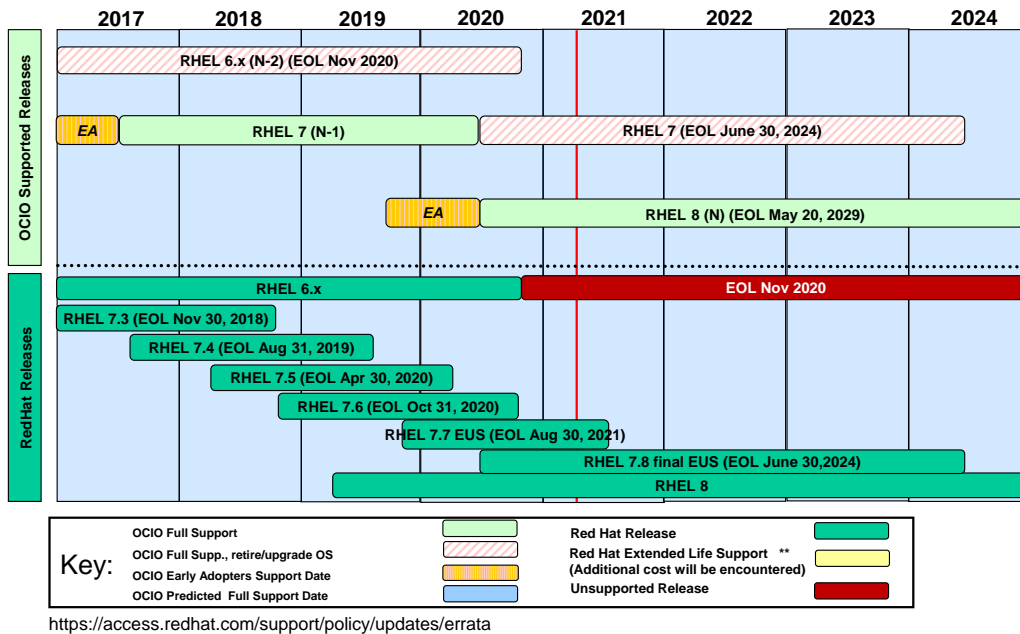
6

Technology Roadmap – Microsoft Windows Server



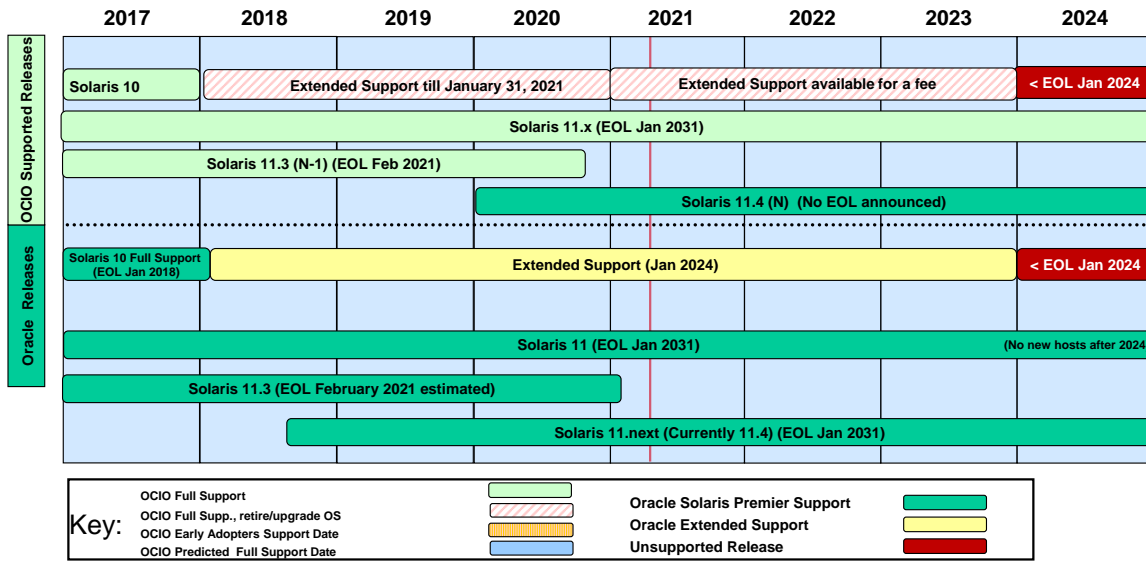
7

Technology Roadmap – Red Hat Enterprise Linux



8

Technology Roadmap – Oracle Solaris



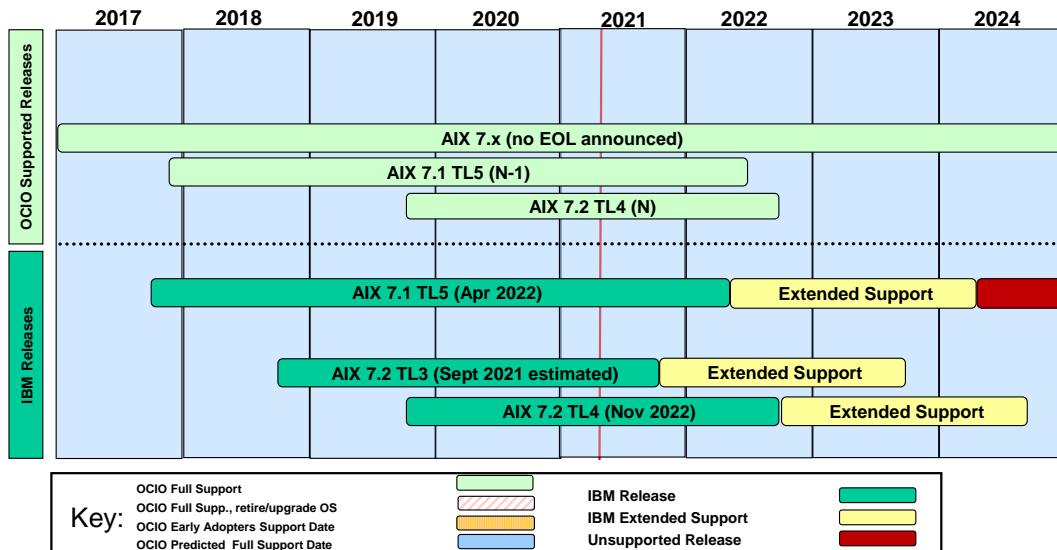
<http://www.oracle.com/us/support/library/lifetime-support-hardware-301321.pdf>

On Jan 18th, 2017, Oracle announced that they are moving to a Continuous Delivery model for Solaris 11, and will not be releasing a Solaris 12 OS. This change to the Solaris OS lifecycle has been branded Solaris 11.Next.

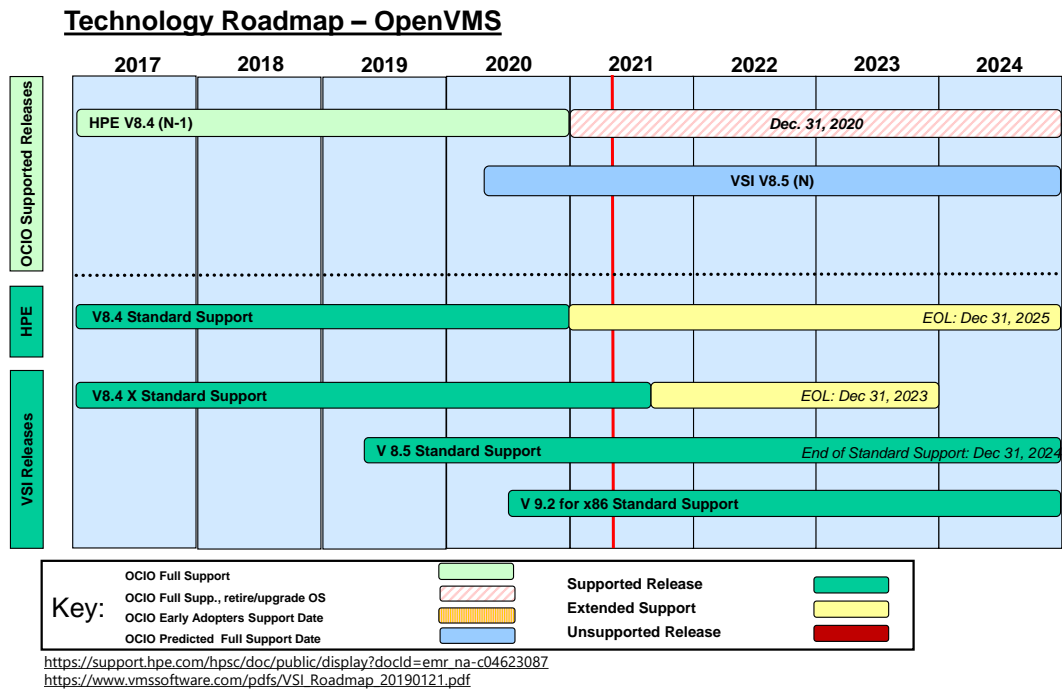
It is recommended that clients with Solaris hosts begin planning for migration to other operating systems. No new hosts will be purchased after 2024.

9

Technology Roadmap – IBM AIX O/S



<http://www-01.ibm.com/support/docview.wss?uid=isg3T1012517>



Shared Database – MSSQL Services Roadmap

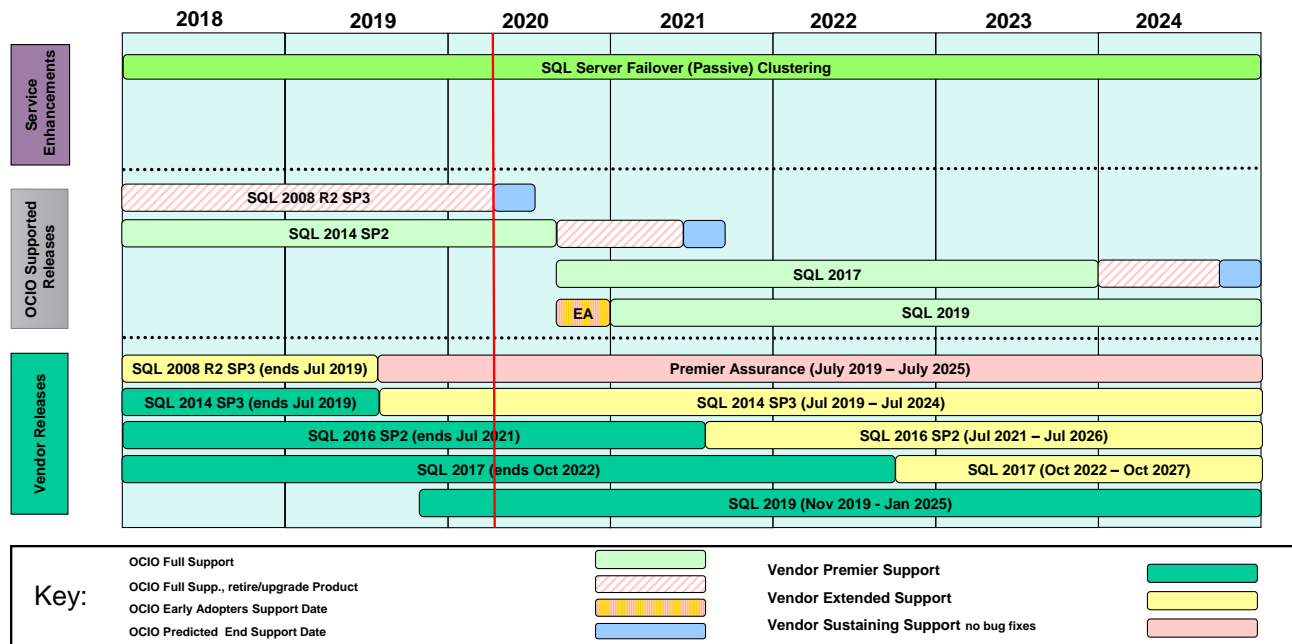
March 2020

Office of the Chief Information Officer
Shared Database - MSSQL Roadmap

INTRODUCTION PAGE

- Shared Database - MSSQL Services provides a shared MS SQL environment that offers a low cost solution for the development, testing, and production support of databases. This service is appropriate for customers that are looking to manage application schemas only. Customers with modest or moderate database needs derive value from this shared environment as it is a more cost effective solution than dedicated server environments.
- The Shared Database - MSSQL Service provides a secure, reliable environment for databases on a Shared Database Server and includes databases, of multiple supported versions, backups, monitoring, licensing and a base allocation of managed storage for each database instance. Clients who choose to purchase this service must purchase a minimum of two Shared Databases (one Shared Database for production and one Shared Database for test and development).
- All Shared Database – MSSQL Services run Standard Edition only.
- Once all clients migrate off MSSQL 2008 R2, MSSQL 2017 will be added to the service. All client databases should plan to transition to MSSQL 2017 between summer of 2020 and summer of 2021.
- An MSSQL 2019 early adopter option will be added to the service in the summer of 2020.

Technology Roadmap – Shared Database – MSSQL





Topic

Data and APIs

Province provided Data and API Services

Documentation

[BC Government API Registry](#)[BC Data Catalogue](#)[BC Web Mapping And Spatial Services](#)[BC Government API Guidelines](#)[BC Government OpenAPI Specifications](#)

NOTE: This is a living document, [posted here for your feedback](#). We gratefully acknowledge the assistance of [the Government of Canada in sharing their API standards](#), providing a baseline for this document.

BC Government API Guidelines

Published by the [Technical Assets Working Group](#) under the [BC Data Council](#)

Purpose : The purpose of these guidelines is to promote consistency and provide guidance around the use of Application Programming Interfaces (APIs) across the BC government, and to enable exchange and integration of data between systems, agencies, businesses and citizens.

- **Why API First?** – APIs are an efficient and secure way to share data and expose functionality between government's digital services. "API First" is a design principle which stipulates that an API is the first interface for a given application; it is the first artefact to be developed over the data layer, and it is self described.
- **What's in the API Guidelines?** – the B.C. Government API Guidelines provide design and best practices for building interfaces between systems or exposing data for secondary use. Other topics include security, metadata, versioning and management. The guidelines have been developed by BC Government IT professionals using internal references and a thorough review of several public and private sector leaders.
- **When to use the API Guidelines?** – most real time data integration requirements are best satisfied through APIs. In general, data sharing and integration also encourage the use of APIs to promote platform independence and loosely coupled service design.

API Design

Design Principles:

- **Simplicity and Reusability** : strive to make the API the best way for clients to consume your data
- **Consistency** : design API's with a common look and feel using a consistent style and syntax
- **Security by Design** : adopt a philosophy where security is inherent in API development
- **Continuous Improvement** : actively improve and maintain API's over time by incorporating consumer feedback
- **Sustainability** : avoid short-term optimizations at the expense of unnecessary client-side obligations
- **Quality** : ensure flexibility, scalability and that your API presents actionable



- **Well Described** : adopt a simple, consistent and durable API specification and endpoint naming standard that includes API meta information
- **Open Standards Based** : stay compliant with the standard HTTP methods including status and error codes

Design Patterns:

- **Use a RESTful Approach** – use HTTPS request/response format for data access and manipulation and provide proper error responses to the client
- **Use JSON** – use JavaScript Object Notation (JSON) as the message structure for all web service APIs
 - Form responses as a JSON object and not an array
 - Use consistent grammar case by using underscore or CamelCase
 - APIs into legacy systems may be required to use a different representation such as XML
- **Use URIs to represent resources** – URIs (Uniform Resource Identifiers) represent business entities, not the operations on those entities. If data is returned as a part of a response, use URIs to uniquely identify the data as a resource
- **Always Use HTTPS** –
 - ACCEPT and CONTENT-TYPE request headers are mandatory
 - AUTHORIZATION header is mandatory for secured APIs
 - Pass the API key in the header rather than the URI
 - API keys/tokens must be securely setup and used appropriately
 - The response must contain the CONTENT-TYPE header
 - If caching is desirable, response headers must also include CACHE-CONTROL
- **Don't overload verbs** – Each verb should represent a single operation on a given resource. Avoid using request parameters to pass additional operations. The following are appropriate uses of HTTP verbs in the context of a RESTful API:
 - GET – read either a single or a collection resource
 - POST – create a new resource or initiate an action
 - PUT – update or replace an existing resource
 - DELETE – remove a resource
- **Follow properties according to [RFC 7231](#) and [RFC 5789](#):**

Method	Safe	Idempotent	Cacheable
GET	✓ Yes	✓ Yes	✓ Yes
HEAD	✓ Yes	✓ Yes	✓ Yes
POST	✗ No	:heavyexclamationmark: No, but Should: Consider To Design POST and PATCH	◆ May, but only if specific POST endpoint is safe . Hint: not supported by

PUT	✗ No	✓ Yes	✗ No
PATCH	✗ No	:heavyexclamationmark: No, but Should: Consider To Design POST and PATCH Idempotent	✗ No
DELETE	✗ No	✓ Yes	✗ No
OPTIONS	✓ Yes	✓ Yes	✗ No
TRACE	✓ Yes	✓ Yes	✗ No

Source: <https://opensource.zalando.com/restful-api-guidelines/#http-requests>

- **USE W3C HTTP Methods** – follow the standard methods as described by the W3 Consortium - <https://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html>
- **Segment response data for large queries** – APIs exposing large datasets must support some form of data segmentation. The following are some common patterns for pagination along with appropriate use cases:
 - *page* and *perpage* – best used to navigate large static datasets (e.g., reference data) where the same set of data is likely to be returned given the same page reference over time
 - *offset* and *Limit* – best used for APIs fronting Structured Query Language (SQL) based backends where the offset represents the data cursor on a given indexed column
 - *since* and *Limit* – Best used for queries where the consumer is interested in the delta since the last query and the backend data structure is indexed based on time
- **Respond with message schemas that are easy to understand and consume - the following practices should be applied:**
 - **Use common information models** – Leverage industry recognized common information models where possible. If you must define your own information model, create a model which is technology and platform agnostic and avoid using proprietary schemas
 - **Standardized error codes** – Avoid building custom error codes and schemes which require heavy parsing by the consuming system. Conform to common HTTP status codes when building RESTful API's - <https://www.w3.org/Protocols/HTTP/HTRESP.html>
 - A quality error code will indicate what went wrong and why and should include 3 basic criteria:
 - 1) HTTP Status Code
 - 2) Internal reference ID mapped to internal reference documentation
 - 3) Human readable messaging to summarize the context, cause and a general solution
 - Standard HTTP error codes are classified as follows:

- 3XX – Redirection - to indicate status of the resource or endpoint; useful in subdomains or moving a resource from one server to another
- 4XX – Client Error - occurrences such as when a URI is incorrectly formed or the client has sent too many requests
- 5XX – Server Error - indicates a server side error (not a client issue)
- **Abstract internal technical details** – Responses, including error messages, should abstract technical details which the API consumer has no visibility into. Internal technical errors, thread dumps, and process identifiers should all be removed from response data
- **Implement stateless interactions** – The interaction between API consumer and provider must be stateless. APIs must not expect any concept of session or management of state on the part of the consumer. Any transaction where multiple APIs are called in a repeatable sequence to create a singular business interaction should be implemented as a composite API
- **Prefer 'Pull' over 'Push'** – use APIs to pull data rather than push data into databases. Having consuming systems query APIs based on specific parameters ensures that only data that's required in the context of a business process or transaction is being passed, and that the transmission of data is granular and secure. Data sink APIs and Event Driven Architectures (EDA) often require additional complexity in queuing considerations; however, this approach to data streams can provide lower latency and intermittent fault tolerance than batch or bulk data integration techniques. Bulk or batch data integration techniques and tools should be reserved for data synchronization patterns when network limitations are prevalent, or another limitation dictates its necessity
- **Bulk Dataset's via API's** – in some cases APIs will be used to transfer bulk datasets between systems or external to BC Government. In those scenarios, apply the following considerations:
 - *small datasets* – Smaller datasets should be returned in low overhead formats (e.g., Comma-separated values (CSV) or JSON) rather than XML. Do not use compressed file attachments as this is a possible method of bypassing content scanning mechanisms
 - *trigger API* – An API may be implemented as a trigger to initiate an out-of-band interface such as a managed file transfer
 - *search and link API* – If the dataset is published on file servers already available to the consumer, an API could be implemented to return a link to a specific file based on specific request parameters

API Security

The following practices must be followed for any API which provides access to protected or privileged data and are strongly recommended as part of a "security by design" philosophy for all API development. Outside of this baseline set of security controls, additional controls (e.g., message-level encryption, mutual authentication, and digital signatures) may be required based on the sensitivity of the data:

- **Secure Data in Transit** – always send data over a secure and encrypted network connection, regardless of data classification; enable TLS 1.2 or higher



- **Security by Design** – durable API design will include protection against common API attacks such as buffer overflows, SQL injection and cross site scripting. Treat all submitted data as untrusted and validate before processing. Data validation (for both input parameters and inbound data) should be considered in the service tier but should also extend into the data model itself, with such considerations as data staging, mandatory values and referential integrity constraints as appropriate
 - See [here](#) for the OWASP REST Security Cheat Sheet Project
- **Do not put Sensitive Data in URIs** – use the JSON payload to submit queries for sensitive data rather than putting it in the URI string
- **Authenticate and Authorize** – ensure only privileged or authorized users can invoke your API once they are properly authenticated using either an API key or OAUTH token
 - Ensure that the API key/secret is adequately secured
 - Use API keys with all data API's to track and meter usage
 - For each API key, rate limits are applied across all API requests
 - For system-to-system integrations consider key/secret revocation and reissue capabilities
 - See here for BC Government standards on identity management: https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard#id_mgt
 - See here for BC Government standards on general IT security: https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard#it_sec
- **Token management** – avoid using custom or proprietary tokens in favor of open industry standards such as JSON Web Token (JWT). All access tokens must expire within a reasonable amount of time (less than 24 hours) and refresh intervals should reflect the security characteristics of the data being accessed. Use fine grained access and the principle of least permission when defining tokens
- **Restrict dynamic or open queries** – the ability to inject consumer defined query strings or objects into an API must be limited to open data, reporting, and statistical APIs only, and strictly prohibited on master data, transactional or business APIs. Dynamic and open queries create dangerous attack surfaces for APIs. It's better to invest more effort in identifying all the valid query use cases and design the API to specifically meet them
- **Restrict wildcard queries** – wildcard queries in APIs can be dangerous from a data performance perspective. If wildcard characters are allowed, ensure there are restrictions on which and how many parameters can have wildcard input to prevent large data query sizes
- **Use gateways and proxies instead of IP whitelists** – When exposing APIs to the internet, use a secure gateway layer to provide a security control point instead of simply whitelisting inbound Internet Protocol addresses (IPs). When consuming external APIs, route flows through a forward (egress) proxy instead of using IP address whitelisting on the outbound firewall
- **Integrate Security Testing** - automate security testing to validate any new changes to API source code and to ensure robustness of requested changes. Assess the change impact and conduct testing accordingly



- **Audit Access to Sensitive Data** – all API based access to non-public data must be logged and retained for audit purposes. Logging attributes must include the source system, client identifier and associated timestamp from the target system
- **Monitor and Log API Activity** – track API usage and activity to identify performance bottlenecks, peak usage periods and abnormal access patterns. Use open standards-based logging frameworks such as CEF (Common Event Format) and collect logs in a central repository
 - When usage limits are exceeded, by default, a 1-hour timeout (block) will be used
 - X-RATELIMIT-LIMIT and X-RATELIMIT-REMAINING can be inspected in the HTTP response to view current usage

API Encoding and Metadata

Consistent metadata and encoding ensures that APIs are interoperable across organizations and helps to maintain data consistency. The following practices should be followed when defining your API:

- **Use Unicode for Encoding** – Unicode Transformation Format-8 ([UTF-8](#)) is the standard encoding type for all text and textual representations of data through APIs. It must be used for all APIs published across the BC Government for both internal and external consumption
- **Standardize Datetime Format** – use the ISO 8601 Standard for datetime representation in all BC Government APIs. The standard date format is YYYY-MM-DD while timestamp format YYYY-MM-DD HH24:MI:SS. If other formats are required due to source system limitations, convert it to the standard format within the API
- **Support Official Languages** – ensure the API can return responses in both English and French. External facing APIs must reply with content in the requested language if the backend data support it. APIs must interpret the ACCEPT-LANGUAGE HTTP header and return the appropriate content. If the header is not set, then content in both languages should be returned

API Documentation

BC Government APIs must be published to the [BC Government API Registry](#) to be discoverable. The documentation MVP for BC Government APIs includes everything the API does, including resources, endpoints and methods, parameters, error codes, and example requests and responses:

- **Publish OpenAPI Specification** – OpenAPI is a machine-readable interface specification for RESTful APIs. There are open source tools (e.g., [Swagger](#)) which can then generate human-readable documentation from this specification which avoids the need to create and maintain separate documentation
 - Sample BC Government API Specifications can be found [here](#)
- **Publish code samples and test data** – the most effective way to document the scope and functionality of an API is to publish the code and data examples used to validate it alongside the API contract



- **Maintain concise documentation** – if there is a need to extend the API documentation beyond the OpenAPI specification, this is an indication that the API is too large and/or too complex
 - Be sure to document differences between versions of the API
 - Include documentation on any consumption constraints such as availability, authorization and rate limiting
- **Gather Feedback** – provide a clear mechanism to allow consumers to provide feedback, issue identification and enhancement requests
 - The BC Government API Registry can be found here: <https://catalogue.data.gov.bc.ca/group/bc-government-api-registry>
 - The BC Government API Github Repo can be found here: <https://github.com/bcgov/api-specs>
 - Provide a point of contact in the API documentation such that consumers can seek assistance if required

API Consumption

The best way to validate your API design is to consume it with a production application within your organization. Ideally, once the data layer is built, the next step is to build the application on top of an API:

- **Build once for Multiple Channels** – APIs should be designed in such a way that they can be consumed by systems internal to BC Government, external agencies and the broader public. Design should accommodate for all levels of access to encourage reuse
- **Consume what you Build** – build your application on top of an API layer that connects to the data layer rather than creating hard dependencies. This ensures the API is production ready for consumers outside of the line of business

API Lifecycle Management

APIs will change over time as corresponding source systems evolve. To provide a robust and durable interface to applications, API lifecycle management must include a standard versioning scheme such that any changes to an API do not break the contract with existing consumers:

- **Use Standard Endpoints** – each endpoint is a combination of the URI path (e.g. www.gov.bc.ca/finances/accounts/) and the verb (e.g. GET, PUT, POST, DELETE)

<https://<base domain>/<business function>/<application name>/<plural noun>>
- **API Versioning** – each iteration of an API that changes the response type, data format, API functionality or breaks the contract with consumers must be versioned. Follow the `v<Major>.<Minor>.<Patch>` versioning structure whereby:
 - *Major* = Significant release that introduces incompatible API changes
 - *Minor* = Addition of optional attributes or new functionality that is backwards compatible, but should be tested
 - *Patch* = Internal fix which should not impact the schema and/or contract of the API



- moving from v1.1.0 to v1.1.1 would allow a simple deploy-in-place upgrade
- moving from v1.1.0 to v2.0.0 would be a major release and would require the legacy version to be kept while consumers test and migrate to the new version
- **URI vs Accept Header Versioning** – both URI and Accept Header versioning are acceptable and the following guidelines are recommended:
 - Using a resource specific header approach can be used to maintain a single and consistent URI for an API. This method also allows for other parameters such as caching, compression and content negotiation
 - The base URI for the API should always correspond to the latest version
 - e.g. <https://api.example.com>
 - Previous versions of an API can use a versioned style URI
 - e.g. <https://api.example.com/v1>
 - Accept header versioning is recommended for API's designed exclusively for machine to machine interfaces as well as non breaking changes (minor/patch)
 - e.g. <https://news.api.gov.bc.ca/api/Home?api-version=1>
- **Respect Existing Consumer Dependencies** – support at least one previous major version (N-1) to ensure consuming systems have time to migrate to the latest version of the API
 - Set and publish a version deprecation policy and timeline so consumers can plan their dependencies accordingly
 - Ensure adequate testing on all minor and major releases
 - Backport high value changes to the previous (N-1) version where version integrity can be maintained
 - Provide a way to gather feedback from consumers to inform future development
- **API Ownership** – publish and maintain a designated point of contact to the API Registry as part of the metadata record; including name, organization, email and phone (for high critically API's)
- **Define an SLO up Front** – each API should have a clearly defined Service Level Objective (SLO), which should include:
 - Support contact and availability
 - Service uptime objective (e.g., 99%)
 - Support response time (e.g., within the hour, 24 hours, best effort)
 - Scheduled outages (e.g., nightly, weekly, every 2nd Sunday evening)
 - Throughput limit (e.g., 100 requests per second per consumer)
 - Message size limit (e.g., <1Mb per request)
- **API Publishing** – all APIs should be published to the API Registry for the purposes of discovery and lifecycle management. APIs must be tagged with the appropriate metadata to indicate their desired audience (security classification) and appropriate usage patterns
 - Publishing a metadata record to the [BC Government API Registry](https://developer.gov.bc.ca/Data-and-APIs/BC-Government-API-Guidelines) helps people discover your API and promote its use



- If the API is an Open Data API, publish a terms of use, such as the example found [here](#)

API Performance Management

API performance should be benchmarked periodically to ensure the performance and capacity meets the expectations of the SLO. This may include:

- **API Load Testing** – run performance tests against the API using a simulated workload to determine the response time and throughput. Performance tests should be integrated into the development lifecycle, preferably through an automated CI/CD pipeline
- **Publish Performance Data** – performance summaries (e.g., average response time) should be included in the metadata record for the API as well as the SLO
- **Performance Monitoring** – performance should be monitored and reported on routinely, particularly as part of major releases
- **API Throttling** – throttling mechanisms should be implemented to control throughput against the stated SLO (e.g. number of requests per second). This is typically handled by the API Gateway:
 - Information on the primary BC Government API Gateway can be found [here](#)

[Create An Issue](#)



Guidelines on the Use of Open Source Software

Release 1.0 April 2012

Architecture, Standards and Planning Branch

Office of the CIO • Province of BC

People • Collaboration • Innovation

Guidelines on the Use of Open Source Software

This document is prepared by the Office of the Chief Information Officer (OCIO) for the Province of British Columbia. It provides a Provincial perspective on the use of open source software. It discusses the business benefits and risks that are associated with the use of open source software and provides principles and guidance for adopting open source software by the Province of British Columbia.

This document addresses the use of open source software. The modification and re-publication of open source software by the Province of British Columbia leads into topic areas not addressed in this document.

Introduction

The purpose of this document is to introduce its readers to the topic of open source software and to offer some guidance for the use of open source software by or on behalf of the Province of British Columbia.

The term “open source software” or OSS refers to software applications that are made available in source code form under a license agreement that imposes very few restrictions on the use, modification and redistribution of the source code. Open source software is commonly made available at no cost.

The OCIO position on open source software is neutral: there is no overarching preference for commercial software or for open source software. The choice of a software solution should be based on the business value proposition, the total cost of ownership and an assessment of the associated risks.

Open source software development began as a small cottage industry. Over the past 30 years the open source movement has steadily grown and evolved. Today open source is a recognized strategy that organizations may choose to meet their needs and pursue their goals. This document offers guidance on things to consider when open source software is being proposed or evaluated for use by the Province of British Columbia.

How is Open Source Different from Proprietary Software?

Traditional proprietary software involves a variety of restrictions imposed through a license agreement. The aims of these restrictions are to protect the property rights of the author. The open source software community takes an approach that emphasizes the rights of the user.

Open source software is licensed to users with the following freedoms:

- The software may be used for any purpose.
- The source code may be studied and modified.
- The software may be redistributed without royalty payments or other restrictions.

It is these kinds of freedoms that are foundational to open source software. They provide the transparency needed for community peer review, which improves quality and robustness.

Secondly, open source is developed primarily by volunteers. Although in recent years development is increasingly done by “paid volunteers” from the private sector. Development is hosted on the Internet, which means that volunteers can collaborate from anywhere on the planet. The volunteers themselves vary in ability from hobbyists and amateurs to dedicated professionals and subject matter experts. Their motives range from communitarianism to enlightened self-interest.

Thirdly, the development process itself is highly transparent. When issues emerge about the viability or direction of a project they are usually highly visible. This is good, because not all open source software projects are robust. And no one wants to deploy a system only to discover later that the system has a doubtful future.

Why is a Clear Definition for Open Source Software Important?

In the marketplace, software is distributed under many types of licenses: shared source, community source, shareware, freeware and others. The proliferation of license types leads to misunderstandings and incorrect assumptions about open source software. This situation is further compounded by the difficulty the average person has understanding license agreements.

There is an easy way to simplify this problem. The Open Source Initiative (OSI) is an organization established to promote open source software. The OSI publishes an Open source definition that is widely accepted. Furthermore the OSI has a process for reviewing and approving licenses. They publish a list of licenses (currently around 70) that conform to the OSI definition.

The OCIO recommends that the Province use the term “open source software” to refer exclusively to “software that is distributed under a license that is endorsed by the Open Source Initiative (OSI)”.

In practice, 9 of the 70 OSI endorsed licenses are the most widely used ones. Thus, adhering to a standardized definition of “open source software” should help streamline the procurement process by limiting the amount of intervention needed to ensure the Province’s rights and obligations are understood and acceptable.

What Advantage is Open Source Software from an Organizational Perspective?

Less process. Open source software rarely involves an up-front purchase cost. Therefore, acquiring open source software can involve fewer approvals, fewer meetings, less process and delay resulting from the financial approvals process inside government. When facing deadlines less process is a welcome.

Greater flexibility. Licensing open source software does not involve negotiating a contractual agreement for the software. No contract means less commitment, which in turn means the Province has more flexibility if plans need to change.

Better sustainability. Market forces can undermine the sustainability of a software product. A software system can become redundant through the consolidation of an overcrowded market or through strategic mergers and acquisitions. Adopting an open source solution is a strategy to help insulate I/T investments from external market forces. Having “open source” rights to the application code reduces dependencies.

Greater freedom. In the open source model of development third party vendors compete to offer software support. Having “open source” rights to the application code ensures vendor lock-in is not a concern.

Self determination. Open source systems are developed in an open, collaborative manner. Supporters can exert an influence on a system's direction. Users have direct input into improvements and setting priorities.

What are Some Potential Legal Issues of Using Open Source Software?

In simply acquiring and deploying open source software, an area of concern is the potential consequences of unwittingly infringing the intellectual property (IP) rights of someone. This can happen when software includes code of disputed ownership. IP infringement can result in disruption and/or have negative financial consequences to the end user.

The uncertain possibility of IP infringement via open source software is best dealt with through risk management. Evaluate the risk. How likely is the risk? What are the consequences? Is the risk acceptable or should it be mitigated? What options are available to mitigate such risk? What steps would a reasonable person take?

Some open source software is marketed with user indemnification bundled into the product. Third party insurance is also available that indemnifies users of designated open source software. Services are also available that review and rank open source software in accordance

with its various aspects of interest to prospective users (i.e., a kind of Consumer Reports approach.). For further advice on managing risks you may wish to consult the Province's Risk Management Branch.

Another consideration is the Province's existing legal/contractual arrangements. Not all software licenses can be assumed to be mutually compatible¹. Core policy requires a legal review of the contract terms for new software licenses, both open source and proprietary.

More information and assistance may be available through the Province's Legal Services Branch.

What are the Operational Issues of Open Source Software?

Under the open source software development model the source code is open to public scrutiny and peer review. Thus any coding vulnerabilities in a system can be spotted and quickly fixed. Unfortunately this also means vulnerabilities can be spotted and quickly exploited too. It is common practice that attacks are developed that target known vulnerabilities on unpatched systems.

It is important that software, open source or proprietary, be maintained in a timely, systematic manner. Security advisories should be monitored and reviewed regularly. Patches should be applied soon as they become available. Updates should be applied as soon as practicable. Systems of concern (i.e. for which the risks are greater) should maintain a "system security plan"². The responsibility lies with the business program area to ensure that risks are being assessed and business application software is being properly maintained.

Business continuity is another important consideration. Critical business functions need to be available to users and customers on demand. When selecting software a business area should ask itself questions about the impact of open source on business continuity. There are many aspects to consider. How long has the project existed? Is the project healthy, well organised? Does it have a corporate sponsor? Is the software mature or underdeveloped? Are software updates published on a regular basis? Does the project publish a technology roadmap? Is the

¹ Commonly heard is that the Province's Oracle license prohibits the use of Oracle products in combination with any software released under the GNU license. The Province's primary Oracle license contains no such prohibition.

² SANS offers the following explanation: The purpose of the system security plan (SSP) is to provide an overview of the security requirements of the system and describe the controls in place or planned, responsibilities and expected behaviour of all individuals who access the system.

software in wide use? Is there a stable community of users? Have they voiced issues with the project?

The impact of open source on business continuity should be understood and managed accordingly. Consider some questions like: “what would we do if...”. Managing risk means having a mitigation plan. Once fully understood a risk may be worth taking, or not. Either way the decision should be informed by facts. This approach is much less stressful than depending on opinions.

Help with risk management is available through the Province’s Risk Management Branch and the Information Security Branch. Third party services are available that rank open source software in accordance with its various aspects of interest/concern to prospective users.

Open source software may be acquired for free, but maintaining any software in a production environment costs money. Factor the ongoing costs into the cost of the decision.

Principles for Adopting Open Source Software

1. The OCIO recommends that open source licensed software be defined as “any software that is distributed under a license endorsed by the Open Source Initiative”.
2. Open Source Software must be given impartial consideration (alongside proprietary software) when being proposed in response to a procurement.
3. The choice of software should be based on the business value proposition, the assessment of the associated risks and compliance with standards.
4. Acquirers must ensure their intended use of open source software is compatible with the software’s license terms.
5. Acquirers must ensure that the sources used for downloading and updating open source software are trustworthy.
6. Acquirers must undertake to keep their open source software patched and up-to-date, consistent with best security practice.

Further Guidance

- The OCIO endorsement of OSI approved licenses is not an endorsement for the use of any proposed software.

- The use of open source software (and proprietary software) must meet the Province's requirements for privacy and security.
- All software selections should be suitable for integration with existing infrastructure investments, such as identity management.
- Software distributed under licensing agreements known as "freeware", "shareware", "community source" or "shared source" (i.e. not OSI approved) are not endorsed by the Province unless authorized by the OCIO on a case by case basis.
- The acquirer must ensure that contracted providers of software notify the Province of any open source software components used in a deliverable.
- Core Policy Chapter 6 requires that all information technology procurement be done through Shared Services BC³.
- Acquirers must follow the STRA standard to evaluate the risks of software plans by using the Province's Information Security Management and Risk Tool (iSMART).
- The Province's Legal Services Branch and Risk Management Branch may be able to provide additional assistance.

Glossary

Acquirer – an employee, contracted resource, program area or business unit that acquires software for or on behalf of the Province of British Columbia.

Total Cost of Ownership - is a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system.

³ Chapter 6 of CPPM applies when downloading and running of opens source software on behalf of the Province.

References

Open Source Definition:

<http://www.opensource.org/osd.html>

OSI Approved Licenses:

<http://www.opensource.org/licenses/alphabetical>

Example of Vendor Indemnification:

<http://www.oracle.com/us/technologies/linux/ubl-indemnify-066152.pdf>

Example of Third Party Indemnification coverage:

<http://www.openlogic.com/products/indemnification.php>

Ministry of Finance, Risk Management Branch:

<http://www.fin.gov.bc.ca/PT/rmb/index.shtml>

Ministry of Labour, Citizen's Services and Open Government: Information Security Branch

<http://www.cio.gov.bc.ca/cio/informationsecurity/index.page>

Questions about this document? Please e-mail ASB.CIO@gov.bc.ca



Physical Address and Geocoding Standards

Conceptual Model

Version 1.0

Prepared by

***Michael Ross, DataBC
Enterprise Data Services***

Mar 15, 2010

Document Control

Date	Author	Version	Change Reference
May 29, 2009	Michael Ross, GeoBC	Draft v0.3	Initial Release
June 16, 2009	Michael Ross, GeoBC	Draft v0.4	Incorporated internal review comments
June 24, 2009	Michael Ross, GeoBC	Draft v.0.5	Incorporated review comments by geocoder vendor (Refractions Research)
June 29, 2009	Michael Ross, GeoBC	Draft v0.6	Incorporated review comments from June 25 presentation to NRSIWG
Sep 30, 2009	Michael Ross, GeoBC	Draft v0.7	Incorporated comments from Aug 26 NRSIWG review meeting including VIHA and Elections BC reps; revised introduction and scope; added context section; added support for non-civic addresses; added high level Site class diagram; expanded definition of geocoder operation
Nov 23, 2009	Michael Ross, GeoBC	Draft v0.8	Reorganized document into information model and service model sections. Elaborated on application/geocoder interaction in section 3.2.5 Added geocoding examples, concordance, and business context Incorporated feedback from Ministry of Small Business and Revenue (K Hatch)
Nov 25, 2009	Michael Ross, GeoBC	Draft v0.81	Revised definition of physical address.
Feb 9, 2010	Michael Ross, GeoBC	Draft v0.9	Incorporated feedback from ASRB review; removed compliance schedule Fixed OCL definition of PhysicalAddress.SiteName; expanded definition of PhysicalAddress.addressString and added examples; revised queryAddress parameter description in section 3.4.2 Restructured CivicAccessPoint into AccessPoint, CivicAddressPoint, NonCivicAddressPoint Added retire date to Site and AccessPoint In section 2.1, added retire date for site and accessPoint; added fullSiteDescriptor In section 2.2.6, fixed problems in OCL with civic and non-civic address operations Added geocoding examples (section 3.6) Improved OCL of geocoder operations (section 3.4) In section 3.4.2, added more examples of unstructured addresses Made minor edits throughout

Date	Author	Version	Change Reference
Feb 19, 2010	Michael Ross, GeoBC	Draft v0.91	<p>In section 2.1.3, simplified presentation of address string formats and examples</p> <p>In section 3.2.2 added some missing standardization steps</p> <p>In section 3.4.2, simplified presentation of queryAddress formats and examples</p>
Feb 25, 2010	Michael Ross, GeoBC	Draft v0.92	<p>Added the concept of a street intersection; sections 2 and 3 updated</p> <p>In section 1, redefined physical address to include both site and street intersection addresses.</p> <p>In section 2, renamed PhysicalAddress SiteAddress to support new definition of Physical Address.</p> <p>In sections 2.3.1, 2.3.2.2, 2.3.6.9, added fullName operation to Street</p>
Mar 1, 2010	Michael Ross, GeoBC	Draft v0.93	<p>Incorporated latest feedback from ASRB</p> <p>In section 1.5, expanded discussion of security and privacy issues and added note on legal disclaimer.</p> <p>In section 3.3, Added copyrightNotice, copyrightLicense, disclaimer, and privacyStatement attributes to Geocoder, SearchResults, and IntesectionSearchResults</p> <p>Made some minor edits throughout</p>
Mar 10, 2010	Michael Ross, GeoBC	Draft v0.94	<p>Incorporated latest feedback from ASRB</p> <p>In section 1.4, Out of Scope, added Address Data Management</p> <p>In section 1 Introduction, added section 1.7 Related Standards</p> <p>In section 3.4.1 changed setBack type from integer to Real</p> <p>In section 3.4.2 added SetBack:Real to parameter list</p>
Mar 15, 2010	Michael Ross, GeoBC	V1.0	released
Aug 30, 2012	Michael Ross, DataBC	V1.0.1	Minor corrections only; updated gov't organization names

TABLE OF CONTENTS

1. INTRODUCTION	7
1.1 TERMINOLOGY	7
1.2 APPLICABILITY	8
1.3 EXEMPTIONS	8
1.4 SCOPE	8
1.5 SECURITY, PRIVACY, AND LEGAL CONSIDERATIONS	10
1.6 CONTEXT	10
1.6.1 Business Context	10
1.6.2 Standards Context	11
1.7 RELATED STANDARDS	12
2. INFORMATION MODEL	13
2.1 SITE ADDRESS	13
2.1.1 DataType Diagram	13
2.1.2 DataType Definition	14
2.1.3 Attribute Definitions	14
2.2 STREET INTERSECTION ADDRESS	19
2.2.1 DataType Diagram	19
2.2.2 DataType Definition	19
2.2.3 Attribute Definitions	19
2.3 SITE, STREET INTERSECTION, AND RELATED CLASSES	21
2.3.1 Class Diagram – High Level	21
2.3.2 Class Diagrams – Detail	22
2.3.2.1 Site, AccessPoint, BlockFace, Block	22
2.3.2.2 Street, StreetIntersection, Locality	23
2.3.3 Class Definitions	24
2.3.4 Attribute Definitions By Class	25
2.3.4.1 Site	25
2.3.4.2 SiteAlias	26
2.3.4.3 AccessPoint	26
2.3.4.4 CivicAccessPoint	26
2.3.4.5 BlockFace	27
2.3.4.6 Block	27
2.3.4.7 Street	28
2.3.4.8 StreetAlias	29
2.3.4.9 StreetIntersection	29
2.3.4.10 Locality	29
2.3.4.11 LocalityAlias	29
2.3.4.12 Province	30

2.3.5	Relationship between Site Address and Site	30
2.3.6	Operations by Class	30
2.3.6.1	Site.....	30
2.3.6.2	SiteAlias	34
2.3.6.3	AccessPoint	35
2.3.6.4	CivicAccessPoint.....	35
2.3.6.5	NonCivicAccessPoint	36
2.3.6.6	Integer.....	37
2.3.6.7	BlockFace	37
2.3.6.8	Block	39
2.3.6.9	Street	40
2.3.6.10	StreetIntersection	40
2.3.7	Constraints.....	40
2.4	GEOMETRY	41
2.5	CHANGE TRACKING	42
2.6	DATA ELEMENT CONCORDANCE	42
2.7	ADDRESS EXAMPLES.....	43
2.7.1	A Single Site with A Single Address	44
2.7.2	A Single Building with Addresses on Two Streets.....	45
2.7.3	A Mobile Home Park	46
2.7.4	A Five Acre Lot with a House Set Back From The Road.....	47
2.7.5	A House On a Five Acre Lot is Demolished and Replaced By New Houses	48
2.7.6	Two Buildings Assigned The Same Civic Number	49
2.7.7	One House with Two Addresses.....	50
2.7.8	A House Gets a new Civic Number	51
2.7.9	A Multiple Unit Dwelling	52
2.7.10	Two Addresses with The Same Street Name But Different Street Types.....	53
2.7.11	Two Buildings On The Same Natural Feature (Non-civic Addresses).....	54
3.	SERVICE MODEL (GEOCODER)	55
3.1	CLASS DIAGRAM.....	55
3.2	CLASS DEFINITION.....	56
3.2.1	Overview	56
3.2.2	Address Standardization	56
3.2.3	Match Quality	57
3.2.4	Positional Accuracy	58
3.2.4.1	Civic Addresses.....	58
3.2.4.2	Non-Civic Addresses	59
3.2.5	Using the Geocoder as an Address Hub in Client Applications.....	60
3.3	ATTRIBUTES.....	61
3.4	OPERATIONS.....	64
3.4.1	Geocode Structured Address.....	64
3.4.2	Geocode Unstructured Address	66
3.4.3	Geocode Street Intersection	68

3.4.4	Reverse Geocode Sites Inside An Area Of Interest	69
3.4.5	Reverse Geocode Street Intersections Inside An Area Of Interest.....	70
3.4.6	Reverse Geocode Street Intersections Near a Given Point.....	71
3.4.7	Reverse Geocode Sites Near a Given Point	71
3.4.8	Reverse Geocode Site Identifier	72
3.4.9	Reverse Geocode Street Intersection Identifier	73
3.4.10	Reverse Geocode Sites Within A Given Time Period and Area.....	73
3.4.11	Smart String Matcher	74
3.4.12	Site, Street, and Locality Name Expander	75
3.4.13	Circle in Square Generator	75
3.4.14	Geometry Reprojection.....	75
3.5	CONSTRAINTS	77
3.6	GEOCODING EXAMPLES	78
3.6.1	A Perfect Match	78
3.6.2	A Missing Street Direction	79
3.6.3	A Missing Civic Number.....	80
3.6.4	Interpolation Required.....	81
4.	REFERENCES.....	82

1. INTRODUCTION

Geocoding is the process of determining the geographic position (coordinates) of a street intersection, house, building, etc., from its physical address. Government has long expressed a need for a single, authoritative, physical address registry and geocoding service. This standard is an important step toward establishing such services.

1.1 Terminology

Civic Address means a site address in a part of the province that is administered by a civic address authority and includes a site name, unit, civic number, street name, and province.

Delivery Address means an address that describes a location with sufficient detail to allow delivery of physical goods.

GeoBC is the GEOBC Branch in the Integrated Resource Operations Division of the Ministry of Forest, Lands and Resource Operations.

Locality means a municipality, subdivision, community, Indian reserve, named natural feature, regional district, or aboriginal lands. The primary locality of a site is assigned by the appropriate administrative authority, not Canada Post. Direct location is represented by points in a coordinate reference system.

Mailing Address is an address that describes a location that can receive posted mail. Canada Post is the authority for mailing addresses in Canada.

MAY means that it is optional; often there is a practice to do something, however it is not a requirement.

MUST means an absolute requirement of the specification.

Non-civic Address means a site address in a part of the province not administered by a civic address authority and includes a site name, unit, locality, and province but not civic number and street name.

Physical address means the relative and direct location of a site or street intersection on the earth. Direct location is represented by coordinates (e.g., latitude, longitude) in a coordinate reference system. Relative location is represented by a site or street intersection address.

Site Address means the relative and direct location of a site on the earth. Direct location is represented by coordinates (e.g., latitude, longitude) in a coordinate reference system. Relative location is represented by a civic or non-civic address.

SHOULD means that there may exist valid reasons in particular circumstances to use alternate methods, but the full implications *MUST* be understood and carefully weighed before choosing a different course.

Site means a constructed geographic feature in British Columbia with known coordinates (latitude/longitude) and a site address that is needed in the conduct of provincial business. Examples of constructed geographic features include houses, cabins, permanent campsites, mobile home and RV parks, units within houses and buildings, buildings within complexes, stores, malls, offices, industrial plants, bandshell, golf courses, hospitals, universities, recreation centres, places of worship, parks, municipal pumping stations, hydro sub-stations, wharves, airports, train stations, and landmarks.

Street Intersection Address means the relative and direct location of the place where two or more streets meet or cross. Direct location is represented by a point in a coordinate reference system. Relative location is represented by the names of all the streets that meet or cross at the intersection.

1.2 Applicability

This standard applies to the conceptual models of information systems within core government that provide or consume geocoding services.

1.3 Exemptions

Exemptions to this standard may be granted through the OCIO Architecture and Standards Branch. See <http://www.cio.gov.bc.ca/legislation/standards/> for more information on the exemption process.

1.4 Scope

This standard defines a conceptual model of sites and street intersections in British Columbia, their associated physical addresses, and geocoding services.

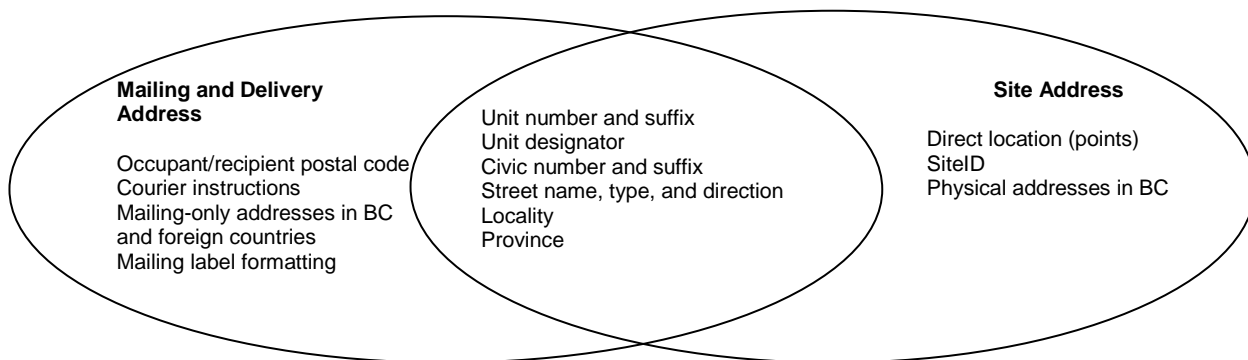
A geocoding service provides the following functions:

1. Address validation.
2. Address standardization.
3. Geocoding of both site and street intersection addresses.
4. Provision of unique site ids and street intersection ids for use in address maintenance by business applications.
5. Support for both real-time and batch operation (e.g., validation of a single address during form input and batch geocoding of one million addresses).

The following are out of scope:

1. Mailing and delivery address standards and requirements. This excludes:
 - a. Certain address elements such as site occupants and postal code
 - b. Mailing-only address types (e.g., lock box, rural route, and general delivery),
 - c. Mailing label formatting information
 - d. Courier instructions
 - e. Assignment of locality by Canada Post. Since this standard is about geocoding, not mail delivery, the locality of a site is that defined by the appropriate administrative authority. For example, an address in the municipality of Esquimalt will be assigned a locality of Esquimalt whereas Canada Post would assign a locality of Victoria.
2. Site classification and usage. This tends to be business specific and sensitive in many cases.
3. Identification of data sources for addresses, road network, and locality extents (i.e., boundaries).
4. Driving directions between two civic addresses. No routing functions are defined.
5. Civic address assignment and signage guidelines. This is the responsibility of each municipality.
6. Address data management and related access control. Only read access in support of geocoding is in scope.

The following diagram illustrates the differences between mailing/delivery address and site address:



The conceptual model consists of an information model that defines the classes and associations needed to represent sites, street intersections, and physical addresses; and a service model for geocoding.

All models are defined in the Unified Modelling Language 2.0 [R5]. Operations are defined in UML Object Constraint Language 2.0 notation [R6].

All geometric data types used in this standard (e.g., Point, Polygon) conform to the OGC Simple Feature Access specification [R4].

All time and date types conform to the BC Date and Time Standard [R18].

1.5 Security, Privacy, and Legal Considerations

This conceptual model can be used as the basis for a secure or public geocoding service implementation. Ideally, a public geocoder will be implemented for general use and secure geocoders will be implemented to suit specialized business needs. It is the responsibility of the geocoding service implementer to complete the required Privacy Impact Assessment and Security Threat and Risk Assessment.

Although there are no personal attributes in the conceptual model, a geocoding service that aspires to public access must not store any personal or sensitive information. Diligence is required to prevent this information from seeping in, particularly into the site name and narrative location attributes. For example, a site name of “Secret Military Installation 33412” reveals its sensitive classification and a narrative location that includes “follow the creek east two miles past Roy Roger’s Double R Bar Ranch” reveals personal information.

Given that some data used by a compliant geocoder may not be accurate, it is important to include an appropriate legal disclaimer with all geocoding service responses. See section 3.3 for details.

The conceptual model includes privacy statement, disclaimer, and copyright attributes as part of the Geocoder class definition (see section 3.3 for details).

1.6 Context

1.6.1 Business Context

Most government data has a spatial component which is usually an address. Address data is usually not represented spatially, denying many business areas the valuable techniques of geographic visualization and analysis. Address data is also not managed centrally which has led to duplication of effort, varying address data quality, and difficulty in sharing addresses across government.

Standardizing physical addresses and geocoding services enables common understanding and is a necessary step towards a government-wide distribution hub for all physical addresses in BC. Benefits of such a hub include the following:

1. Improved service delivery (e.g., fewer ambulances dispatched to the wrong address, fewer people not notified of emergency evacuations and oil and gas activity, fewer eligible voters not registered).
2. Increased revenue through more accurate application of tax laws (e.g., property tax assessment and administration).
3. Reduced cost of service delivery through more accurate geographic analysis (e.g., fewer non-residents approved for resident-only services, better fraud detection, fewer new facilities serving smaller than anticipated catchment populations).
4. Reduced cost of address management through the elimination of duplicate data, duplicate systems, and duplicate maintenance.
5. Increased sharing of address data across government.

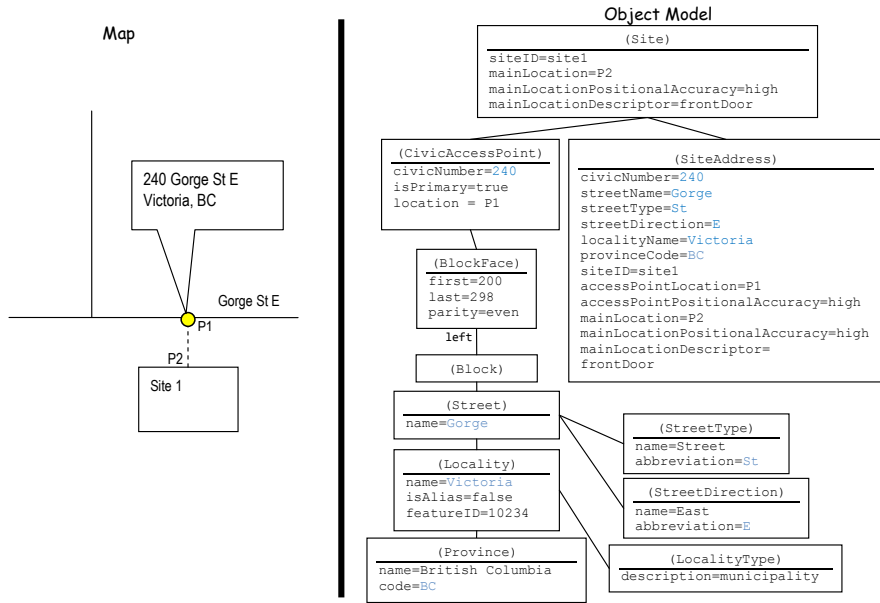
1.6.2 Standards Context

The Enterprise Geocoding Conceptual Model was derived from the original AddressBC conceptual data model [R14], the Canada Post Addressing Guidelines [R1], the BC Enterprise Civic Geocoder User Guide [R16], and the address model published by James Rumbaugh [R11]. The following address models and guidelines were also consulted:

- BC Mailing and Delivery Address standard [R7]
- Nova Scotia Civic Address Guide[R3]
- URISA Street Address Data Standard[R13]
- United States Postal Addressing Standards[R9]
- UK Spatial Datasets For Geographical Referencing B7666-2006[R10]
- ESRI Address Data Model for the City of Calgary[R12]
- ISO TC211 address standards proposals[R8]
- ISO 19112 – Geographic information – Spatial Referencing by geographic identifiers [R20]
- OpenGIS Location Service (OpenLS) Implementation Standards [R15]

What distinguishes the geocoding conceptual model from the Address BC Data Model and the BC Mailing and Delivery Address Standard?

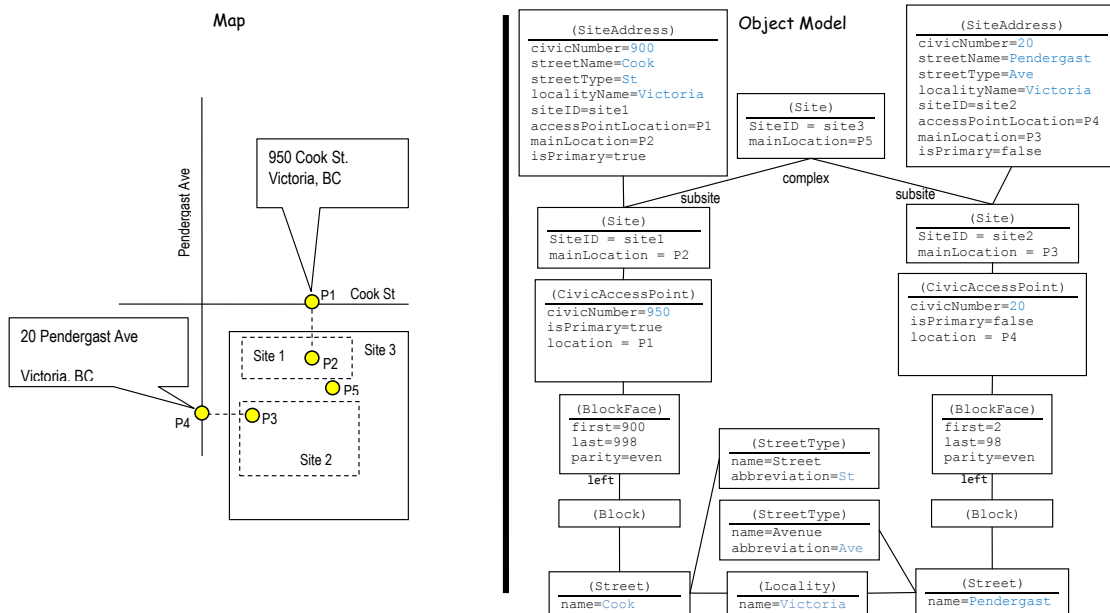
2.7.1 A Single Site with A Single Address



44

Version 1.0

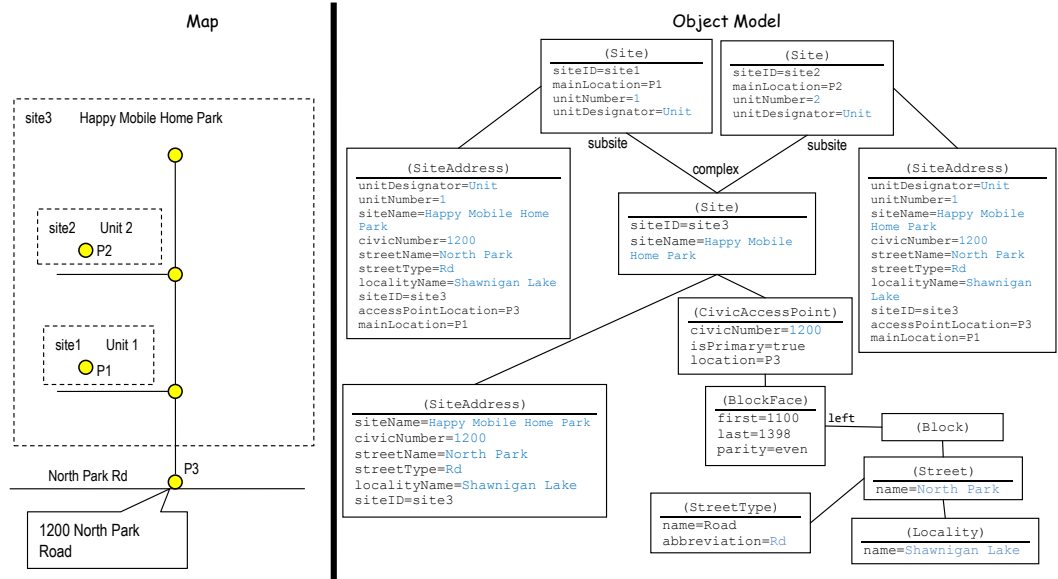
2.7.2 A Single Building with Addresses on Two Streets



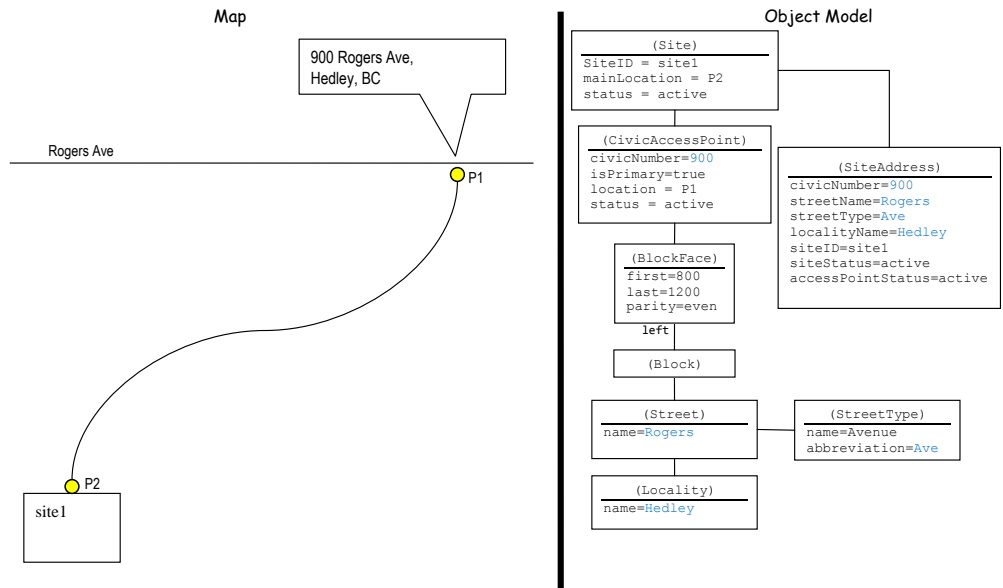
45

Version 1.0

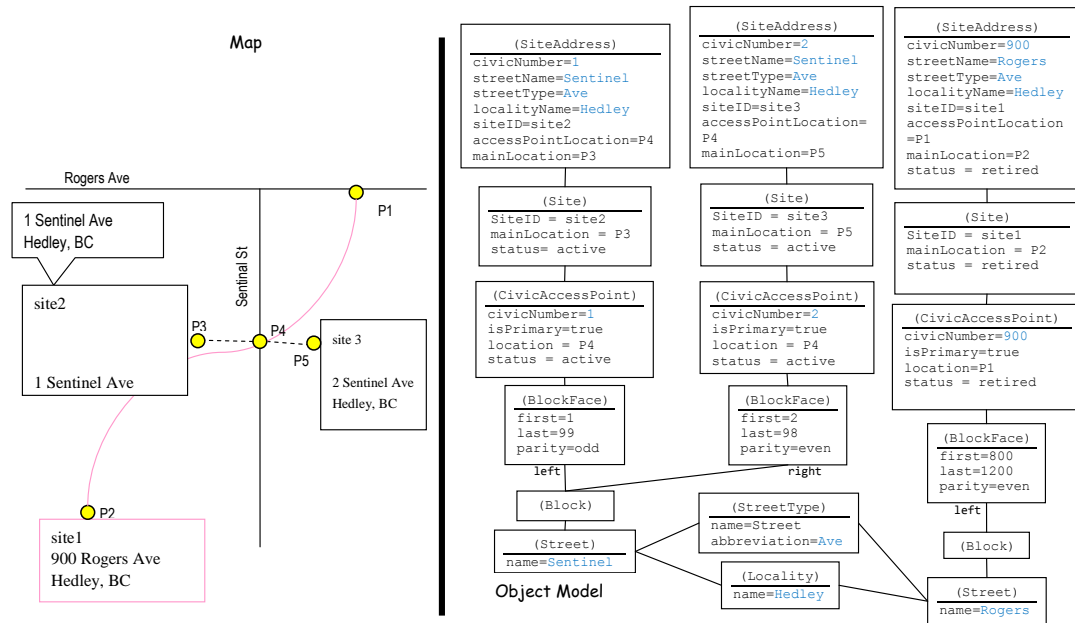
2.7.3 A Mobile Home Park



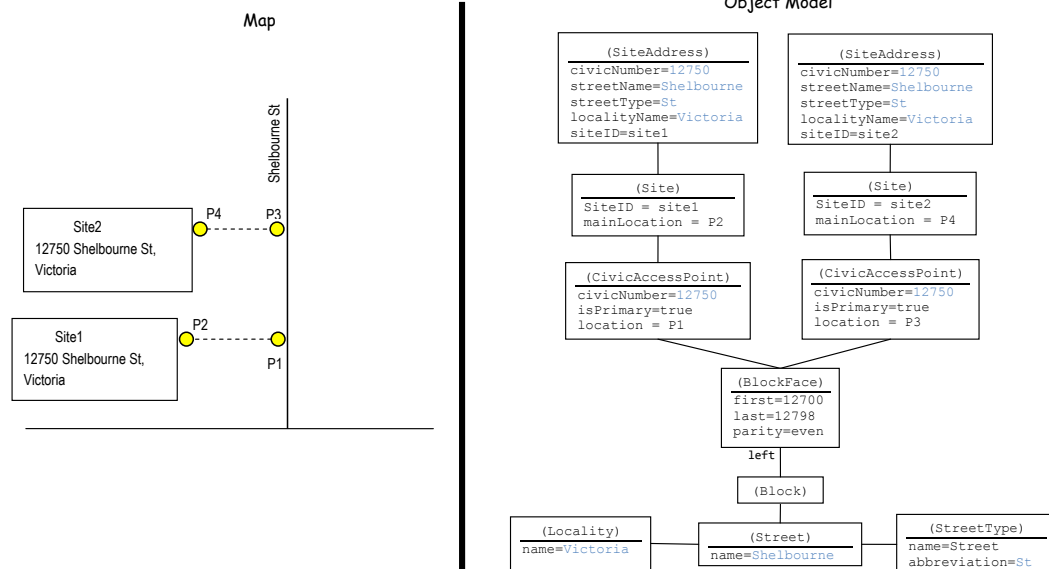
2.7.4 A Five Acre Lot with a House Set Back From The Road



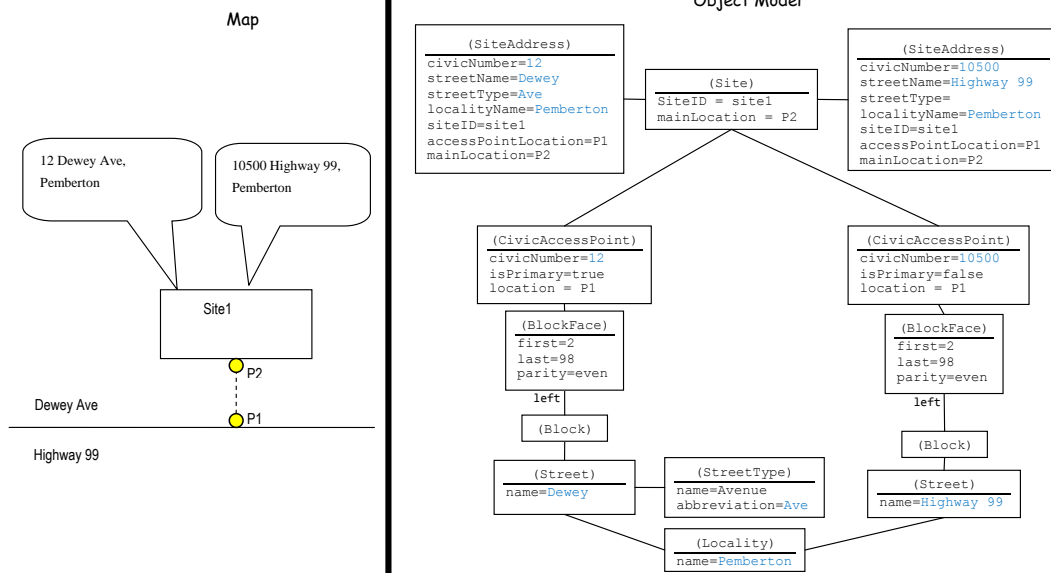
2.7.5 A House On a Five Acre Lot is Demolished and Replaced By New Houses



2.7.6 Two Buildings Assigned The Same Civic Number



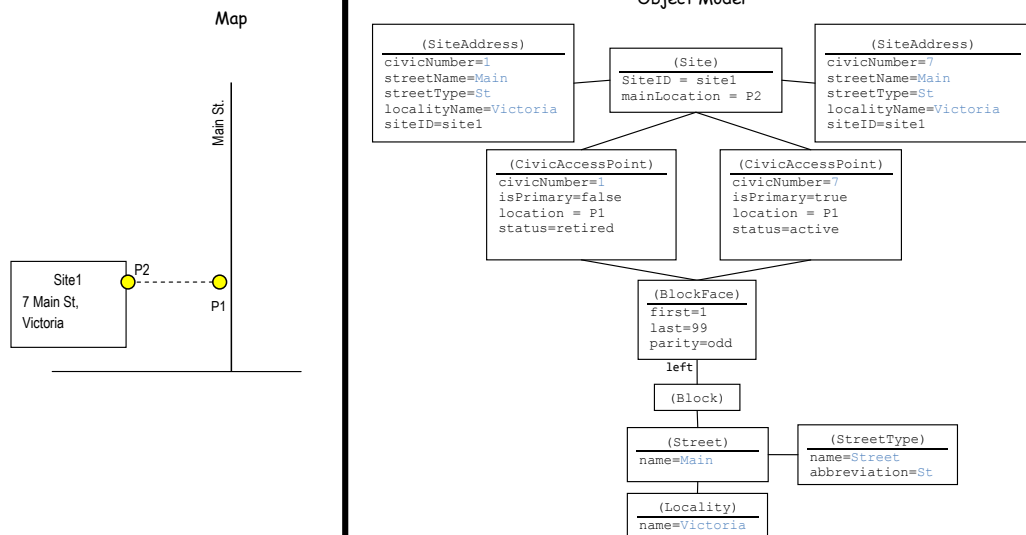
2.7.7 One House with Two Addresses



50

Version 1.0

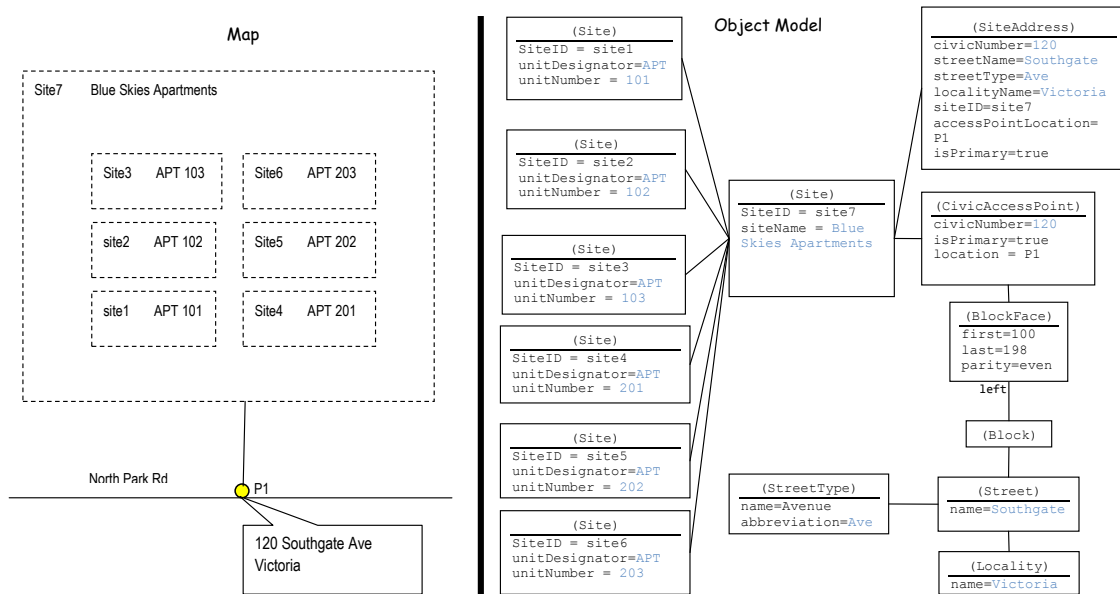
2.7.8 A House Gets a new Civic Number



51

Version 1.0

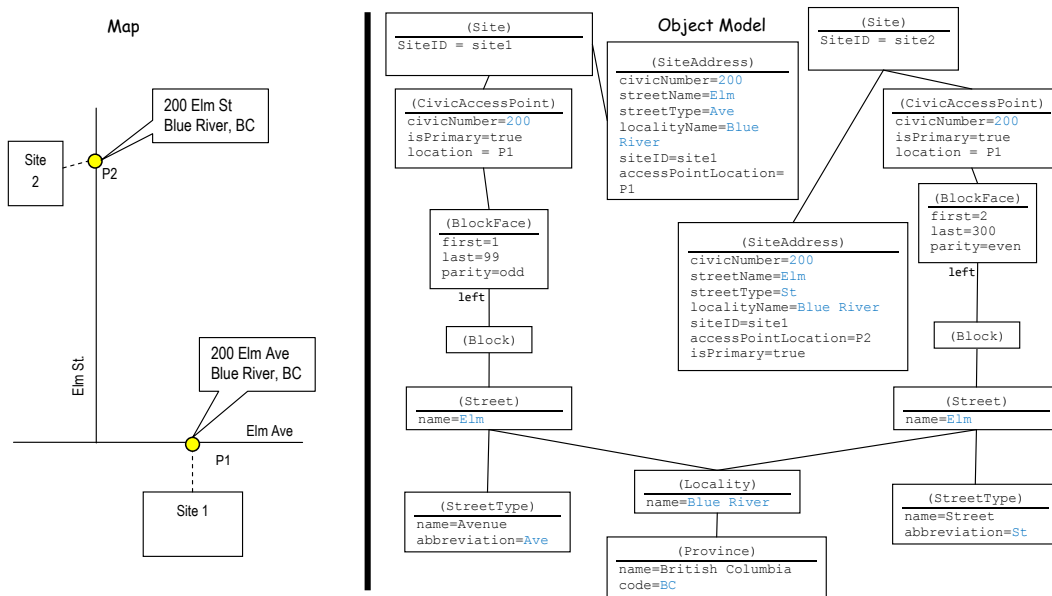
2.7.9 A Multiple Unit Dwelling



52

Version 1.0

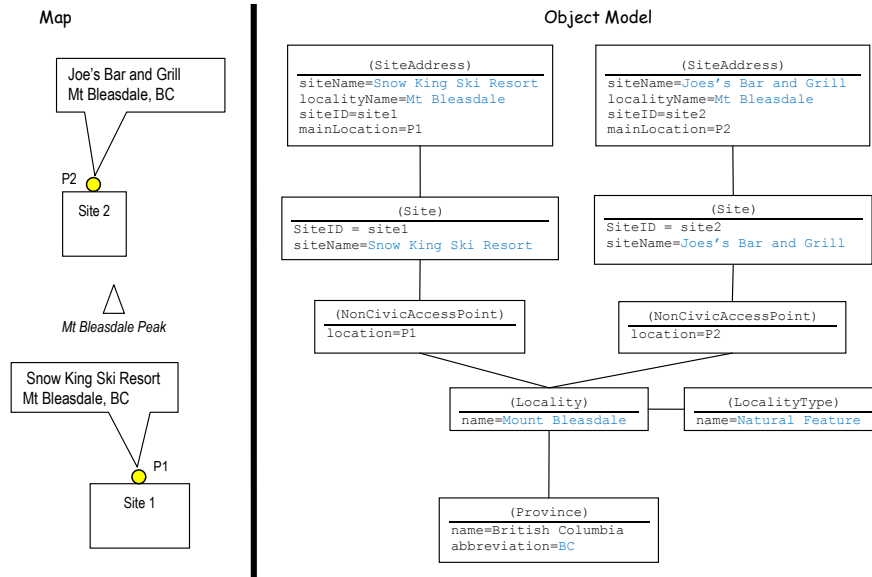
2.7.10 Two Addresses with The Same Street Name But Different Street Types



53

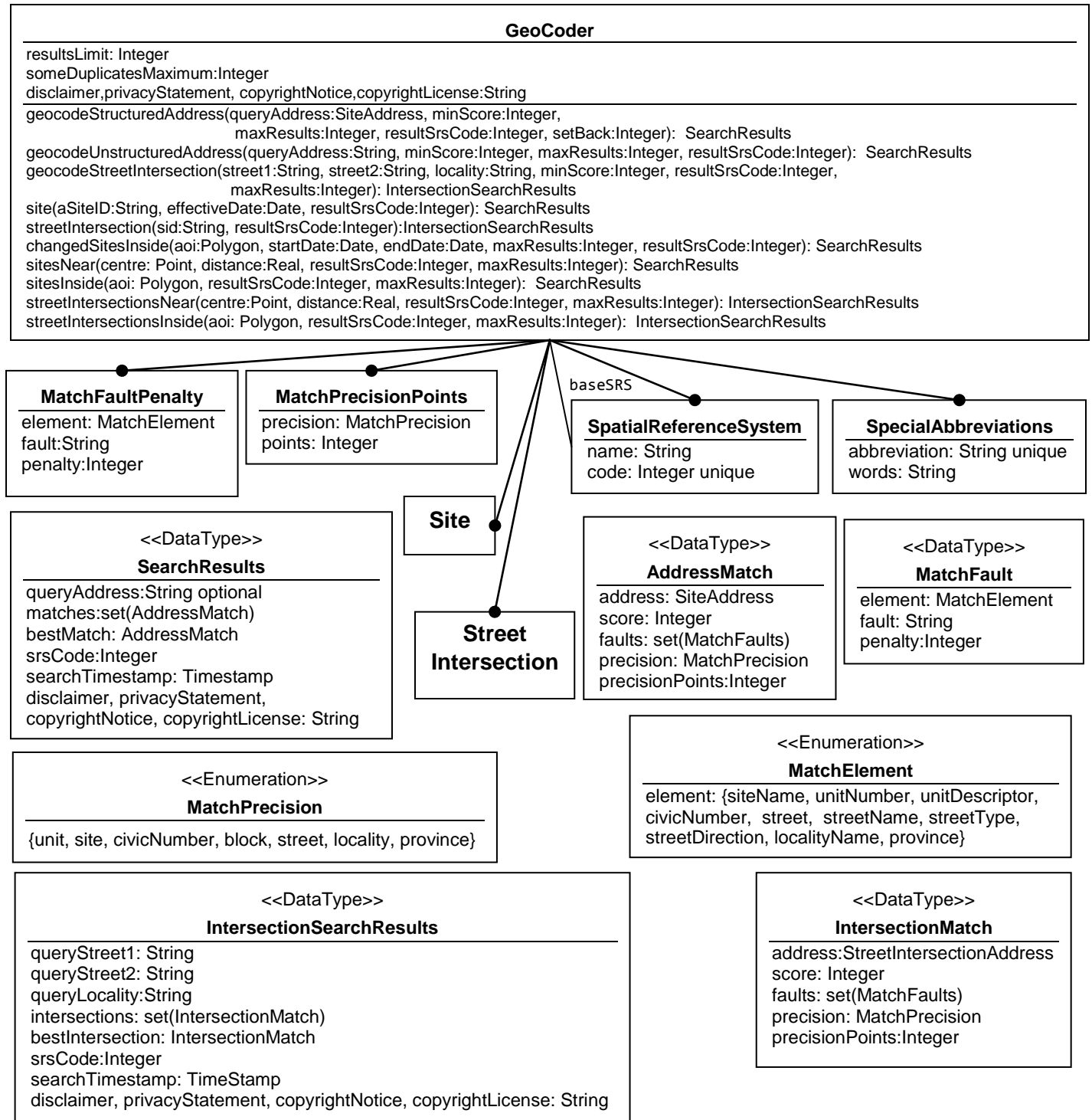
Version 1.0

2.7.11 Two Buildings On The Same Natural Feature (Non-civic Addresses)



3. SERVICE MODEL (GEOCODER)

3.1 Class Diagram



```
Context: Geocoder::streetIntersection(sid:String, resultSrsCode:Integer): SearchResults
```

3.2 Class Definition

3.2.1 Overview

The Geocoder class performs geocoding and reverse geocoding. Geocoding returns the geographic coordinates of a civic address, street intersection address, site identifier, street intersection identifier, site name within a natural feature, or site name within a locality. Reverse geocoding returns all addresses within a geographic area or near a geographic location.

The Geocoder is forgiving. It tries to correct spelling errors in input, overlook missing address elements, replace street and locality aliases, and return all matches regardless of match quality.

The SpatialReferenceSystem class defines the spatial reference systems that the Geocoder supports. A geocoder must support SpatialReferenceSystems with the following codes: lat/lon(4326), bc albers(3005), and UTM NAD83 Zones 7 - 11 (26907-26911). Additional spatial referencing systems may be defined. baseSRS is the SpatialReferenceSystem that all geometry is kept in.

SearchResults and AddressMatch are data types used to hold the results of a site address geocoding or reverse geocoding request. IntersectionSearchResults and IntersectionMatch are used to hold the results of a street intersection address geocoding request.

An AddressMatch conveys site address match quality through *score*, *precision*, and *faults* properties. MatchFault is a data type that defines the nature of the fault, the address property affected, and the fault penalty. MatchPrecisionPoints defines the points assigned to each match precision level. MatchPrecision is an enumeration of all precision levels. MatchFaultPenalty defines the penalty value of each possible fault. Penalties are subtracted from the appropriate precision level points to arrive at a match score.

An IntersectionMatch conveys street intersection address match quality in the same way AddressMatch does.

3.2.2 Address Standardization

Geocoding operations standardize their input addresses as follows:

- Abbreviated site names, street names, and locality names are expanded. For example, “W Broadway” is expanded to “West Broadway” and “N Vancouver” is expanded to “North Vancouver”
- Misspelled street names are corrected.

- Unabbreviated street types are abbreviated.
- Unabbreviated street directions are abbreviated.
- Missing street types and directions are added.
- Site aliases are replaced by their official sitenames (e.g., “Malaspina College” is replaced by “Vancouver Island University”)
- Street aliases are replaced by their official street names
- Locality aliases are replaced by their prime localities (e.g., “Fairfield” is replaced by “Victoria”).
- Unabbreviated province names are abbreviated.
- An alternate or retired address is augmented by its associated primary address. For example, if 5 Elm St. was retired and replaced by 7 Elm St, both 5 and 7 Elm St are added to the set of match results. For another example, if an input address is 5 Elm St, and the primary address for that site is 41 Maple Ave, both 5 Elm St and 41 Maple Ave are added to the set of match results.

Address as a single string is standardized and returned as the addressString attribute of a SiteAddress. See section 2.1.3 for further details.

3.2.3 Match Quality

An AddressMatch conveys match quality through precision level, faults, and overall score. MatchPrecision is an enumeration of all precision levels. MatchFault is a data type that defines the nature of a fault and the address element affected.

MatchPrecisionPoints defines the number of points for each match precision level. The maximum number of points allowed is 100. Recommended initial values are as follows:

Precision Level	Points
site	100
unit	100
civicNumber	100
block	95
street	40
locality	20
province	0

Here is the definition of each precision level:

- **province** – no match was found; lowest precision
- **locality** – the locality was matched but not the street, civicNumber, or siteName
- **street** – the street and locality matched but the civicNumber didn't match or fall within a block range
- **block** – the street and locality matched and the civicNumber falls within a block range
- **civicNumber** – the civicNumber, street, and locality matched; highest precision
- **unit** – the unitNumber, unitDesignator(if input), civicNumber, street, and locality matched; highest precision
- **site** – the site name and locality matched; if civicNumber and street were input, they matched too; highest precision

MatchFaultPenalty defines the penalty value of each possible fault. Determining penalty values is best done through trial and error.

MatchFault is a data type with the following attributes:

element is the name of the address element involved in the fault. Element values are defined in the MatchElement enumeration in section 3.1. Examples include **civicNumber**, **streetName**, and **locality**.

fault represents the nature of the fault. Examples include **isSiteAlias**, **isStreetAlias**, **isLocalityAlias**, **someDuplicates**, **manyDuplicates**, **spellCorrected**, **notMatched**, **missing**, **notinBlock** (only applies to **civicNumber** element), **misplaced**, and **notinLocality** (only applies to **street** element). So, for a given address match, the **civicNumber** element may be **notinBlock** (not found on any block of a given street), the **streetDirection** element may be **missing** and the locality element may be **spellCorrected** because it was spelled **Ross** instead of **Woss**.

penalty is the amount (between 1 and 100) that was subtracted from the appropriate MatchPrecisionPoints.

Match score is determined by taking the appropriate precision level points and subtracting any fault penalties. Match score must be between 0 and 100.

3.2.4 Positional Accuracy

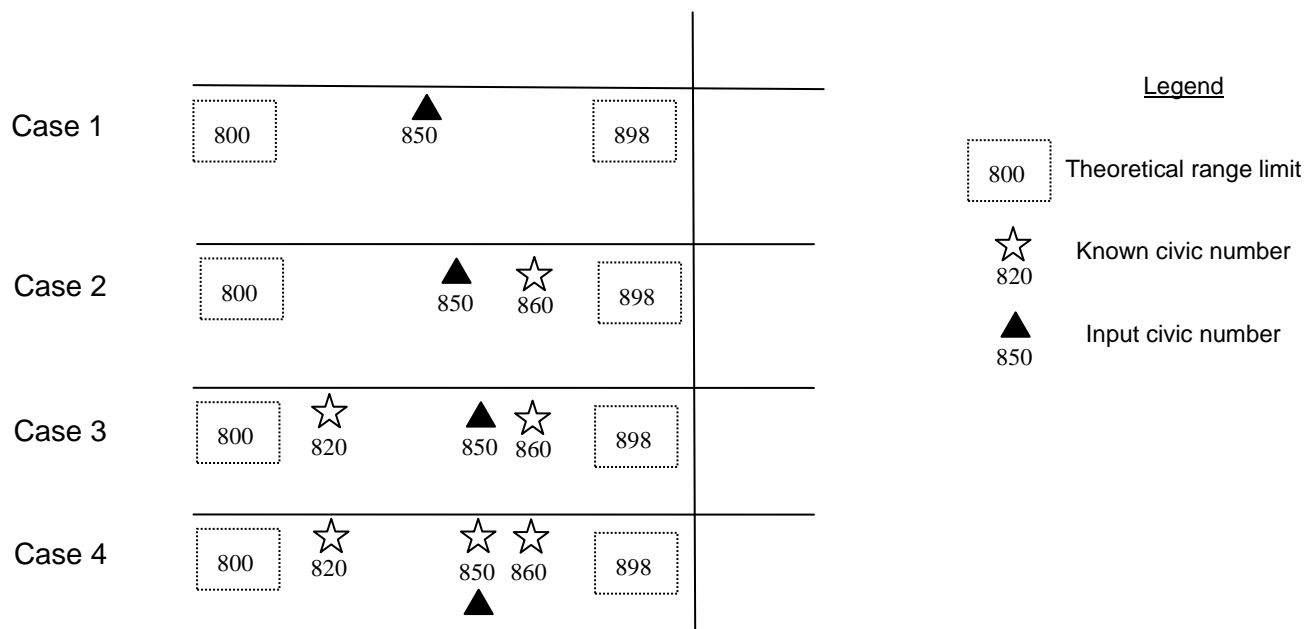
Positional accuracy is determined differently for civic and non-civic addresses.

3.2.4.1 Civic Addresses

To achieve the highest positional accuracy for civic addresses, the geocoder uses adaptive address interpolation which has four cases as follows:

1. The input address matches to a block range defined by two theoretical civic number limits. A linear interpolation is performed based on the block range and the input civic number.
2. The input address matches to a block sub-range defined by one known site access point and a theoretical civic number limit. A linear interpolation is performed based on the sub-range and the input civic number.
3. The input address matches to a block sub-range defined by two known site access points. A linear interpolation is performed based on the sub-range and the input civic number.
4. The input address matches to the civic number of an associated site.

Interpolation accuracy of all cases is illustrated in the following diagram:



Since there is no interpolation involved in case 4, the geocoder would return the value of `CivicAccessPoint.positionalAccuracy`. For cases 1-3, the geocoder will return an `accessPointPositionalAccuracy` of **medium**.

3.2.4.2 Non-Civic Addresses

To achieve the highest positional accuracy for non-civic addresses, the geocoder will utilize the site name, main location, and locality. Here are three cases:

1. The input address matches to a site name within a locality and the site's *mainLocation* is defined. The returned *accessPointLocation* is set to the value of *mainLocation* and *accessPointPositionalAccuracy* is set to *mainLocationPositionalAccuracy*.

2. The input address matches to a *siteName* within a *locality* but the site's *mainLocation* is not defined. The returned *accessPointLocation* is set to the value of *locality.asPoint* and *accessPointPositionalAccuracy* is set to **low**.
3. The input address doesn't match a *siteName* but does match a *locality*. The returned *accessPointLocation* is set to the value of *locality.asPoint* and *accessPointPositionalAccuracy* is set to **low**.

SearchResult and AddressMatch are used to hold the results of an address geocoding or reverse geocoding request.

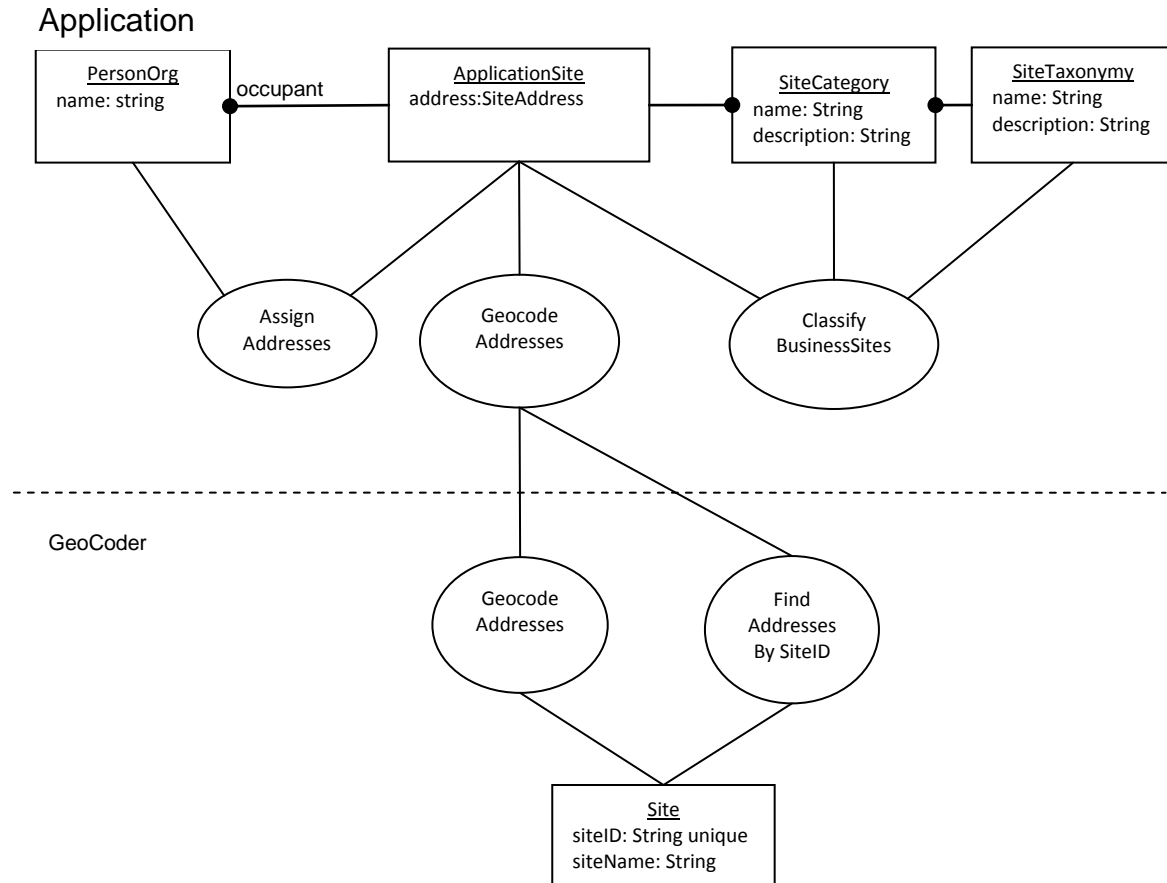
IntersectionSearchResults and IntersectionMatch are used to hold the results of a street intersection geocoding request.

3.2.5 Using the Geocoder as an Address Hub in Client Applications

The geocoder class was designed to allow applications to update their own addresses and on their own schedules. Here's an update scenario:

1. A client application uses the geocoder to geocode a set of addresses and stores the results. Addresses that matched down to the site level will include a unique, immutable siteID.
2. According to a business area's own update schedule,
 - a. A client application makes a request to the geocoder for all sites that have changed since a given date and applies the changes as appropriate.
 - b. Addresses in the client application that weren't initially matched down to the matchPrecision level of site are batch geocoded and changes are stored as appropriate. See section 3.2.3 for a discussion of match precision levels.

The following diagram illustrates the scenario described above:



The application avoids having to manage Site, AccessPoint, BlockFace, Block, Street, Locality, and Province objects by using a single ApplicationSite.address property of type SiteAddress instead. Use of such a denormalized value doesn't risk update anomaly because ApplicationSite.address is never updated; it is only replaced in its entirety by a new value returned by the geocoder. As is common with applications that manage addresses, the application in the diagram also tracks site occupants and classifies sites according to multiple, application-specific taxonomies.

An application can manage street intersection addresses like civic and non-civic addresses with the intersectionID playing the same role as siteID.

The need for information sharing agreements should be considered by each project implementing a multi-agency, geocoding service.

3.3 Attributes

A geocoder has the following attributes:

resultLimits defines the absolute maximum number of search results that can be returned in a single request. A given request can specify a lower limit.

someDuplicatesMaximum defines the largest number of duplicate matches that can be considered a matchFault of **someDuplicates** instead of **manyDuplicates**.

privacyStatement defines the privacy policy governing the information accessible to the geocoder. For an example, see <http://www.gov.bc.ca/com/privacy.html>

disclaimer defines the warranty disclaimer. For an example, see <http://www.gov.bc.ca/com/disclaimer.html>

copyrightNotice is the text of the notice. For example:

Copyright (c) 2010, Province of British Columbia

copyrightLicense defines the license under which the geocoder service is copyrighted. For an example, see <http://www.gov.bc.ca/com/copyright.html>

privacyStatement, *disclaimer*, *copyrightNotice*, and *copyrightLicense* are included with all geocoder search results.

A SearchResults is a data type with the following attributes:

queryAddress is the SiteAddress as provided to the geocoder

matches is the set of all AddressMatches

bestMatch is the best-matching address in *matches*

srsCode is the code of the spatial reference system of the points in *matches*

searchTimeStamp is the completion time of the operation that created the search results.

privacyStatement (see above)

disclaimer (see above)

copyrightNotice (see above)

copyrightLicense (see above)

An **AddressMatch** is a data type with the following attributes:

address is a matching civic or non-civic **SiteAddress**. If the match precision level is **site**, **civicNumber**, or **unit**, *siteID* is set appropriately; otherwise it is set to the empty string. In the case of a score of zero (no match), *address.accessPointLocation* and *address.mainLocation* are set to *province.asPoint*.

score represents the quality of the match; 0 means no match, 100 means a perfect match (see section 3.2.3 for details).

faults represents the problems that were encountered in matching an input address to a known address. See section 3.2.3 for some examples.

precision is the level of precision of the match (see section 3.2.3 for details)

precisionPoints is the number of points assigned to the *precision*.

An **IntersectionSearchResults** is a data type with the following attributes:

queryStreet1 and *queryStreet2* are the two streets input to the **geocodeStreetIntersection** operation.

queryLocality is the locality name input to the **geocodeStreetIntersection** operation.

intersections is the set of **IntersectionMatches** found.

bestIntersection is the **IntersectionMatch** with the highest score.

srsCode is the code of the Spatial Referencing System that the results are returned in.

searchTimeStamp is the completion time of the operation that created the search results.

privacyStatement (see above)

disclaimer (see above)

copyrightNotice (see above)

copyrightLicense (see above)

An **IntersectionMatch** is a data type with the following attributes:

address is the **StreetIntersectionAddress** of the matching **StreetIntersection**.

score represents the quality of the match; 0 means no match, 100 means a perfect match.

faults represents the problems that were encountered in matching an input address to a known address. See section 3.2.3 for some examples.

precision is the level of precision of the match.

precisionPoints is the number of points assigned to the *precision*.

3.4 Operations

3.4.1 Geocode Structured Address

```
context:Geocoder::geocodeStructuredAddress(queryAddress:SiteAddress, minScore:Integer,
maxResults:Integer, resultSrsCode:Integer, setback:Real): SearchResults
```

Returns all sites whose site addresses match a queryAddress.

setback (in metres) must be zero or greater

```
pre: setback >=0
```

minScore defines the minimum score that a match must achieve for inclusion in search results.

```
pre: 0 <= minScore and minScore <= 100
```

maxResults defines the maximum number of search results returned. It cannot be larger than resultsLimit.

```
pre: 0 < maxResults and maxResults <= resultsLimit
```

resultSrsCode defines the code of the spatial reference system that accessPoints and mainLocations are to be returned in. resultSrsCode must be a supported spatial reference system

```
pre: spatialReferenceSystem->exists(s| s.code=resultSrsCode)
```

For best matching, any of the following sets of SiteAddress elements should be provided:

unitNumber, unitNumberSuffix, civicNumber, civicNumberSuffix, streetName, streetType, streetDirection, locality

civicNumber, civicNumberSuffix, streetName, streetType, streetDirection, locality

siteName, locality (if non-civic address)

Matching is possible with the following element combinations but the match quality is lower:

street, locality
street
locality

unitDesignator and province are optional

streetType, streetDirection, and locality are optional but if missing, may result in a lower match score.

post:

Given a civic address (e.g., 1204 Esquimalt Rd, Esquimalt, BC) and a matched address, the following table shows how access point and related properties are determined at each match precision level:

match Precision	siteID	accessPointLocation	accessPoint positional Accuracy	mainLocation	mainLocation positional accuracy
province	None	Province.asPoint	Low	Province.asPoint	low
locality	None	Locality.asPoint	Low	Locality.asPoint	low
street	None	street.asPoint	Low	Street.asPoint	low
block	None	matchedBlock.interpolateAlongCentre Line(civicNumber)	Medium	matchedBlock.interpolateMain Location(civicNumber, aSetBack)	medium
civicNumber	matchedSite .siteID	matchedAccessPoint.location	High	matchedSite.mainLocation()	matchedSite.main LocationPositional Accuracy()
unitNumber	matchedSite .unitNumber	matchedSite.unitNumber	High	matchedSite.mainLocation()	matchedSite.main LocationPositional Accuracy()

Given a non-civic address (e.g., Remote Logging Camp, Faraway Lake, BC) and a matched address, the following table shows how access point and related properties are determined at each match precision level:

match Precision	siteID	accessPointLocation	accessPoint Positional Accuracy	mainLocation	mainLocation positional accuracy
province	none	matchedProvince.asPoint	Low	Province.asPoint	low
locality	none	matchedLocality.asPoint	Low	Locality.asPoint	low
site	matchedSite.siteID	matchedAccessPoint.location	matchedAccessPoint. positionalAccuracy	matchedSite.mainLocation()	matchedSite.mainLocation PositionalAccuracy()
unitNumber	matchedSite.siteID	matchedAccessPoint.location	matchedAccessPoint. positionalAccuracy()	matchedSite.mainLocation()	matchedSite.mainLocation PositionalAccuracy()

If no match is found in a given locality, alias sites, streets, and localities are searched.

All string comparisons ignore case and are made using the smartMatch operation; smarter alternatives to smartMatch are allowed.

All expanded forms of queryAddress.siteName, queryAddress.streetName, and queryAddress.locality are smartMatched. Expansion is performed by the expandName operation (see section 3.4.11)

Score values are set as per section 3.2.3.

Valid result

```
post: not result->isEmpty()
post: result.matches->forall(m | m.address.siteID.notEmpty() implies Site->exists( s |
m.address.siteID= s.siteID and (m.address= s.civicAddress(resultSrsCode) or
m.address=nonCivicAddress(resultSrsCode) ) ) )
post: result.matches->forall(m | m.score <= bestMatch.score)
post: result.matches->forall(m | 0<=m.score and m.score <= 100)
post: result.matches->exists(m| m = bestMatch)
```

3.4.2 Geocode Unstructured Address

```
Context: Geocoder::geocodeUnstructuredAddress(queryAddress:String, minScore:Integer,
maxResults:Integer, resultSrsCode:Integer, setback: Real): SearchResults
```

Returns all addresses that match or partially match an unstructured (free form) address string.

minScore defines the minimum score that a match must achieve for inclusion in search results.

```
pre: 0 <= minScore and minScore <= 100
```

maxResults defines the maximum number of search results returned. It cannot be larger than resultsLimit.

```
pre: 0 < maxResults and maxResults <= resultsLimit
```

resultSrsCode defines the code of the spatial reference system that accessPoints and mainLocations are to be returned in. resultSrsCode must be a supported spatial reference system

```
pre: spatialReferenceSystem->exists(s| s.code=resultSrsCode)
```

setback (in metres) must be zero or greater

```
pre: setback >=0
```

pre: queryAddress is an address as a single string and can take one the following formats (square brackets means zero or one occurrences; an asterisk following square brackets means zero or more):

Format 1. [[unitDesignator unitNumber[unitNumberSuffix]] [siteName],]*
civicNumber[civicNumberSuffix] streetName streetType [streetDirection]
[,localityName] [,provinceCode]

Format 2. unitNumber[unitNumberSuffix]-
civicNumber[civicNumberSuffix] streetName streetType [streetDirection]
[,localityName] [,provinceCode]

Format 3. civicNumber[civicNumberSuffix] streetName streetType [streetDirection]
[[unitDesignator unitNumber[unitNumberSuffix]]
[,localityName] [,provinceCode]

Format 4. [[unitDesignator unitNumber[unitNumberSuffix]] [siteName],]*
[,localityName] [,provinceCode]

Format 5. streetName streetType [streetDirection], [,localityName] [,provinceCode]

Format 6. localityName [,provinceCode]

Here are some examples:

1. A civic address with no unit number:

1025 HAPPY VALLEY RD, METCHOSIN, BC
420 GORGE RD E, VICTORIA, BC

2. A civic address with a unit number:

PAD 2, 1200 NORTH PARK RD, SHAWNIGAN LAKE, BC
1200 NORTH PARK RD PAD 2, SHAWNIGAN LAKE, BC
2-1200 NORTH PARK RD, SHAWNIGAN LAKE, BC

3. A civic address with a simple site name:

PORT ALICE HEALTH CENTRE, 1090 MARINE DRIVE, PORT ALICE, BC
ROYAL ATHLETIC PARK, 1014 CALEDONIA AVE, VICTORIA, BC

4. A civic address with a unit within a named complex:

PAD 2, HAPPY MOBILE HOME PARK, 1200 NORTH PARK RD, SHAWNIGAN LAKE, BC
ROOM 103A, CLEARIHUE BUILDING, UNIVERSITY OF VICTORIA, 3800 FINNERTY RD,
VICTORIA, BC
ROOM 230, WEST BLOCK, ROYAL JUBILEE HOSPITAL, 1952 BAY ST, VICTORIA, BC

5. A civic address with a unit within a named complex and the unit has both a number and a name:

CABIN C HERON, HAPPY FISHING RESORT, WHOPPER, BC

6. A civic address with a unit within a unit of a named complex:

PAD 11, TERMINAL 3, BC SPACEPORT, 1 MILKY WAY, STAR CITY, BC

7.A street within a locality:

WILLOW DRIVE, 70 MILE HOUSE, BC
HORSE LAKE ROAD, 100 MILE HOUSE, BC

8.A locality within the province:

PEACE RIVER REGIONAL DISTRICT, BC
100 MILE HOUSE, BC
V8T, BC

post: see section 3.4.1 Geocode Structured Address

3.4.3 Geocode Street Intersection

```
context Geocoder::geocodeStreetIntersection(street1:String, street2:String,
                                           locality:String, minScore:Integer resultSrsCode:Integer,
                                           maxResults:Integer): IntersectionSearchResults
```

Returns the geographic location of all intersections of the two given streets within the given locality

street1 and street2 may take one of the following forms:

```
streetName
streetName streetType [streetDirection]
```

minScore defines the minimum score that a match must achieve for inclusion in search results.

pre: 0 <= minScore and minScore <= 100

maxResults defines the maximum number of search results returned. It cannot be larger than resultsLimit.

pre: 0 < maxResults and maxResults <= resultsLimit

resultSrsCode defines the code of the spatial reference system that intersection locations are to be returned in. resultSrsCode must be the code of a supported spatial reference system

pre: spatialReferenceSystem->exists(s| s.code=resultSrsCode)

post:

An IntersectionMatch is created for each StreetIntersection that has associated streets named *street1* and *street2* within the locality named *locality*.

Multiple IntersectionSearchResults may be returned in the following cases:

- Two streets named street1 and street2 are found and their road centrelines cross at several intersections.
- For a given locality, no streetType was specified for a streetName that has more than one (e.g., Happy St, Happy Rd),
- No streetDirection was specified for a streetName/Type that has more than one (e.g. Gorge Rd E, Gorge Rd W),
- The locality was unspecified.

If streetType, streetDirection, or locality are not specified in street1 or street2, matches may still be possible but will have a lower score.

If no match is found in a given locality, street and locality aliases are searched.

All expanded forms of the name part of street1 and street2 are smartMatched. Expansion is performed by the expandName operation (see section 3.4.12).

All string comparisons are made using the smartMatch operation.

Score values are set as per section 3.2.3

Valid result

```
post: not result->isEmpty()
post: result.intersections->forall(m | m.score <= bestIntersection.score)
post: result.intersections->forall(m | 0 <= m.score and m.score <= 100)
post: result.intersections->exists(m | m = bestIntersection)
post: result.matches->forall(m | m.address.srsCode = resultSrsCode)
```

3.4.4 Reverse Geocode Sites Inside An Area Of Interest

```
context Geocoder::sitesInside(aoi: Polygon, resultSrsCode: Integer,
                             maxResults: Integer): SearchResult
```

Returns all sites and their addresses within a given area of interest. Only the primary address of each site is returned.

```
--- A valid area of interest can't be null and must be a valid polygon
pre: not aoi.isNull()
pre: not aoi.isNull() implies aoi.isValid
```

maxResults defines the maximum number of search results returned. It cannot be larger than resultsLimit.

```
pre: 0 < maxResults and maxResults <= resultsLimit
```

resultSrsCode defines the code of the spatial reference system that **accessPoints** and **mainLocations** are to be returned in. **resultSrsCode** must be a supported spatial reference system

```
pre: spatialReferenceSystem->exists(s| s.code=resultSrsCode)
```

```
--- aoi is assumed to be defined in the spatial reference system
```

```
--- defined by resultSrsCode
```

Valid result

```
post: not result->isEmpty()implies
      result.matches->forall(m | m.address.siteID.notEmpty())
```

```
post: result.matches->forall(m | Site->exists( s | m.address.siteID = s.siteID and
      (m.address= s.civicAddress(resultSrsCode) or
       m.address=nonCivicAddress(resultSrsCode))))
```

```
post: result.matches->forall(m |
      m.address.accessPointLocation.inside(aoi)
```

```
post: not result->isEmpty()implies
      result.matches->forall(m | m.score=100)
```

```
post: not result->isEmpty()implies result.matches->exists(m| m = bestMatch)
```

3.4.5 Reverse Geocode Street Intersections Inside An Area Of Interest

```
context Geocoder::streetIntersectionsInside(aoi: Polygon, resultSrsCode:Integer,
      maxResults:Integer): IntersectionSearchResults
```

Returns all street intersections that intersect a given area of interest.

maxResults defines the maximum number of search results returned. It cannot be larger than **resultsLimit**.

```
pre: 0 < maxResults and maxResults <= resultsLimit
```

resultSrsCode defines the code of the spatial reference system that intersection locations are to be returned in. **resultSrsCode** must be the code of a supported spatial reference system

```
pre: spatialReferenceSystem->exists(s| s.code=resultSrsCode)
```

```
--- A valid area of interest can't be null and must be a valid polygon
```

```
pre: not aoi.isNull()
```

```
pre: not aoi.isNull() implies aoi.isValid
```

```
--- aoi is assumed to be defined in the spatial reference system defined by
resultSrsCode
```

Valid result

```

post: not result->isEmpty() implies
      result.intersections->forall(m | m.score = 100 and m.precisionLevel=block)

post: not result->isEmpty() implies result.intersections->exists(m| m = bestIntersection)

post: result.matches->forall(m | m.address.srs = resultSrsCode)

```

3.4.6 Reverse Geocode Street Intersections Near a Given Point

```

context Geocoder::streetIntersectionsNear(centre:Point, distance:Real,
      resultSrsCode:Integer, maxResults:Integer): IntersectionSearchResults
--- returns all street intersections within a given distance of a given point

```

maxResults defines the maximum number of search results returned. It cannot be larger than **resultsLimit**.

```
pre: 0 < maxResults and maxResults <= resultsLimit
```

resultSrsCode defines the code of the spatial reference system that intersection locations are to be returned in. **resultSrsCode** must be the code of a supported spatial reference system

```
pre: spatialReferenceSystem->exists(s| s.code=resultSrsCode)
```

A valid centre must not be null and must be a valid point.

```
pre: not centre.isNull()
pre: not centre.isNull() implies centre.isValid()

```

Valid distance

```
pre: distance > 0
```

```

--- centre is assumed to be defined in the spatial reference system
--- defined by resultSrsCode

```

Valid result

```

post: result = streetIntersectionsInside(circleInSquare(centre, distance))

post: result.matches->forall(m | m.address.srs = resultSrsCode)

```

3.4.7 Reverse Geocode Sites Near a Given Point

```
context Geocoder::sitesNear(centre: Point, distance:Real, resultSrsCode:Integer,
```

```
maxResults:Integer): SearchResults
```

Returns all sites and their addresses within a given distance of a given point. Only one address per site is returned (e.g., primary civic address or non-civic address).

`maxResults` defines the maximum number of search results returned. It cannot be larger than `resultsLimit`.

```
pre: 0 < maxResults and maxResults <= resultsLimit
```

`resultSrsCode` defines the code of the spatial reference system that `accessPoints` and `mainLocations` are to be returned in. `resultSrsCode` must be the code of a supported spatial reference system

```
pre: spatialReferenceSystem->includes(resultSrsCode)
```

A valid centre must not be null and must be a valid point.

```
pre: not centre.isNull()
```

```
pre: not centre.isNull() implies centre.isValid()
```

```
--- centre is assumed to be defined in the spatial reference system
--- defined by resultSrsCode
```

Valid distance

```
pre: distance > 0
```

Valid result

```
post: not result->isEmpty() implies
      result.matches->forall(m | m.address.siteID.notEmpty())
```

```
post: result.matches->forall(m | Site->exists( s | m.address.siteID = s.siteID and
      (m.address= s.civicAddress(resultSrsCode) or
       m.address=nonCivicAddress(resultSrsCode))))
```

```
post: result.matches->forall(m |
      m.address.accessPointLocation.inside(circleInSquare(centre, distance))
```

3.4.8 Reverse Geocode Site Identifier

```
Context: Geocoder::site(aSiteID:String, effectiveDate:Date, resultSrsCode:Integer):
SearchResults
```

Returns all addresses associated with a given site identifier as of a given date.

The address as of the date, `effectiveDate` is returned

resultSrsCode defines the code of the spatial reference system that **accessPoints** and **mainLocations** are to be returned in.

```
--- resultSrsCode must be the code of a supported spatial reference system
pre: spatialReferenceSystem->exists(s | s.code = resultSrsCode)

--- Effective date must be the today or in the past
pre: effectiveDate <= today()

--- A site with id, siteID must exist
pre: Site->exists(s | s.siteID = aSiteID)

post: see section 3.4.1 Geocode Structured Address
```

3.4.9 Reverse Geocode Street Intersection Identifier

Context: `Geocoder::streetIntersection(sid:String, resultSrsCode:Integer): IntersectionSearchResults`

Returns address associated with a given street intersection identifier, **sid**

resultSrsCode defines the code of the spatial reference system that the intersection location is to be returned in.

```
--- resultSrsCode must be the code of a supported spatial reference system
pre: spatialReferenceSystem->exists(s | s.code = resultSrsCode)

--- A street intersection with id, sid must exist
pre: StreetIntersection->exists(i | i.intersectionID = sid)

post: see section 3.4.3 Geocode Street Intersection
```

3.4.10 Reverse Geocode Sites Within A Given Time Period and Area

Context: `Geocoder::changedSitesInside(aoi:Polygon, startDate:Date, endDate:Date, maxResults:Integer, resultsSrsCode:Integer): SearchResults`

Returns all sites and their addresses inside a given area of interest that have changed within a given time period. Only one address per site is returned (e.g., primary civic address or non-civic address).

```
--- A valid area of interest (aoi) can't be null and must be a valid polygon
```

```

pre:  not aoi.isNull()
pre:  not aoi.isNull() implies aoi.isValid
---   aoi must be defined in the spatial reference system defined by resultSrsCode

---   Valid time period
pre:  startDate <= today()
pre:  endDate <= today()
pre:  startDate <= endDate

---   maxResults defines the maximum number of search results returned.
---   It cannot be larger than resultsLimit.
pre:  0 < maxResults and maxResults <= resultsLimit

---   resultSrsCode defines the code of the spatial reference system that
---   accessPoints and mainLocations are to be returned in.
---   resultSrsCode must be a supported spatial reference system
pre:  spatialReferenceSystem->includes(resultSrsCode)

---   Valid result
post:  not result->isEmpty() implies
       result.matches->forall(m | m.address.siteID.notEmpty())

post:  result.matches->forall(m | Site->exists( s | m.address.siteID = s.siteID and
                                              (m.address= s.civicAddress(resultSrsCode) or
                                              m.address=nonCivicAddress(resultSrsCode))))

post:  result.matches->forall(m | m.accessPointLocation.inside(aoi))

post:  not result->isEmpty() implies
       result.matches->forall(m | m.score=100)

post:  not result->isEmpty() implies result.matches->exists(m| m = bestMatch)

post:  result.matches->forall(m | m.address.srsCode = resultSrsCode)

post:  result.notEmpty() implies
       result.forAll(x | startDate <= x.changeDate and x.changeDate <= endDate)

```

3.4.11 Smart String Matcher

```
context Geocoder::smartMatch(string1:String, string2:String): Boolean
```

`smartMatch` returns true if `string1` approximately matches `string2`. This definition represents the minimum a smart matcher must do to be compliant. Two strings are separated by an edit distance of 1 if they can be made identical by the insertion, deletion, or modification of a single character. Two strings are separated by a swap distance of 1 if they can be made identical by a single swap of two adjacent characters.

smartMatch ignores case

```
post: result = if editDistance(string1, string2) <= 1
                and swapDistance(string1, string2) <= 1 then
                    true
                else
                    false
                endif
```

3.4.12 Site, Street, and Locality Name Expander

```
context Geocoder::expandName(aName:String): set(String)
```

expandName returns all possible expansions of the name of a given site, street, or locality name. Expansion involves replacing abbreviated words with full words.

expandName uses specialAbbreviations which contains abbreviations commonly found in site, street, and locality names. Examples include N (North), Mt (Mount), Mtn (Mountain), CFB (Canadian Forces Base), St. (Saint), and Psg (Passage).

Case is ignored in all string comparisons

Results contain no special abbreviations

```
post: result->forAll(x | SpecialAbbreviations->forAll(y | not x.contains(y.abbreviation) )
)
```

3.4.13 Circle in Square Generator

```
context Geocoder::circleInSquare(centre:Point, radius:real):Polygon
--- returns a square polygon that encloses a circle with a given radius(in metres)
--- and centre point (in lat/lon projection)
--- and that conforms to the Open Geospatial Consortium Simple Feature Specification

pre: not centre.isNull()
pre: not centre.isNull() implies centre.isValid
pre: radius>0

post: result.isValid()
```

3.4.14 Geometry Reprojection

```
context Geocoder::reproject(shape: Geometry, sourceSRS:Integer,
                             resultSrsCode:Integer):Geometry
```

```
---    returns the shape reprojected into the requested spatial referencing system

---    inputSRS and outputSRS is supported
pre:    spatialReferenceSystem.code ->exists(s | s.code=sourceSRS)
        spatialReferenceSystem.code ->exists(s | s.code=resultSrsCode)

pre:    shape.notEmpty()
pre:    shape.isValid()

post:   result.isValid()
```


3.5 Constraints

1. Precision level points must be between 0 and 100

```
context PrecisionLevelPoints inv withinLegalRange  
0<=points and points<=100
```

2. Match fault penalties must be between 0 and 100

```
context MatchFault inv withinLegalRange  
0<=penalty and penalty<=100
```

3. resultsLimit must be positive

```
context Geocoder inv positiveResultsLimit  
resultsLimit>0
```

4. someDuplicatesMaximum must be positive

```
context Geocoder inv multipleSomeDuplicatesMaximum  
someDuplicatesMaximum>1
```

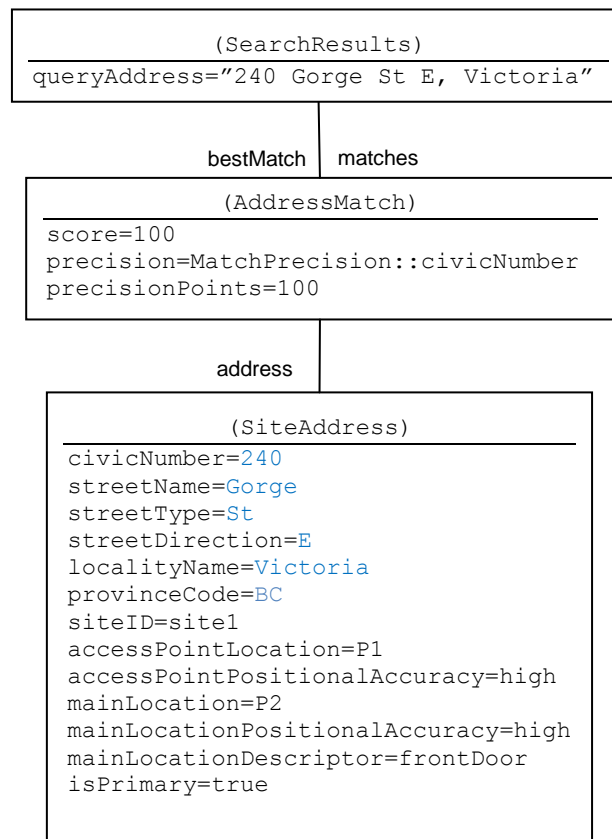
3.6 Geocoding Examples

These examples illustrate requests to geocode a site with a single address as defined in section 2.6.1 with the following additions:

- P1W is the precise access point position of 240 Gorge St W in Saanich
- P3 is the representative point (Street.asPoint) for Gorge St E in Victoria
- P4 is the interpolated position of 212 Gorge St E, Victoria
- Saanich is a LocalityAlias for Victoria (and vice-versa)

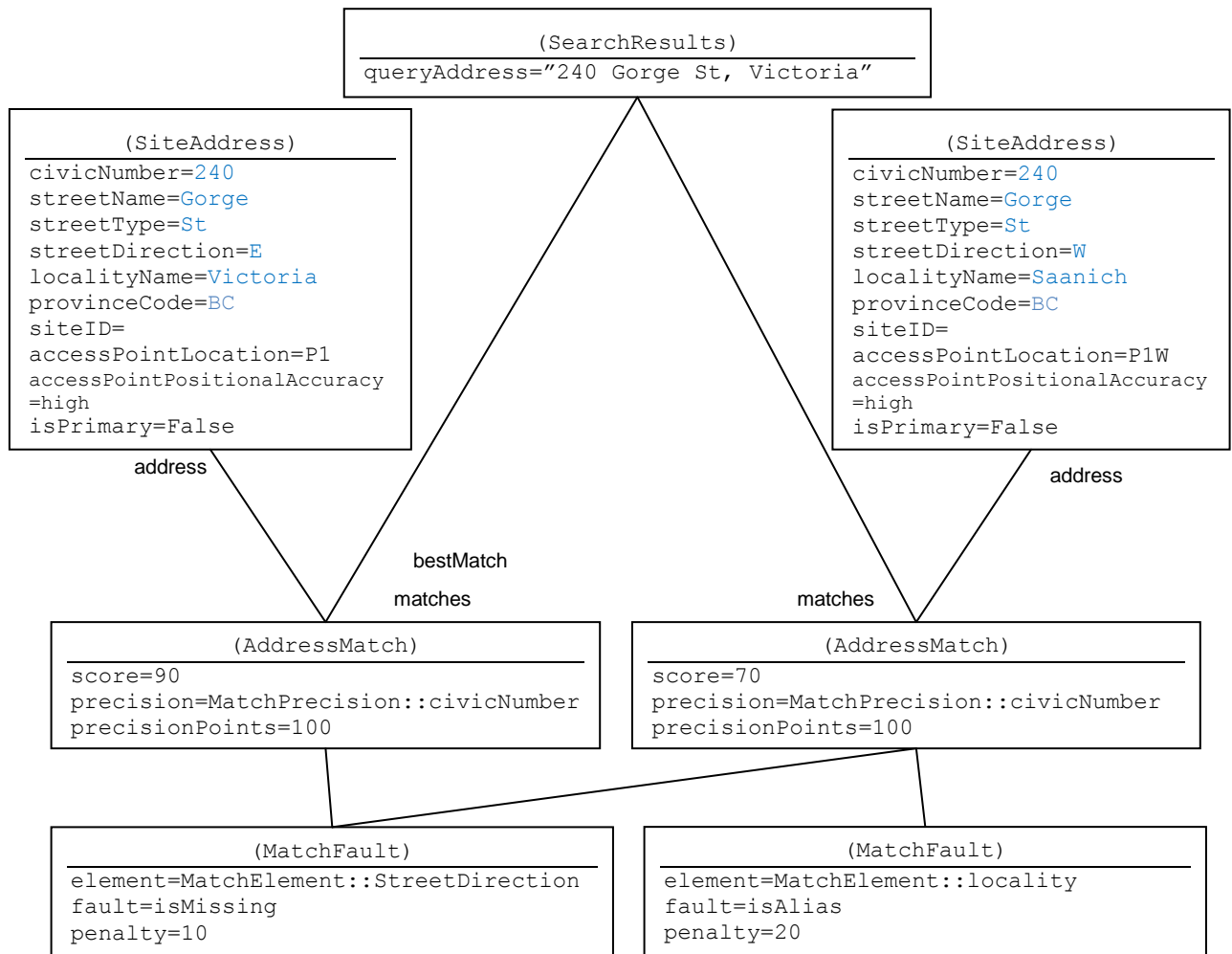
3.6.1 A Perfect Match

```
geocoder.geocodeUnstructureAddress(queryAddress="240 Gorge St E, Victoria",
minScore=0,maxResults=100,resultSrsCode=4326)
```



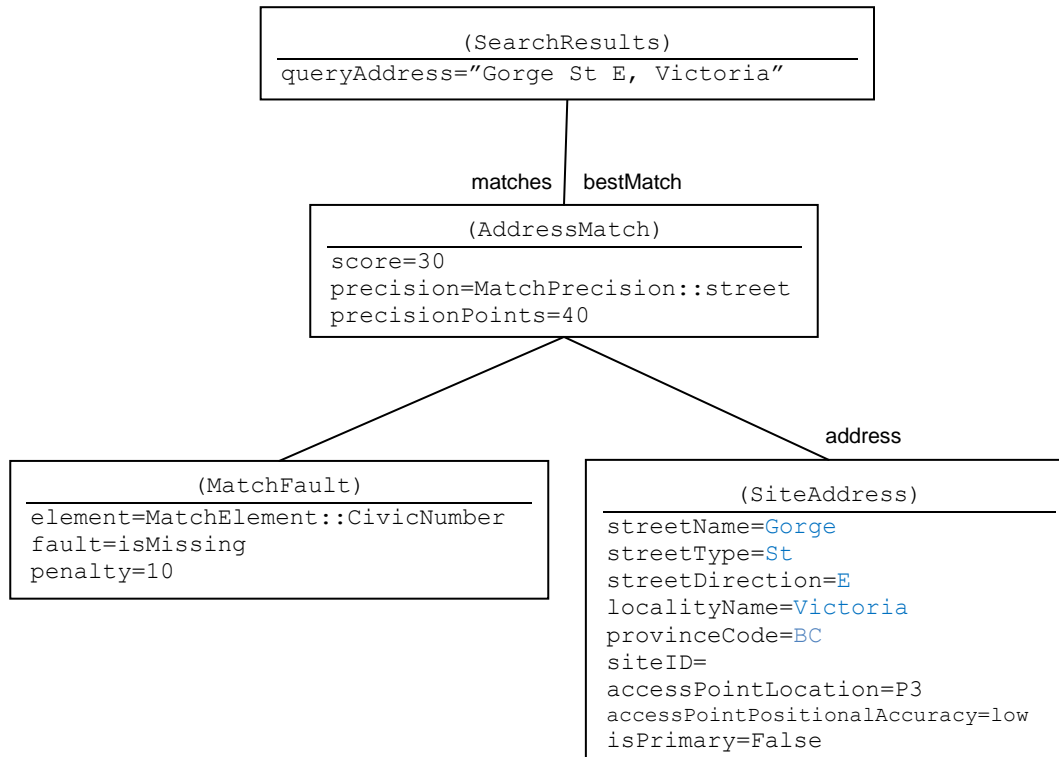
3.6.2 A Missing Street Direction

geocoder.geocodeUnstructureAddress(queryAddress="240 Gorge St, Victoria",
minScore=0,maxResults=100,resultSrsCode=4326)



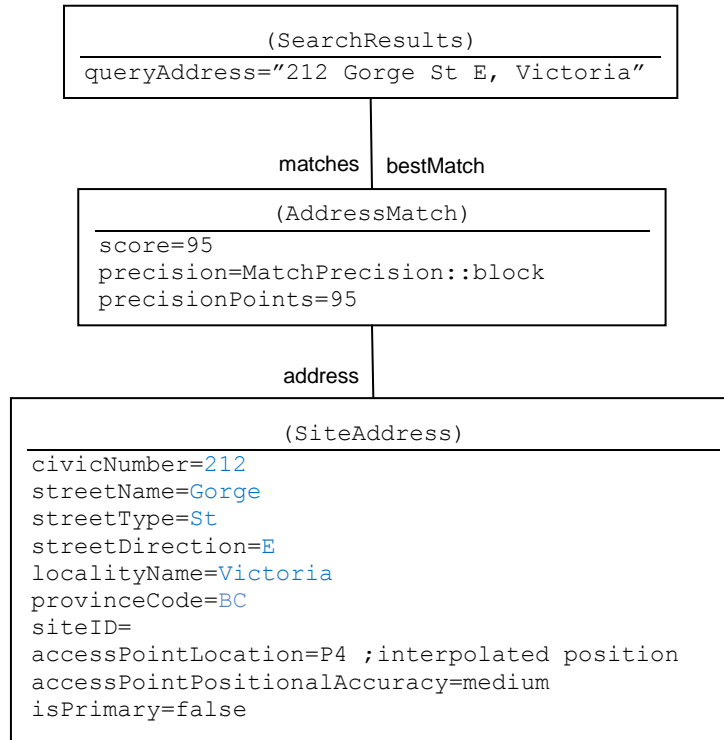
3.6.3 A Missing Civic Number

geocoder.geocodeUnstructureAddress(queryAddress="Gorge St E, Victoria",
minScore=0,maxResults=100,resultSrsCode=4326)



3.6.4 Interpolation Required

geocoder.geocodeUnstructureAddress(queryAddress="212 Gorge St E, Victoria",
minScore=0,maxResults=100,resultSrsCode=4326)



4. REFERENCES

R1 Canada Post Addressing Guidelines

<http://www.canadapost.ca/tools/pg/manual/PGaddress-e.asp>

R2 BC Geographical Names Information Service

<http://geobc.gov.bc.ca/bcnames/>

R3 Nova Scotia Civic Address Users Guide

http://www3.nsgc.gov.ns.ca/civic_help/V5/pdf/CivicAddressUsersGuidev.4.1.pdf

R4 Open Geospatial Consortium Simple Feature Access

<http://www.opengeospatial.org/standards/sfa>

R5 Unified Modelling Language 2.0

http://en.wikipedia.org/wiki/Unified_Modeling_Language

R6 Object Constraint Language 2.0

http://en.wikipedia.org/wiki/Object_Constraint_Language

R7: BC Mailing and Delivery Address Standards

http://www.cio.gov.bc.ca/other/DAF/docs/MailingDeliveryAddress_Standards.doc

R8: Towards An International Address Standard

http://www.isotc211.org/address/Copenhagen_Address_Workshop/papers/CoetzeeEtAl_TowardsAnInternationalAddressStandard_GSDI-10_2008.pdf

R9 United States Postal Service Postal Addressing Standards

<http://pe.usps.gov/cpim/ftp/pubs/Pub28/Pub28.pdf>

R10: Spatial Referencing for Geographical Datasets (BS7666-2006)

http://www.agi.org.uk/SITE/UPLOAD/DOCUMENT/Standards/BS7666_1.pdf

R11: *Trouble with twins* , James Rumbaugh, pp16-21, Journal of Object Oriented Programming; July/August 1994

R12: ESRI Address Data Model

<http://support.esri.com/index.cfm?fa=downloads.dataModels.filteredGateway&dmid=32>

R13: URISA Street Address Data Standard

<http://www.urisa.org/about/initiatives/addressstandard>

R14: AddressBC Technical Specifications v2.0 (June 12, 2008)

R15: OpenGIS Location Service (OpenLS) Implementation Standards

<http://www.opengeospatial.org/standards/ols>

R16: BC Civic Address Geocoder User Guide

http://www.data.gov.bc.ca/local/dbc/docs/geo/geocode/geocoder_user_guide_1.1.pdf

R17: Spatial Referencing System Codes

<http://spatialreference.org/>

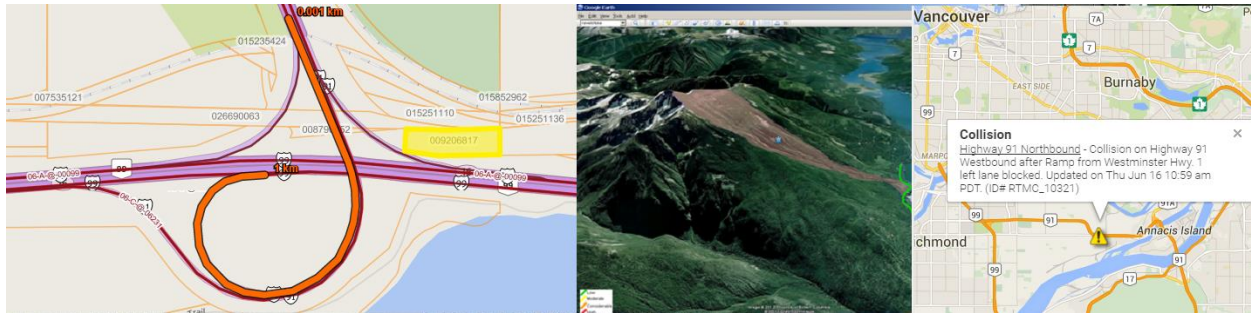
R18: BC Date and Time Standard

R19: ISO 3166-2 Sub-Country Codes

http://en.wikipedia.org/wiki/ISO_3166-2:CA

R20: ISO 19112 Geographic information – Spatial referencing by geographic identifiers

http://people.ischool.berkeley.edu/~ryanshaw/pdf/ISO_19112.pdf



Spatial Data Standards

for

Ministry of Transportation and Infrastructure

Information Management Branch

Prepared By:	Peter Spry, Spatial Data Analyst
Prepared For:	Architecture Data and Digital Services/ Information Management Branch
Document Version:	0.6
Creation Date:	May 11, 2016
Last Updated Date:	Friday, December 3, 2021


Checklist

MoTI strives to keep its published standards and practices updated as new technologies and practices emerge. Ensure that you consult with IMB's Spatial Data Architecture group to verify your spatial designs before undertaking development.

To ensure a fast and efficient delivery of any spatial application release, this one page version of the guide has been created.

To be signed off by the Project Technical Leader and the IMB Spatial Data Architect.

For each spatial table

<i>Deliverable</i>	<i>Reference</i>	<i>verified</i>
Spatial table design completed and signed off by IMB Data Architect	<p>4.1 Supported Spatial Data Types</p> <p>The supported spatial data type at MoTI IMB is SDO_GEOMETRY. SDO_GEOMETRY supports all vector data types, point, line, polygon, multipoint, multiline, multipolygon and collections of all of the previous types. Spatial data must have a minimum of two dimensions, X and Y, but may also contain one or two additional dimensions. Typical use of third and fourth dimensions are for elevation, Z, and measure, M.</p> <p>IMB is investigating ways to manage and support raster and point cloud data. The results of that investigation will be made available in a new release of this guide.</p> <p>1.1.1 Use Spatial Data Type for Spatial Data!</p> <p>Spatial data, typically point locations, are often displayed as Latitude and Longitude for human readability. However, when stored in a database in this form they are not easily integrated with other spatial data. For that reason, <i>always</i> represent and store spatial data using a spatial data type.</p> <p>However, when application design require access to geographic coordinates for data entry, audit or presentation purposes use Oracle's SDO_TRANSFORM function as shown in section 4.3.3 SDO_POINT.</p>	

	Modelling Spatial Data	
Data custodian identified	4.2.1 Spatial Metadata	<input type="checkbox"/>
Spatial meta data documentation complete	4.2.1 Spatial Metadata	<input type="checkbox"/>
Spatial table generated in DEV environment	See Tables in Data Architecture Guidelines	<input type="checkbox"/>
Spatial table Metadata insert statement delivered and run	5.1 Oracle Spatial Metadata Entry	<input type="checkbox"/>
Initial spatial data loading script(s) delivered and run	5 Creating Spatial Data	<input type="checkbox"/>
Spatial index creation script delivered and run	4.5 Spatial Index	<input type="checkbox"/>
Spatial data validation script delivered and run	5.3 Validating Spatial Data	<input type="checkbox"/>

For each spatial table and view to become a layer in GeoServer OGC services

<i>Deliverable</i>	<i>Reference</i>	<i>verified</i>
GeoServer proxy user created with appropriate role(s) granted	4.6 Users	<input type="checkbox"/>
For layer viewed in WMS, Styled Layer Descriptor (SLD) delivered and deployed	Appendix B Sample SLD	<input type="checkbox"/>
CURL or Jmeter script(s) demonstrating acceptable response time(s)	Appendix C cURL script for WMS performance test	<input type="checkbox"/>
For layer with spatial editing sample scripts to insert, update, and delete	Appendix D cURL scripts for WFS-Transaction test	<input type="checkbox"/>

Version Control

The purpose of this section is to document the history of this particular document in order to track changes and approvals.

<i>Version</i>	<i>Date</i>	<i>Change Description</i>	<i>Author</i>
0.1	2016/05/11	Initial Draft	Peter Spry
0.2	2016/10/28	Incorporating comments and suggestions from team	Peter Spry
0.3	2016/11/08	Incorporating comments and suggestions from Richard Pardo-Figueroa, Gary Belleville, and Christian Baerike.	Peter Spry
0.4	2017/04/03	Incorporating additional comments and suggestions from Christian Baerike and Richard Pardo-Figueroa.	Peter Spry
0.5	2017/05/12	Adding Integrated Transportation Network (ITN) integration requirements.	Peter Spry
0.6	2019/05/21	Updated technical architecture diagrams	Peter Spry

Contents

Checklist	2
For each spatial table.....	2
For each spatial table and view to become a layer in GeoServer OGC services	2
Version Control.....	3
Table of Figures	5
1 Introduction.....	6
1.1 Purpose.....	6
1.2 Audience	6
1.3 Background.....	6
1.4 Related Documents	7
1.5 Document Location	7
1.6 Document Status	7
2 Spatial Database Environments	8
2.1 Onsite	8
2.1.1 Development	8
2.1.2 Test	8
2.1.3 Production	8
2.2 Offsite	8
2.3 Availability of Database Environments.....	9
2.4 Availability of GeoServer Web Services.....	9
3 Spatial Technical Architecture.....	10
3.1 Supported Software Versions.....	11
3.2 Supported Development tools for Building Spatial Applications	12
3.3 Location Integration	12
3.4 COTS Integration and Interoperability	12
3.5 CHRIS	13
3.6 Spatial Data Migration.....	13
3.7 Spatial Application Updates	13
3.8 Supported Features of GeoServer at MoTI.....	13
4 Spatial Database	15
4.1 Supported Spatial Data Types	15
4.1.1 Use Spatial Data Type for Spatial Data!.....	15

4.2	Modelling Spatial Data	15
4.2.1	Spatial Metadata	15
4.2.2	Collection of Spatial Data	16
4.3	SDO_GEOMETRY.....	17
4.3.1	SDO_GTYPE.....	17
4.3.2	SRID and Standard Projection.....	18
4.3.3	SDO_POINT.....	18
4.3.4	SDO_ELEM_INFO	19
4.3.5	SDO_ORDINATES	19
4.3.6	Table Configuration	19
4.3.7	Estimating spatial table size	20
4.4	Spatial Tables and Views	21
4.5	Spatial Index	21
4.6	Users.....	22
4.6.1	Naming Convention	22
4.7	GeoServer Security Model.....	22
4.7.1	WebADE Profiles and Roles	22
4.7.2	GeoServer Roles	22
5	Creating Spatial Data	22
5.1	Oracle Spatial Metadata Entry	23
5.2	Initial Data Loading.....	24
5.2.1	SQL Scripts	24
5.2.2	FME Workspaces	24
5.3	Validating Spatial Data	25
5.4	Updates to Spatial Data.....	25
6	Appendix A. Glossary of Terms	26
7	Appendix B Sample SLD	27
8	Appendix C cURL script for WMS performance test	30
8.1	Hudson's Hope Bridge (rural)	30
8.1.1	BBOX values for 13 zoom levels beginning with the provincial extent	30
8.1.2	Complete cURL requests	30
8.2	Port Mann Bridge (urban).....	31
8.2.1	BBOX values for 13 zoom levels beginning with the provincial extent	31

8.2.2	Complete cURL requests	32
9	Appendix D cURL scripts for WFS-Transaction test.....	34
9.1	Create a record	34
9.2	Update a Record	35
9.3	Delete a Record	37

Table of Figures

Figure 1: Three tiered architecture for spatial services..... **Error! Bookmark not defined.**

Figure 2: Designer work around for SDO_GEOMETRY datatype. **Error! Bookmark not defined.**

1 Introduction

Spatial data, the location of assets, events and routes is a critical component in the business of the Ministry of Transportation and Infrastructure (MoTI). The goal of the Information Management Branch (IMB) is to ensure that data is clearly defined, well designed, appropriately available and well performing. That goal is achieved when Business Owners, Data Custodians and Project Staff work towards that common purpose.

1.1 Purpose

This document defines the standards, procedures and guidelines comprising the IMB support service offering for development of spatial applications at the MoTI.

1.2 Audience

This guide will be of interest to IMB staff and consultants who take on the following project roles:

- Project Team Spatial Technical Leaders: when designing, creating or maintaining spatial application systems.
- Programmers: when creating or maintaining spatial application systems.
- Project Managers and Business Analysts when defining system requirements for spatial applications.

1.3 Background

Up until the turn of the century, digital location data at MoTI was based primarily on driven distances from known points known as Linear Reference Methods or LRM. In support of the ministry's business the transportation network was broken into segments based on the type of location need. The three most important LRMs used were: The Road Features Inventory (RFI) method--more than 21,000 segments; The Landmark Kilometer Inventory (LKI)--nearly 400 segments; and the Numbered Highways, known internally as the Data Sharing Application (DSA) method--87 segments.

In 2001 the ministry acquired "Highways by exor" which enabled locations to be translated between LRMs. The Corporate Highway Resource Inventory System (CHRIS), as it is known now, included an internet accessible map. At the same time, an innovation to the long running Photolog program was introducing the ministry to Web Mapping. These two systems relied on two technologies developed by Environmental Systems Research Institute (ESRI): Spatial Data Engine (ArcSDE) and Internet Mapping System (ArcIMS).

By 2004 CHRIS, Photolog and the Snow Avalanche and Weather System (SAWS) mapping application were making use of the new Internet Mapping Framework (IMF) from the Ministry of Sustainable Resource Management (now DataBC). The IMF allowed applications whose spatial data was exposed via ArcIMS to be built relatively quickly and by 2009 the ministry was running more than a dozen web mapping applications for such diverse business needs as Bridge Information, Collision Information, Development Approvals, Highway Planning and Engineering Documents, Property Acquisition and Traffic Volumes and Surveys. The technology stack of that time was comprised of an Oracle Database, ArcSDE, ArcIMS, the IMF and the client browser.

During the next few years the IMB undertook the migration of its spatial data from ESRI's SDEBINARY storage format to Oracle's native spatial format, SDO_GEOMETRY. This eliminated the need for the ArcSDE layer of software to manage spatial data and simplified the management of spatial data considerably.

In 2012, driven by ESRI discontinuing support for ArcIMS, the retirement of the IMF was announced. The ministry needed to replace ArcIMS in its technology stack and re-write portions of all its spatial applications. The chosen replacement for ArcIMS was the GeoServer open source project. The replacement for the IMF was the OpenLayers open source JavaScript library.

1.4 Related Documents

For background information on IMB development standards and guidelines refer to the following documents available on the IMB SharePoint .

- **MoTI Spatial Application Developer's Guide** ([https://projects.sp.th.gov.bc.ca/StrategicServices/Information Management/Spatial Architecture/MoTI_Spatial_Application_Development_Guide.docx?Web=1](https://projects.sp.th.gov.bc.ca/StrategicServices/Information%20Management/Spatial%20Architecture/MoTI_Spatial_Application_Development_Guide.docx?Web=1))
- **MoT Data Architecture Standards** (https://projects.sp.th.gov.bc.ca/StrategicServices/_layouts/15/start.aspx#/Data%20Architecture/Forms/AllItems.aspx?RootFolder=%2FStrategicServices%2FData%20Architecture%2FStandards)
- **Oracle Application Server 10g J2EE Applications Services Guide** (<https://isb-doc.th.gov.bc.ca/Shared%20Documents/MoT%20Oracle%20Application%20Server%2010g%20J2EE%20Services%20Guide%20-%20Draft%20v%202%201%2011%20published.doc?Web=1>)
- **IMB Technology Matrix** ([https://projects.sp.th.gov.bc.ca/StrategicServices/Information Management/Standards and Guidelines/MoTI Infrastructure Technology Matrix.docx?Web=1](https://projects.sp.th.gov.bc.ca/StrategicServices/Information%20Management/Standards%20and%20Guidelines/MoTI%20Infrastructure%20Technology%20Matrix.docx?Web=1))

Further information can be found in the following guide.

- **GeoServer User Manual** (<http://docs.geoserver.org/maintain/en/user/>)
- **Oracle Spatial Developer's Guide** (https://docs.oracle.com/cd/E11882_01/appdev.112/e11830/toc.htm)

1.5 Document Location

The Spatial Data Services Guide is currently available on the MoTI IMB Hub SharePoint site.

(https://projects.sp.th.gov.bc.ca/StrategicServices/Information%20Management/Spatial%20Architecture/MoTI_Spatial_Data_Services_Guide.docx?Web=1)

1.6 Document Status

The Spatial Data Services Guide was created by Peter Spry. This document is currently maintained and distributed by the Architecture Data & Digital Services section of the IMB at MoTI.

2 Spatial Database Environments

The term *Environment* refers to the set of data, programs and procedures in a particular phase of the application development life cycle, for example *Development*.

2.1 Onsite

2.1.1 Development

The Development environment is to be used by Programmers and Project Team Spatial Technical Leaders for the development, unit testing and integration testing of application components. This environment is not normally available to end-users.

2.1.2 Test

The Test environment is to be used for acceptance testing by Programmers, Project Team Spatial Technical Leaders and end-users alike. This environment is separate from development in order to ensure that users can perform testing in a stable environment. One of the main purposes of acceptance testing is to ensure that major problems will be detected before systems are implemented in the production environment.

The only way components are created or updated in the Test environment is through a formal release from the Development environment or through the installation of packaged software provided by a vendor. For instance, developers therefore cannot make ad-hoc changes to this environment that impact end-users in the process of acceptance testing.

The Test environment should mirror the Production environment as closely as possible, including software versions, system capacity and availability, and database sizes to ensure relevant test results.

2.1.3 Production

The Production environments are the "live" environments where the Ministry's business functions are performed. The Production environments differ from the other environments in the following ways:

- Targets are established for system availability and performance.
- Integrity of data is carefully managed. For example, full point-in-time recovery of data is guaranteed.
- Change to the Production environments is tightly controlled in order to meet targets for performance, availability and reliability.
- Components are created or updated in the Production environments only through a release from the Test environment.

2.2 Offsite

Consulting firms developing spatial applications for the Ministry may be required to create and manage their own "Offsite" development environment. These environments will be constructed using the consulting firm's own hardware and software.

The Offsite environment is to be used by consultants (Programmers and Project Team Spatial Technical Leaders) for the development, unit testing and integration testing of application components. Once integration testing is complete, the application should be delivered into the Ministry's Development environment.

The Offsite environment should mirror the ministry's Development environment as closely as possible to minimize issues during application delivery.

2.3 Availability of Database Environments

IMB operations staff is available to ensure MoTI Database environments are available to users and developers during regular BC Government working hours, that is, Monday to Friday 8:30am to 4:30pm.

Outside of those hours, weekends, statutory and government holidays, MoTI database environments should normally be available to users and developers, and any issues are dealt with on a best-effort basis. The ministry is working to implement procedures to ensure 24x7 availability on a per-application basis where required.

2.4 Availability of GeoServer Web Services

GeoServer is an Open Geospatial Consortium (OGC) compliant implementation of a number of open standards including Web Feature Service (WFS), and Web Map Service (WMS). MoTI hosts two separate spatial services. One requiring authenticated and authorized access to data, one serving data to public, anonymous requests. Both services are normally available at all times, but IMB operations support is available only during office hours.

3 Spatial Technical Architecture

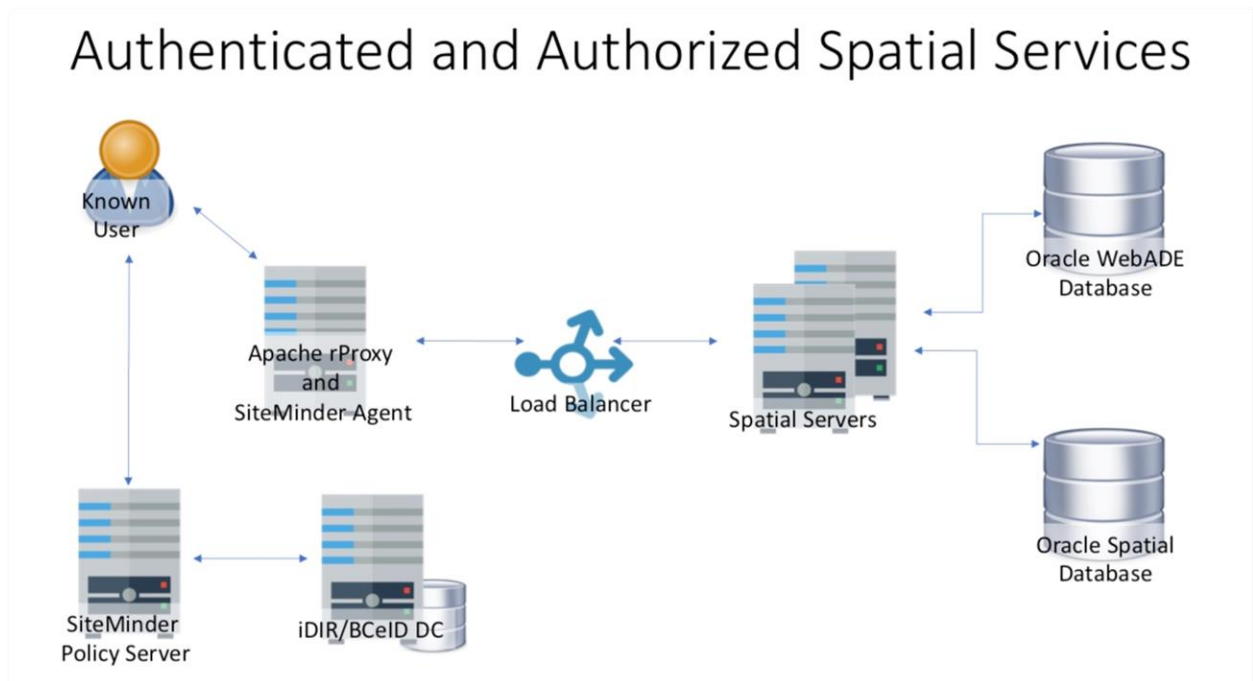
MoTI supports a three-tiered architecture for spatial applications: Database Server; GeoServer; and Client Browser/Application. The exceptions to this pattern are:

1. The Corporate Highway Resource Information System (CHRIS), the MoTI implementation of a commercial product, that updates spatial data via a desktop application; and
2. Applications which require bulk updates or do not yet have spatial editing capabilities. These updates are performed by database administrators via SQL or specialized tools such as FME.

For all other applications, reading and writing of spatial data should be managed by OGC services calls through MoTI GeoServer. *By adhering to published international standards application code will be resilient in the face of any future changes to Database or Spatial Server engines.*

3.1 Internal Spatial Technical Architecture

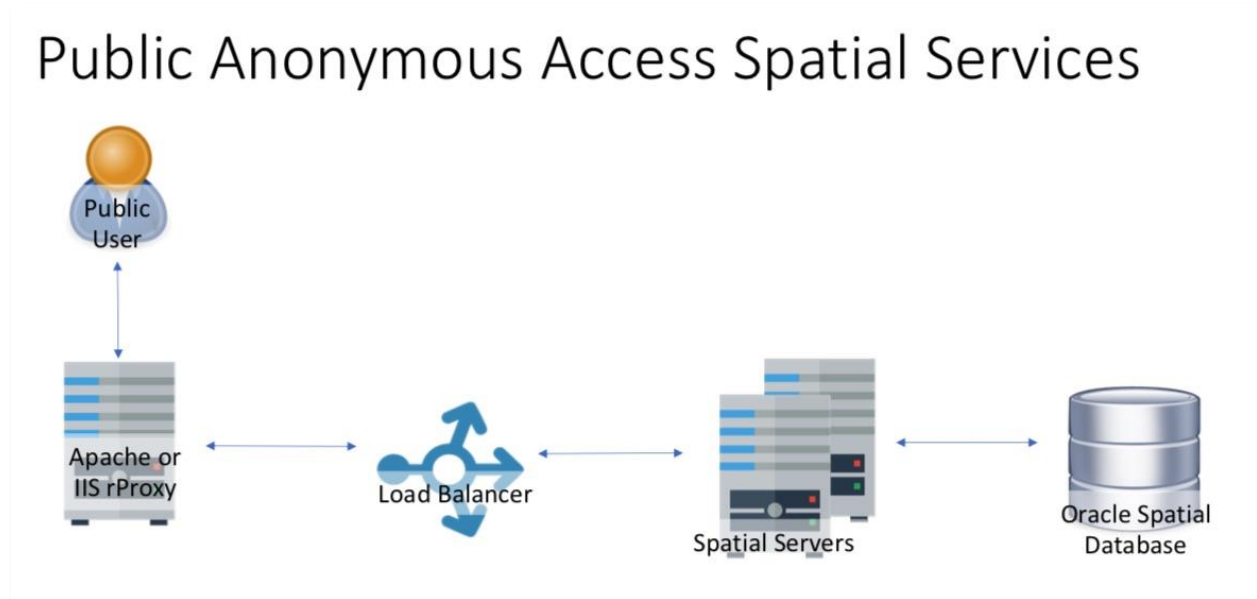
MoTI's internal spatial technical architecture provides authenticated users secure access to data only they have authorization to view or update.



Known users access begins when they make requests to prdoas2.apps.th.gov.bc.ca/ogs-geoV06 where the SiteMinder Agent gathers user's credentials. SiteMinder rules for this URL allow access only to iDIR and BCeID users. If the user is authenticated a session is created, SiteMinder headers applied, and the requests are forwarded by the reverse proxy server to the load balancer. The load balancer forwards the request to one of the two spatial servers. On the spatial server, the request is received by the security subsystem. The security subsystem takes the user's credentials and queries MoTI's WebADE database for that user's roles. Based on the roles returned for that user the spatial service allows, read, write or no permissions to data. If the user's roles permit it, the spatial data database request is made, and results returned via load balancer and reverse proxy to the user.

3.2 Public Spatial Technical Architecture

MoTI's public spatial architecture provides read only access to a selected spatial data.



Public users make requests to either prdoas3.apps.th.gov.bc.ca/ogs-geoV06 or maps.th.gov.bc.ca/geoV05 at which point Apache or IIS reverse proxy respectively forward the requests to the load balancer and from there to the spatial server which queries spatial database and returns the results back via the load balancer and reverse proxy to the user.

3.3 Supported Software Versions

At the time of writing, the currently supported¹ versions of software at MoTI are:

Oracle RDBMS	11gR2
WebLogic Application Server	10.3.6.0
GeoServer	2.15

Additional software and newer versions may be approved in consultation with the IMB.

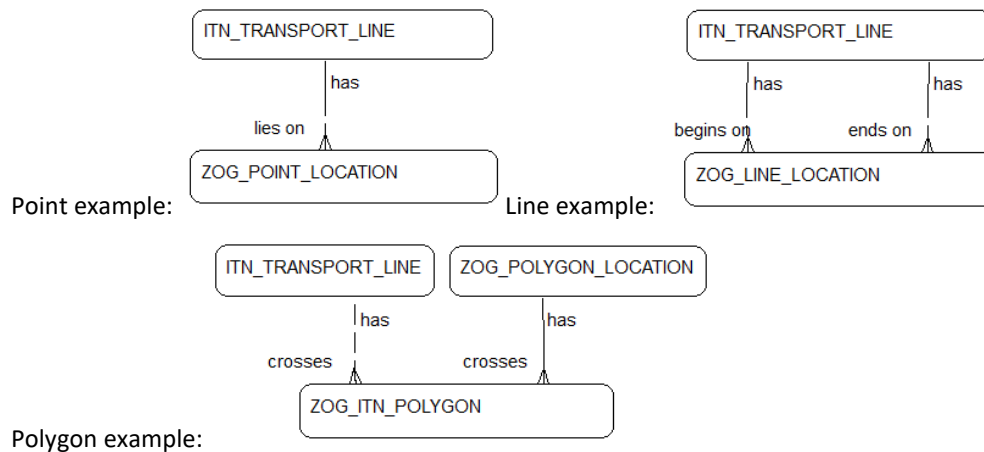
¹ IMB Technology matrix

3.4 Supported Development tools for Building Spatial Applications

IMB supports a modified version of the Java 2 Enterprise Edition architecture for Java application development. Refer to **Oracle Application Server 10g J2EE Applications Services Guide** for more information. Additional development frameworks may be supported and published in the **MoTI Spatial Application Developer's Guide**.

3.5 Location Integration

The Integrated Transportation Network (ITN) is the common provincial network that MoTI uses as the backbone of its critical business systems. All spatial data which is located on or relative to the network must carry a persistent association with the TRANSPORT_LINE_ID of the ITN. Specifically, location entities must have a mandatory foreign key relationship to the ITN. This association with the ITN primary key allows the subject location data to be unambiguously located in all other network aware systems.



3.6 COTS Integration and Interoperability

Where applications are not built to our specifications, but delivered as Commercial-Off-The-Shelf (COTS) packages, it may be specified that they integrate and operate with existing and planned MoTI systems. The mandated interface for such integration and interoperability is the **REST API Development Standard**². For spatial data, COTS must provide an **OGC Standard**³ API.

Where integration and interoperability with other MoTI or BC Government systems has been specified, all spatial data which is located on or relative to the network must carry a persistent association with the TRANSPORT_LINE_ID of the ITN. Therefore, COTS APIs must include TRANSPORT_LINE_ID.

The IMB is developing a platform to become a central location to access, feed, consume, distribute and share information that is relevant across the different business areas of the Ministry. This platform will be comprised of different database platforms, file storage systems and application interfaces (APIs) that will allow systems, applications and individuals to access and consume the information contained in different storage and database

² http://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/rest_api_development_standard.pdf

³ <http://www.opengeospatial.org/docs/is>

sources in a manner that is platform and database agnostic, at the same time that provides flexibility, increases security and promotes collaboration.

The platform foundation is the Enterprise Data Model (EDM), which includes spatial and attribute data and relies on Application Interfaces (APIs) for access, maintenance and distribution of information. The goal is to minimize duplication, increase collaboration, integration, accuracy, flexibility and reporting capabilities; facilitate accessibility, data consumption and reduce development, maintenance and enhancement costs.

3.7 CHRIS

CHRIS is the primary application used to create and maintain spatial MoT road related information in a production environment. For more information on CHRIS contact the CHRIS project manager or refer to the following user manuals:

- Spatial Manager - Basic Functionality/Administration Guide.

Spatial data with a linear reference (driven distance on a route) should have its location entered as an "asset" in CHRIS so that its shape data can be generated out of CHRIS. This is the preferred method of creating shape data for road inventory because:

- CHRIS centre line network is the ministry's corporate linear reference.
- Its shape can be extracted and re-extracted from CHRIS as and when changes are made to the centerline network.
- Relative position to all other ministry assets will be maintained.
- Derivation of location is documented and understood

3.8 Spatial Data Migration

In this pattern, spatial information is considered an immutable part of the application. The development environment is used to maintain or load spatial data. The data is then migrated from the Development environment to the Test environment and finally to the Production environment. This is the same migration path used for application releases--deployment to the development environment then to test and finally the production environment.

3.9 Spatial Application Updates

The OGC Web Feature Service⁴ Transaction (WFS-T) request is the recommended method for creating, updating and deleting spatial data in production applications other than CHRIS. While the WFS-T standard supports feature locking or pessimistic locking, MoTI recommends the use of concurrency control to implement optimistic locking. Example concurrency control code may be found in the **MoTI Spatial Application Developer's Guide**.

WFS-T is supported only on the Authenticated Spatial Server.

3.10 Supported Features of GeoServer at MoTI

Web Map Service (WMS)	Versions 1.1.1 and 1.3.0
-----------------------	--------------------------

⁴ See <http://www.opengeospatial.org/standards/wfs> for all standard specifications of all WFS versions.

Web Feature Service (WFS)	Versions 1.0.0, 1.1.0 and 2.0.0
Web Feature Service Transaction (WFS-T)	Versions 1.0.0 and 1.1.0
Web Coverage Service (WCS)	Pending results of raster storage investigation.

Consult with MoTI if support for additional services such as Web Processing Service (WPS) is required.

GeoServer supports a variety of vendor parameters are non-standard request parameters that are defined by an implementation to provide enhanced capabilities. However, the use of these is discouraged in application development as it binds the application code to a specific implementation of OGC services. Use of GeoServer vendor parameters may only be done in consultation with the IMB and must be specified in the application's Technical Architecture document.

4 Spatial Database

MoTI's standard for the persistence of spatial data is Oracle Spatial. Oracle Spatial is supported in the Oracle Enterprise Edition and "is an integrated set of functions and procedures that enables spatial data to be stored, accessed, and analyzed quickly and efficiently"⁵. A subset of these functions and procedures available in the Oracle Standard Edition is known as Oracle Locator.

4.1 Supported Spatial Data Types

The supported spatial data type at MoTI IMB is SDO_GEOMETRY. SDO_GEOMETRY supports all vector data types, point, line, polygon, multipoint, multiline, multipolygon and collections of all of the previous types. Spatial data must have a minimum of two dimensions, X and Y, but may also contain one or two additional dimensions. Typical use of third and fourth dimensions are for elevation, Z, and measure, M.

IMB is investigating ways to manage and support raster and point cloud data. The results of that investigation will be made available in a new release of this guide.

4.1.1 Use Spatial Data Type for Spatial Data!

Spatial data, typically point locations, are often displayed as Latitude and Longitude for human readability. However, when stored in a database in this form they are not easily integrated with other spatial data. For that reason, *always* represent and store spatial data using a spatial data type.

However, when application design require access to geographic coordinates for data entry, audit or presentation purposes use Oracle's SDO_TRANSFORM function as shown in section 4.3.3 SDO_POINT.

4.2 Modelling Spatial Data

Data for all ministry information systems must be modeled in a Data Architecture modeling tool that supports Barker notation regardless of the intended destination database platform. If you are unfamiliar with MoTI database development practices, refer to the ministry **Data Architecture Standards**⁶.

4.2.1 Spatial Metadata

Simply by looking at spatial data alone, it is impossible to tell how accurate its position is, how old it is, and so on. For example, there can be enormous differences in accuracy between collection methods. Thus, it is important to document information about the data, so that the end users of the data know whether or not it is fit for their use. To make this metadata available to all potential users of the data information about MoTI spatial data should be documented in the DataBC Data Catalogue⁷. The guide to entering information into the DataBC Data Catalogue,

⁵ http://docs.oracle.com/cd/B28359_01/appdev.111/b28400/sdo_intro.htm#SPATL010

⁶

https://projects.sp.th.gov.bc.ca/StrategicServices/_layouts/15/start.aspx#/Data%20Architecture/Forms/AllItems.aspx?RootFolder=%2FStrategicServices%2FData%20Architecture%2FStandards

⁷The catalogue itself is at <https://catalogue.data.gov.bc.ca/dataset>

For readings on custodianship see

http://apps.bcgov/standards/dbc/A_Guide_for_Data_Custodians_and_Data_Managers

complete with video tutorials, may be found at <http://webapps.bcgov/guide/edc/>. The fields and examples are reproduced below.

Spatial Metadata Record.

Title: *a descriptive title*

URL: *(generated by title)*

Organization: *Ministry of Transportation and Infrastructure*

Sub-Organization: *e.g. Information Management - Transportation*

Description: *Some useful notes about the data*

Purpose: *Summary of the intentions for which the dataset was developed*

Data Quality: *Descriptive text that can include info about issues, completeness, consistency, etc.*

Lineage Statement: *Information about the events of source data used in constructing the data.*

More info: *URL links*

Keywords: *Prepopulated list that can be added to*

ISO Topic Category: *This is a fixed list from which you select.*

Contacts

Name: *Contact name*

Email:

Organization: *Ministry of Transportation and Infrastructure*

Sub-Organization:

Role: *businessExpert/custodian/distributor/pointOfContact*

Contact Displayed *(yes/no)*

Data Currency/Update

Resource Status:

completed/destroyed/historicalArchive/obsolete/onGoing/planned/required/underDevelopment

Date type: *Archived/Created/Destroyed/Modified/Published*

Date: *YYYY-MM-DD*

(these two fields may be repeated as often as required)

Access & Security

Who can view this data?: *Government/Named users/Public*

Who can download this data?: *Government/Named users/Public*

Who can view this record?: *IDIR/Public*

License: *Access Only/Open Government License-British Columbia/...*

Security Classification: *HIGH-CABINET/HIGH-CONFIDENTIAL/HIGH-SENSITIVITY/LOW-PUBLIC/LOW-SENSITIVITY/MEDIUM-PERSONAL/MEDIUM-SENSITIVITY*

More optional information

Preview Information

Image URL:

Link to iMap: *for data sets stored in the BCGW*

GeoGraphic Extent

North: *60.0* South: *48.0* East: *-113.5* West: *-139.5*

Object Name:

Photo upload *(upload or link)*

4.2.2 Collection of Spatial Data

Spatial data is created in myriad ways, from engineering surveys, to Inertial Measuring Units (IMU), to users clicking on a web map. Spatial data should always be collected with its end purpose in mind. If a large data collection project is to be undertaken it is prudent to perform a small sample collection to verify that the results

are fit for their purpose. Engage the IMB Spatial Data Architecture team *before* collecting spatial data destined for inclusion in a ministry information system to ensure trouble free integration of your data.

For standards for engineering data refer to the **General Survey Guide for the BC Ministry of Transportation and Infrastructure** (http://www.th.gov.bc.ca/publications/eng_publications/survey/general_survey_guide.pdf). For most other survey types refer to the GeoBC's **Standards and Specifications** page, <http://geobc.gov.bc.ca/base-mapping/atlas/gsr/specs.html>.

Where web maps such as Google, Bing, or Open Street Map are used to collect locations from user clicks it is important to know that the error of such positions is in the order of 10 meters⁸.

4.3 SDO_GEOMETRY

Oracle's SDO_GEOMETRY datatype is an object datatype defined as follows:

```
CREATE TYPE sdo_geometry AS OBJECT ( SDO_GTYPE NUMBER, SDO_SRID NUMBER,  
SDO_POINT SDO_POINT_TYPE, SDO_ELEM_INFO SDO_ELEM_INFO_ARRAY, SDO_ORDINATES  
SDO_ORDINATE_ARRAY );
```

The following sections describe each of the subtypes.

4.3.1 SDO_GTYPE

SDO_GTYPE is a four digit number indicating if this is a POINT, LINESTRING, POLYGON, COLLECTION, MULTIPOINT, MULTILINESTRING, MULTIPOLYGON, the number of dimensions and whether or not a Linear Reference System (LRS) measure is used.

Value	Geometry Type	Example
dl01	POINT	2001 , A simple point
dl02	LINE or CURVE	2002 , A simple line string 3302 , A measured line string (may be represented as 3002*) 3002 , A line string with elevation
dl03	POLYGON	2003 , A simple polygon
dl04	COLLECTION	2004 , A single geometry object containing disparate geometry types
dl05	MULTIPOINT	2005 , Two or more points in a single geometry object
dl06	MULTILINE or MULTICURVE	2006 , Two or more line segments in a single geometry object
dl07	MULTIPOLYGON	2007 , Two or more polygons in a single geometry object

The **d** in the Value column is the number of dimensions: 2, 3, or 4. For example, an SDO_GTYPE value of 2003 indicates a two-dimensional polygon.

The **l** identifies the linear referencing measure dimension for a three-dimensional linear referencing system (LRS) geometry, that is, which dimension (3 or 4) contains the measure value. *For a non-LRS geometry, or to accept the spatial default of the last dimension as the measure for an LRS geometry, specify 0.

⁸ An Evaluation of the Horizontal Positional Accuracy of Google and Bing Satellite Imagery and Three Roads Data Sets Based on High Resolution Satellite Imagery

http://www.ciesin.columbia.edu/confluence/download/attachments/19726351/Ubukawa_PositionalAccuracy_march2013.pdf?version=1&modificationDate=1363795265000

4.3.2 SRID and Standard Projection

All MoTI standard projection for spatial data is BC Albers which is an Albers Equal Area Conic projection with parameters of :

- Central meridian: -126.0 (126:00:00 West longitude)
- First standard parallel: 50.0 (50:00:00 North latitude)
- Second standard parallel: 58.5 (58:30:00 North latitude)
- Latitude of projection origin: 45.0 (45:00:00 North latitude)
- False northing: 0.0
- False easting: 1000000.0 (one million metres)

And a chosen datum of NAD83, based on the GRS80 ellipsoid. Therefore SRID will always be 3005.

This projection is also known by European Petroleum Survey Group as EPSG:3005⁹ and NAD_1983_BC_Environment_Albers (EPSG:3005) in ESRI nomenclature. It has been in use in the government of BC for more than two decades. Adherence to this standard for the *internal* representation simplifies the operation and maintenance of spatial data through its entire life cycle.

4.3.3 SDO_POINT

The SDO_POINT attribute is defined using the SDO_POINT_TYPE object type, which has the attributes X, Y, and Z, all of type NUMBER. If SDO_POINT is used, the remaining two elements should be NULL.

Example insert statement

```
INSERT INTO TSG_SURVEY (SURVEY_ID, GEOMETRY) VALUES (1,  
MDSYS.SDO_GEOMETRY(2001, 3005, MDSYS.SDO_POINT_TYPE(1452017.1014, 890806.808,  
NULL), NULL, NULL));
```

Insert using Well Known Text¹⁰ (WKT) constructor

```
INSERT INTO SAMPLE_LOCATION VALUES (1, 'Trent River Sign', 49.64155, -  
124.93151, SDO_GEOMETRY('POINT(1077204.891 514506.395)', 3005));
```

Insert that re-projects from World Geodetic System

```
INSERT INTO TIG_TMS_GEOMETRY_EXT (ID, GEOMETRY) VALUES (1,  
SDO_CS.TRANSFORM(SDO_GEOMETRY(2001, 4326, SDO_POINT_TYPE(-119.5354, 49.8817,  
NULL), NULL, NULL), 3005));
```

Note that because Longitude is the X axis, it is listed *before* Latitude, the Y axis.

Display BC Albers Point as Geographic

```
SELECT SDO_CS.TRANSFORM(S.GEOMETRY, 4326).SDO_POINT.Y AS LAT,  
SDO_CS.TRANSFORM(S.GEOMETRY, 4326).SDO_POINT.X AS LAT FROM SAMPLE_LOCATION S  
WHERE ROWNUM = 1;
```

⁹ <http://spatialreference.org/ref/epsg/nad83-bc-albers/>

¹⁰ For more examples of WKT visit https://en.wikipedia.org/wiki/Well-known_text

4.3.4 SDO_ELEM_INFO

SDO_ELEM_INFO is an object of type SDO_ELEM_INFO_ARRAY which is a varying length array (1048576) of NUMBER. It describes the elements stored in the SDO_ORDINATES object. The SDO_ELEM_INFO_ARRAY consists of:

1. an Ordinate Offset
2. an Element Type
3. an Interpretation

This triplet may repeat itself for Compound Linestrings and Compound Polygons. When that happens, in the first triplet the "Interpretation" field represents the number of Linestrings that make up this shape.

4.3.5 SDO_ORDINATES

SDO_ORDINATES is a VARRAY(1048576) of NUMBER that stores ordered coordinate values. The array consists of repeating values of:

- X and Y; or
- X, Y, Z or M if a third dimension *or* measures for Linear Referencing is used; or
- X, Y, Z and M if a third dimension *and* measures (being the fourth dimension) is used.

Example insert of a two dimensional line

```
INSERT INTO CIS_LKI_SEGMENT_GEOMETRY_EXT (
LKI_SEGMENT_GEOMETRY_EXT_ID,GEOMETRY ) VALUES ( 12, MDSYS.SDO_GEOMETRY(2002,
3005, , (1, 2, 1), (1131719.75, 425154, 1134105.128, 424068.41,
1134828.625, 423733, 1135752.75, 423323.906))) ;
```

Insert of measured line

```
INSERT INTO RFI_ROAD_SEGMENT VALUES
(1,MDSYS.SDO_GEOMETRY(3302,3005,NULL,MDSYS.SDO_ELEM_INFO_ARRAY(1,2,1),MDSYS.S
DO_ORDINATE_ARRAY(933984.25,1086163.109,0,934109.955,1085916.961,0.293,934156
.327,1085882.461,0.355))
```

Insert of polygon

```
INSERT INTO ZZZ_PROPERTY_BOUNDARY (ID, GEOMETRY) VALUES (1,
MDSYS.SDO_GEOMETRY(2003,3005,NULL,MDSYS.SDO_ELEM_INFO_ARRAY(1,1003,
1),MDSYS.SDO_ORDINATE_ARRAY(1234132.1125,469734,1234118.3125,469739.7625,
1234119.275,469719.55,1234133.075,469713.775,1234132.1125, 469734))) ;
```

Polygons must be closed to be valid. Specifically, the last X and Y values of a polygon SDO_ORDINATE array must be identical to the first X and Y values.

4.3.6 Table Configuration

Due to constraints imposed by ESRI products such as ArcSDE, ArcCatalog and ArcMap, IMB had promoted a two table configuration which split tables containing a spatial column from those containing other attributes. With the retirement of the ESRI technology stack these constraints are lifted. A spatial column may be treated like any other attribute column.

The benefits of this single table configuration are:

- Minimizes the number of joins

- Number of attribute queries is minimized. Attribute information for a particular feature is stored in the same row as the shape information.
- The spatial and attribute information are synchronized on data load.
- Data is centralized and integrated.
- Client data analysis tools can be used on all of the data.
- Editing can be performed on both the spatial and attribute data at the same time, thus reducing the number of applications for data maintenance.
- Rendering of spatial data is fast.

4.3.7 Estimating spatial table size

According to an Oracle Technology White Paper¹¹, "Oracle Spatial requires about 1.35 times as much storage as ESRI shapefiles."

A more detailed estimate may be obtained from the following table.

SDO_GTYPE	3 bytes plus 1 byte for every two numeric places
SDO_SRID	1 byte if NULL; or 3 bytes plus 1 byte for every two numeric places
SDO_POINT	1 byte if NULL; or for each of the three numeric values, 1 byte if NULL, or 3 bytes plus 1 byte for every two numeric places
SDO_ELEM_INFO	1 byte if NULL; or for each numeric value, 3 bytes plus 1 byte for every two numeric places, plus 40 bytes overhead for the VARRAY.
SDO_ORDINATES	1 byte if NULL; or for each numeric value, 3 bytes plus 1 byte for every two numeric places, plus 40 bytes overhead for the VARRAY.

Point type example:

Say you have data consisting of 30,000 points with a typical point object being:

```
SDO_GEOMETRY(2001, 3005, MDSYS.SDO_POINT_TYPE(1452017.1014, 890806.808,
NULL), NULL, NULL)
```

SDO_GTYPE	= 3 bytes + 1 byte = 4 bytes
SDO_SRID	= 3 bytes + 2 bytes = 5 bytes
SDO_POINT	= (3 + 5) + (3 + 5) + 1 = 17 bytes
SDO_ELEM_INFO	= 1 byte (set to NULL)
SDO_ORDINATES	= 1 byte (set to NULL)
Total	= 28 bytes

Estimate storage requirements for the geometry column to be 29 x 30,000 = 840,000 bytes or 820 MB.

Line type example:

Say you have data consisting of 5,000 measured line segments with a typical line object being:

¹¹ Based on <http://www.oracle.com/technetwork/database/enterprise-edition/spatial-perf-twp-130138.pdf>

```
SDO_GEOMETRY(3302,3005,NULL,MDSYS.SDO_ELEM_INFO_ARRAY(1,2,1),MDSYS.SDO_
ORDINATE_ARRAY(934310,1076083.505,0,..<500 omitted
vertices>..937920.6,1075895.8,3.723))
```

SDO_GTYPE	= 3 bytes + 1 byte = 4 bytes
SDO_SRID	= 3 bytes + 2 bytes = 5 bytes
SDO_POINT	= 1 byte (set to NULL)
SDO_ELEM_INFO	= 4 bytes + 4 bytes + 4 bytes + 40 bytes = 52 bytes
SDO_ORDINATES	= (avg. number ordinates * (5 + 5 bytes)) + 40 bytes = (500 * 10) + 40 bytes = 5040 bytes
Total	= 5,102 bytes

Estimate storage requirements for the geometry column to be 5,102 x 5,000 =25,510,000 bytes or 24 GB.

Clearly storage requirements for complex line or polygon geometries need to be considered carefully as there is a linear relationship between total number of vertices and storage requirements.

The number of vertices stored should be appropriate for the intended use. Some capture methods create large numbers of closely spaced vertices and may require simplification to achieve acceptable performance.

Please consult with the IM/IT Infrastructure team before implementing any application changes resulting in considerable storage increases to ensure disk space can be procured and table sizes configured appropriately.

4.4 Spatial Tables and Views

All spatial tables and views must follow **Data Architecture Standards**.

While Oracle allows tables and views to contain multiple spatial columns, client software such as GeoServer, ArcMap and QGIS allow only one.

Spatial tables and views intended for use with GeoServer must expose a primary key field.

4.5 Spatial Index

Oracle Spatial layers must have a spatial index defined on their GEOMETRY column. A spatial index cannot be generated from Oracle Designer and must be created from a script. For example:

```
CREATE INDEX CIS_COLLOC_GEOMETRY_I ON
CIS_COLLISION_LKI_LOCATION(GEOMETRY) INDEXTYPE IS MDSYS.SPATIAL_INDEX
parameters ('LAYER_GTYPE=point TABLESPACE=CIS_INDEX1');
```

It is recommended that the parameter 'LAYER_GTYPE' always be specified. It will prevent incorrect data types from being loaded and assist with internal query optimizations. Refer to the table in section 4.3.1 SDO_GTYPE for the list of valid GYPES.

Creating an Oracle Spatial Index generates two Oracle Objects:

- 1) An Oracle Table of the form MDRT_(random characters) and
- 2) An Oracle Sequence of the form MDRS_(random characters) for R Tree index or MDQT_(random characters) for Quad Tree index.

R Tree index is recommended by Oracle.

4.6 Users

Access to spatial data is via proxy user. The proxy user's credentials are used to make the JDBC connection between GeoServer and the Database in **Error! Reference source not found.** The proxy user's database privilege is controlled via the role or roles granted.

4.6.1 Naming Convention

APP_aaa_PROXY_OGS_READ Typically granted aaa_GIS_READ role

APP_aaa_PROXY_OGS_EDIT Typically granted aaa_GIS_EDIT role

where **aaa** is the business application short name.

4.7 GeoServer Security Model

MoTI has two separate GeoServer services: one for spatial data with no access restrictions, and one for spatial data requiring authenticated and authorized access. If there are no access restrictions on your spatial data, it may be accessed by anonymous users from anywhere on the Internet. Authenticated access requires either an IDIR or a BCeID account. Authentication service is provided by SiteMinder. Authorization service is provided by WebADE.

4.7.1 WebADE Profiles and Roles

Named users with either IDIR or BCeID accounts are granted permission to restricted spatial data via WebADE profiles. The end user tool for this is Authority Delegation and Management (ADAM)¹². For complete details on creating WebADE Profiles and Roles for spatial data access refer to the **MoTI Spatial Application Developer's Guide**.

4.7.2 GeoServer Roles

At the OGC service level, access to an entire namespace or individual layer may be restricted to:

NONE No access;

READ Read only access is permitted; and

WRITE WFS-T operations are permitted

GeoServer interrogates WebADE to determine which roles in the OGS Application are assigned the current user.

5 Creating Spatial Data

New information systems may need to be pre-populated with data when launched. This initial load of data must be done in co-operation with the Spatial Data Architecture team and the IM/IT Infrastructure team. Developers

¹² MoTI's ADAM administration is located at <https://devoas1.apps.th.gov.bc.ca/adam/>, <https://tstoas2.apps.th.gov.bc.ca/adam> and <https://prdoas2.apps.th.gov.bc.ca/adam/> for DEV, TST and PRD environments respectively.

should develop spatial data loading scripts against their own database environments prior to delivery to the MoTI development environment.

5.1 Oracle Spatial Metadata Entry

Tables using SDO_GEOMETRY must have a metadata entry in the Oracle Dictionary View USER_SDO_GEOM_METADATA. This entry contains the following:

TABLE_NAME	VARCHAR2(32)	The table that contains the SDO_GEOMETRY column.
COLUMN_NAME	VARCHAR2(1024)	The name of the SDO_GEOMETRY column.
DIMINFO	SDO_DIM_ARRAY: VARRAY(4) of SDO_DIM_ELEMENT object	See SDO_DIM_ELEMENT below.
SRID	NUMBER	To match the SRID in the geometry object. For MoTI this will always be 3005.

Note: All Oracle Spatial table and SDO_GEOMETRY column names must be created in UPPERCASE.

SDO_DIM_ELEMENT object is comprised of:

SDO_DIMNAME	VARCHAR2(64)	Dimension name.
SDO_LB	NUMBER	Lower bound for this dimension in meters
SDO_UB	NUMBER	Upper bound for this dimension in meters
SDO_TOLERANCE	NUMBER	The distance in meters required between two coordinates so they are not considered to be the same coordinate.

Note: Set SDO_TOLERANCE to be 1/2 the smallest distance between any two vertices. For example, where coordinates are accurate to 10cm (0.01 meters), set the SDO_TOLERANCE to be 0.005.

Example meta data insert script for two dimensional layer:

```
INSERT INTO USER_SDO_GEOM_METADATA VALUES (
  'CIS_LKI_SEGMENT_GEOMETRY_EXT',
  'GEOMETRY',
  MDSYS.SDO_DIM_ARRAY(
    MDSYS.SDO_DIM_ELEMENT('X', 200000.000, 1900000.000, 0.005),
    MDSYS.SDO_DIM_ELEMENT('Y', 300000.000, 1800000.000, 0.005)
  ),
  3005
);
```

Note upper and lower bounds shown in this example safely enclose the entire province. Even if your data set has a much smaller extent, it is recommended that you use these bounds to allow for future growth.

Example meta data insert script for three dimensional layer where the third dimension is length measure:

```
INSERT INTO USER_SDO_GEOM_METADATA VALUES (
  'CIS_LKI_SEGMENT_GEOMETRY_EXT',
  'GEOMETRY',
  MDSYS.SDO_DIM_ARRAY(
    MDSYS.SDO_DIM_ELEMENT('X', 200000.000, 1900000.000, 0.005),
    MDSYS.SDO_DIM_ELEMENT('Y', 300000.000, 1800000.000, 0.005),
    MDSYS.SDO_DIM_ELEMENT('M', 0, 1000000, .005)
  ),
  3005
);
```

3005

);

5.2 Initial Data Loading

5.2.1 SQL Scripts

SQL scripts targeting the MoTI database environment must contain no user names, passwords or COMMIT statements. Where user names or passwords are required they should be as prompts. Expected record counts should be listed in the comments at the head of the script.

```
/*
zzz-01-00-00-location-inserts.sql
Purpose: Initial population of location table in ZZZ 1.0 application.
Prepared by: Conscientious Contracting
Date: June 15, 2016
Does 1 insert.
*/
prompt Loading LOCATION TABLE - should DO 100 INSERTs
INSERT INTO ZZZ_LOCATION (LOCATION_ID,GEOMETRY) VALUES (1,
SDO_CS.TRANSFORM(SDO_GEOMETRY(2001, 4326, SDO_POINT_TYPE(-119.5354,
49.8817, NULL), NULL, NULL),3005 ));
```

5.2.2 FME Workspaces

Feature Manipulation Engine Workspaces (FMWs) may be used for spatial data loading. Connection information such as database server, port, schema, username and password must exist only in Published Parameters and never hard-coded in scripts. This allows for portability between environments. For an in-depth discussion of FME template including logging see DataBC's FME Standards and Template¹³ page.

Published Parameter	Example Value
Dest_Instance	DEVAA
User_ID	APP_ZZZ_DEVELOPER
DestFeature1	ZZZ_LOCATION_GEOMETRY
SourceDataset	\\armor\zzz\data\location\Tenure_Areas.gdb
Dest_Server	BRAZEN1.TH.GOV.BC.CA
Dest_Instance_Port	20204
Dest_Password	Your app_zzz_developer password

This script is then portable between environments when run from the command line:

```
"D:\Program Files (x86)\FME\fme.exe"
D:\FMEscripts\PRD\PRDAA\ZZZ_LOC_GEO_LOAD.fmw
```

¹³ http://apps.bcgov/standards/dbc/FME_Standards_and_Template

```
--SourceDataset "\\armor\zzz\data\location\Final_Tenure_Areas.gdb"  
--UserID "APP_ZZZ"  
--Dest_Password "*** enter password here ***"  
--Dest_Instance "PRDAA"  
--Dest_Server "CHASER1.TH.GOV.BC.CA"  
--Dest_Instance_Port "20204"
```

5.3 Validating Spatial Data

The following script will list any invalid geometry records:

```
SELECT f.PK_ID,  
sdo_geom.validate_geometry_with_context(f.GEOMETRY, m.DIMINFO) AS vgeom  
FROM APP_ZZZ.ZZZ_SPATIAL_TABLE f,  
all_sdo_geom_metadata m  
WHERE m.table_name = 'APP_ZZZ.ZZZ_SPATIAL_TABLE'  
AND m.column_name = 'GEOMETRY'  
AND sdo_geom.validate_geometry_with_context(f.SHAPE, m.DIMINFO) NOT IN  
('NULL', 'TRUE', 'FALSE')  
ORDER BY f.PK_ID;
```

where

PK_ID Is the primary key column

ZZZ_SPATIAL_TABLE is the table containing the SDO_GEOMETRY column

GEOMETRY is the name of the SDO_GEOMETRY column

The error codes, if any, returned indicate why the validation failed. ORA 13356 is one of the most typical geometry validation problems. It is caused when the distance between two or more vertices is smaller than the tolerance value set in the USER_SDO_GEOM_METADATA table (5.1 Oracle Spatial Metadata Entry).

5.4 Updates to Spatial Data

Where spatial data is expected to require changes beyond the initial load, the application must provide a mechanism to allow an end users or administrative users the ability to make those changes. *It is not acceptable to rely on scripts run by IMB technical support staff to perform data updates in production.* The exception to this rule is views based on CHRIS spatial data as that data is updated via the CHRIS program.

For information on using applications to update spatial data refer to the **MoTI Spatial Application Developer's Guide**.

6 Appendix A. Glossary of Terms

The following terms are used throughout this document and are defined below for clarification.

<i>Term</i>	<i>Definition</i>
OGC	Open Geospatial Consortium, an international voluntary consensus standards organization dedicated to improving geospatial data sharing.
cURL	A command line tool for getting or sending files using URL syntax.
Metadata	Metadata describes a number of characteristics or attributes of data; that is, "data that describes data"
MoTI	Ministry of Transportation and Infrastructure
IMB	Information Management Branch
WMS	Web Map Service is a standard protocol for serving georeferenced map images over the internet
WFS	Web Feature Service is a standard protocol for creating, modifying and exchanging vector format geographic information over the internet
CHRIS	Corporate Highway Resource Information System is a customization of "Highways by exor" software owned by Bentley Systems.
FME	Feature Manipulation Engine, is data transformation and translation program by Safe Software.
WPS	Web Processing Service specifies a means for a client to request the execution of a spatial calculation from a service.

7 Appendix B Sample SLD

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<StyledLayerDescriptor version="1.0.0" xmlns="http://www.opengis.net/sld"
xmlns:ogc="http://www.opengis.net/ogc" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.opengis.net/sld
http://schemas.opengis.net/sld/1.0.0/StyledLayerDescriptor.xsd">
  <NamedLayer>
    <Name>BSR_simple</Name>
    <UserStyle>
      <Title>BSR Rendering</Title>
      <FeatureTypeStyle>

        <!-- BRIDGE -->
        <Rule>
          <Name>Level3</Name>
          <Title>BRIDGE</Title>
          <Abstract>Zoom Level 3 BSR</Abstract>
          <ogc:Filter>
            <ogc:PropertyIsEqualTo>
              <ogc:PropertyName>STRUCTURE_TYPE</ogc:PropertyName>
              <ogc:Literal>BRIDGE</ogc:Literal>
            </ogc:PropertyIsEqualTo>
          </ogc:Filter>
          <MinScaleDenominator>250000.0</MinScaleDenominator>
          <PointSymbolizer>
            <Graphic>
              <Mark>
                <WellKnownName>circle</WellKnownName>
                <Fill>
                  <CssParameter name="fill">#5A59E7</CssParameter>
                </Fill>
              </Mark>
              <Size>6</Size>
            </Graphic>
          </PointSymbolizer>
        </Rule>
        <Rule>
          <Name>Level2</Name>
          <Title>BRIDGE</Title>
          <ogc:Filter>
            <ogc:PropertyIsEqualTo>
              <ogc:PropertyName>STRUCTURE_TYPE</ogc:PropertyName>
              <ogc:Literal>BRIDGE</ogc:Literal>
            </ogc:PropertyIsEqualTo>
          </ogc:Filter>
          <MinScaleDenominator>30000.0</MinScaleDenominator>
          <MaxScaleDenominator>249999.0</MaxScaleDenominator>
          <PointSymbolizer>
```

```

<Graphic>
  <ExternalGraphic>
    <OnlineResource xlink:type="simple" xlink:href="image/BSR_BRIDGE.png"/>
    <Format>image/png</Format>
  </ExternalGraphic>
  <Size>24</Size>
</Graphic>
</PointSymbolizer>
<TextSymbolizer>
  <Label>
    <ogc:PropertyName>STRUCTURE_NO</ogc:PropertyName>
  </Label>
  <Font>
    <CssParameter name="font-family">Arial</CssParameter>
    <CssParameter name="font-style">Normal</CssParameter>
    <CssParameter name="font-size">11</CssParameter>
    <CssParameter name="font-weight">normal</CssParameter>
  </Font>
  <LabelPlacement>
    <PointPlacement>
      <Displacement>
        <DisplacementX>8</DisplacementX>
        <DisplacementY>8</DisplacementY>
      </Displacement>
    </PointPlacement>
  </LabelPlacement>
  <Halo>
    <Radius>2</Radius>
    <Fill>
      <CssParameter name="fill">#FFFFFF</CssParameter>
      <CssParameter name="fill-opacity">0.7</CssParameter>
    </Fill>
  </Halo>
  <Fill>
    <CssParameter name="fill">#5A59E7</CssParameter>
  </Fill>
  <VendorOption name="group">no</VendorOption>
  <VendorOption name="spaceAround">2</VendorOption>
</TextSymbolizer>
</Rule>
<Rule>
  <Name>Level1</Name>
  <Title>BRIDGE</Title>
  <Abstract>Zoom Level 1 BSR</Abstract>
  <ogc:Filter>
    <ogc:PropertyIsEqualTo>
      <ogc:PropertyName>STRUCTURE_TYPE</ogc:PropertyName>
      <ogc:Literal>BRIDGE</ogc:Literal>
    </ogc:PropertyIsEqualTo>
  </ogc:Filter>

```

```
</ogc:Filter>
<MinScaleDenominator>0</MinScaleDenominator>
<MaxScaleDenominator>29999.0</MaxScaleDenominator>
<LineSymbolizer>
  <Stroke>
    <CssParameter name="stroke">#5A59E7</CssParameter>
    <CssParameter name="stroke-width">8.0</CssParameter>
    <CssParameter name="stroke-linecap">round</CssParameter>
  </Stroke>
</LineSymbolizer>
<TextSymbolizer>
  <Label>
    <ogc:PropertyName>STRUCTURE_NO</ogc:PropertyName>
  </Label>
  <Font>
    <CssParameter name="font-family">Arial</CssParameter>
    <CssParameter name="font-style">Normal</CssParameter>
    <CssParameter name="font-size">11</CssParameter>
    <CssParameter name="font-weight">normal</CssParameter>
  </Font>
  <LabelPlacement>
    <LinePlacement>
      <PerpendicularOffset>9</PerpendicularOffset>
    </LinePlacement>
  </LabelPlacement>
  <Halo>
    <Radius>2</Radius>
  </Halo>
  <Fill>
    <CssParameter name="fill">#FFFFFF</CssParameter>
    <CssParameter name="fill-opacity">0.7</CssParameter>
  </Fill>
  <Halo>
    <Fill>
      <CssParameter name="fill">#5A59E7</CssParameter>
    </Fill>
  </Halo>
  <VendorOption name="group">no</VendorOption>
  <VendorOption name="spaceAround">2</VendorOption>
</TextSymbolizer>
</Rule>
</FeatureTypeStyle>
</UserStyle>
</NamedLayer>
</StyledLayerDescriptor>
```

8 Appendix C cURL script for WMS performance test

Note that the script is using `devoas1.apps.th.gov.bc.ca/ogs-geoV06` as the GeoServer host and path and `name_space:LAYER_NAME` as the namespace and layer name.

First save your SiteMinder credentials in a file named "headers"

```
curl -O -k -X POST --dump-header headers -u "user_name:password"  
"https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG%3A3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
15484541,6140192,-12690421,8549737&foo=.png"
```

Next request your layer at zoom levels appropriate for your application use cases. Given are rural and urban examples.

Response times should be within the performance expectations for the application or service you are building.

8.1 Hudson's Hope Bridge (rural)

zoomX -13579350

zoomY 7556100

8.1.1 BBOX values for 13 zoom levels beginning with the provincial extent

```
-15484541,6140192,-12690421,8549737  
-14277880,6953714,-12880820,8158486  
-13928615,7254907,-13230085,7857293  
-13753982,7405504,-13404718,7706696  
-13666666,7480802,-13492034,7631398  
-13623008,7518451,-13535692,7593749  
-13601179,7537276,-13557521,7574924  
-13590264,7546688,-13568436,7565512  
-13584807,7551394,-13573893,7560806  
-13582078,7553747,-13576622,7558453  
-13580714,7554924,-13577986,7557276  
-13580032,7555512,-13578668,7556688  
-13579691,7555806,-13579009,7556394
```

8.1.2 Complete cURL requests

```
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
15484541,6140192,-12690421,8549737&foo=.png"  
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
14277880,6953714,-12880820,8158486&foo=.png"  
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
```



```
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13928615,7254907,-13230085,7857293&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13753982,7405504,-13404718,7706696&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13666666,7480802,-13492034,7631398&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13623008,7518451,-13535692,7593749&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13601179,7537276,-13557521,7574924&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13590264,7546688,-13568436,7565512&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13584807,7551394,-13573893,7560806&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13582078,7553747,-13576622,7558453&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13580714,7554924,-13577986,7557276&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13580032,7555512,-13578668,7556688&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-
13579691,7555806,-13579009,7556394&foo=.png"
```

8.2 Port Mann Bridge (urban)

zoomX -13671500
zoomY 6312200

8.2.1 BBOX values for 13 zoom levels beginning with the provincial extent

-15484541, 6140192, -12690421, 8549737

-14370030,5709814,-12972970,6914586
-14020765,6011007,-13322235,6613393
-13846132,6161604,-13496868,6462796
-13758816,6236902,-13584184,6387498
-13715158,6274551,-13627842,6349849
-13693329,6293376,-13649671,6331024
-13682414,6302788,-13660586,6321612
-13676957,6307494,-13666043,6316906
-13674228,6309847,-13668772,6314553
-13672864,6311024,-13670136,6313376
-13672182,6311612,-13670818,6312788
-13671841,6311906,-13671159,6312494

8.2.2 Complete cURL requests

```
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-15484541,6140192,-12690421,8549737&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-14370030,5709814,-12972970,6914586&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-14020765,6011007,-13322235,6613393&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-13846132,6161604,-13496868,6462796&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-13758816,6236902,-13584184,6387498&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-13715158,6274551,-13627842,6349849&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-13693329,6293376,-13649671,6331024&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-13682414,6302788,-13660586,6321612&foo=.png"
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=256&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-13676957,6307494,-13666043,6316906&foo=.png"
```

```
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
13674228,6309847,-13668772,6314553&foo=.png"  
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
13672864,6311024,-13670136,6313376&foo=.png"  
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
13672182,6311612,-13670818,6312788&foo=.png"  
curl -O -k -X GET -b headers "https://devoas1.apps.th.gov.bc.ca/ogs-  
geoV06/wms?SERVICE=WMS&VERSION=1.1.1&REQUEST=GetMap&FORMAT=image/png&WIDTH=25  
6&HEIGHT=256&SRS=EPSG:3857&LAYERS=name_space:LAYER_NAME&BBOX=-  
13671841,6311906,-13671159,6312494&foo=.png"
```

9 Appendix D cURL scripts for WFS-Transaction test

The following examples create, update and then delete a spatial record.

First save your SiteMinder credentials in a file named "headers"

```
curl -k -X POST --dump-header headers -u "your_id:your_password"
"https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wms?SERVICE=WFS&VERSION=1.0.0&REQUEST=GetCapabilities"
```

Using the XML files shown below, run the following cURL command:

```
curl -k -H "Content-type: xml" -b headers -v -X POST -d@request.xml
"https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wfs" -o response.xml
```

9.1 Create a record

Use the following request.xml

```
<wfs:Transaction service="WFS" version="1.2.0"
  xmlns:wfs="http://www.opengis.net/wfs"
  xmlns:hed="http://th.gov.bc.ca/name_space"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/wfs
http://schemas.opengis.net/wfs/1.0.0/WFS-transaction.xsd
http://th.gov.bc.ca/name_space https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/wfs/DescribeFeatureType?typename=name_space:LAYER_NAME">
  <wfs:Insert>
    <name_space:LAYER_NAME>
      <name_space:SHAPE>
        <gml:Polygon srsName="EPSG:4326">
          <gml:exterior>
            <gml:LinearRing>
              <gml:posList>
                -128 51 -126 50 -125.5 50.5 -128 51
              </gml:posList>
            </gml:LinearRing>
          </gml:exterior>
        </gml:Polygon>
      </name_space:SHAPE>
      <name_space:NON_SPATIAL_COLUMN>2015</name_space:NON_SPATIAL_COLUMN>
    </name_space:LAYER_NAME>
  </wfs:Insert>
</wfs:Transaction>
```

Where

xmlns:name_space="http://th.gov.bc.ca/name_space"	URI of the namespace
https://devoas1.apps.th.gov.bc.ca/ogs-geoV06	GeoServer URL
name_space	namespace aka Workspace
LAYER_NAME	GeoServer feature type
SHAPE	SDO_GEOMETRY column
NON_SPATIAL_COLUMN	(optional) column
EPSG:4326	Projection for coordinates

The expected response from this insert request should look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<wfs:TransactionResponse xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:wfs="http://www.opengis.net/wfs"
xmlns:hed="http://th.gov.bc.ca/name_space"
xmlns:gml="http://www.opengis.net/gml"
xmlns:ogc="http://www.opengis.net/ogc" xmlns:ows="http://www.opengis.net/ows"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.1.0"
xsi:schemaLocation="http://www.opengis.net/wfs
https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/schemas/wfs/1.1.0/wfs.xsd">
  <wfs:TransactionSummary>
    <wfs:totalInserted>1</wfs:totalInserted>
    <wfs:totalUpdated>0</wfs:totalUpdated>
    <wfs:totalDeleted>0</wfs:totalDeleted>
  </wfs:TransactionSummary>
  <wfs:TransactionResults/>
  <wfs:InsertResults>
    <wfs:Feature>
      <ogc:FeatureId fid="LAYER_NAME.dddd"/>
    </wfs:Feature>
  </wfs:InsertResults>
</wfs:TransactionResponse>
```

Where **dddd** is the unique key for the created record.

9.2 Update a Record

Use the following request.xml

```
<wfs:Transaction service="WFS" version="1.2.0"
xmlns:wfs="http://www.opengis.net/wfs"
xmlns:ogc="http://www.opengis.net/ogc"
xmlns:name_space="http://th.gov.bc.ca/name_space"
xmlns:gml="http://www.opengis.net/gml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.opengis.net/wfs
http://schemas.opengis.net/wfs/1.0.0/WFS-transaction.xsd
http://th.gov.bc.ca/name_space https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wfs/DescribeFeatureType?typename=name_space:LAYER_NAME">
  <wfs:Update typeName="name_space:LAYER_NAME">
    <ogc:Filter>
      <ogc:PropertyIsEqualTo>
        <ogc:PropertyName>LAYER_NAME_ID</ogc:PropertyName>
        <ogc:Literal>dddd</ogc:Literal>
      </ogc:PropertyIsEqualTo>
    </ogc:Filter>
    <wfs:Property xmlns:gml="http://www.opengis.net/gml">
      <wfs:Name>SHAPE</wfs:Name>
      <wfs:Value>
        <hed:SHAPE>
          <gml:Polygon srsName="EPSG:4326">
```

```

        <gml:exterior>
          <gml:LinearRing>
            <gml:posList>
              -128 51 -123 49 -125.5 50.5 -128 51
            </gml:posList>
          </gml:LinearRing>
        </gml:exterior>
      </gml:Polygon>
    </hed:SHAPE>
  </wfs:Value>
</wfs:Property>
<wfs:Property>
  <wfs:Name>NON_SPATIAL_COLUMN</wfs:Name>
  <wfs:Value>2016</wfs:Value>
</wfs:Property>
</wfs:Update>
</wfs:Transaction>

```

where

xmlns:name_space="http://th.gov.bc.ca/name_space"	URI of the namespace
https://devoas1.apps.th.gov.bc.ca/ogs-geoV06	GeoServer URL
name_space	namespace aka Workspace
LAYER_NAME	GeoServer feature type
SHAPE	SDO_GEOMETRY column
LAYER_NAME ID	Unique identifier
NON_SPATIAL_COLUMN	(optional) column update
EPSG:4326	Projection for coordinates

The expected response is

```

<?xml version="1.0" encoding="UTF-8"?>
<wfs:TransactionResponse xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:wfs="http://www.opengis.net/wfs"
xmlns:name_space="http://th.gov.bc.ca/name_space"
xmlns:gml="http://www.opengis.net/gml"
xmlns:ogc="http://www.opengis.net/ogc" xmlns:ows="http://www.opengis.net/ows"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.1.0"
xsi:schemaLocation="http://www.opengis.net/wfs
https://devoas1.apps.th.gov.bc.ca/ogs-geoV06/schemas/wfs/1.1.0/wfs.xsd">
  <wfs:TransactionSummary>
    <wfs:totalInserted>0</wfs:totalInserted>
    <wfs:totalUpdated>1</wfs:totalUpdated>
    <wfs:totalDeleted>0</wfs:totalDeleted>
  </wfs:TransactionSummary>
  <wfs:TransactionResults/>
  <wfs:InsertResults>
    <wfs:Feature>
      <ogc:FeatureId fid="none"/>
    </wfs:Feature>
  </wfs:InsertResults>
</wfs:TransactionResponse>

```

9.3 Delete a Record

Use the following request.xml

```
<wfs:Transaction service="WFS" version="1.2.0"
  xmlns:wfs="http://www.opengis.net/wfs"
  xmlns:ogc="http://www.opengis.net/ogc"
  xmlns:name_space="http://th.gov.bc.ca/name_space"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.opengis.net/wfs
http://schemas.opengis.net/wfs/1.0.0/WFS-transaction.xsd
http://th.gov.bc.ca/name_space https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/wfs/DescribeFeatureType?typename=name_space:LAYER_NAME">
  <wfs:Delete typeName="name_space:LAYER_NAME">
    <ogc:Filter>
      <ogc:PropertyIsEqualTo>
        <ogc:PropertyName>LAYER_NAME_ID</ogc:PropertyName>
        <ogc:Literal>dddd</ogc:Literal>
      </ogc:PropertyIsEqualTo>
    </ogc:Filter>
  </wfs:Delete>
</wfs:Transaction>
```

where

xmlns:name_space="http://th.gov.bc.ca/name_space"	URI of the namespace
https://devoas1.apps.th.gov.bc.ca/ogs-geoV06	GeoServer URL
name_space	namespace aka Workspace
LAYER_NAME	GeoServer feature type
LAYER_NAME_ID	Unique identifier

The expected response is:

```
<?xml version="1.0" encoding="UTF-8"?>
<wfs:TransactionResponse xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:wfs="http://www.opengis.net/wfs"
xmlns:name_space="http://th.gov.bc.ca/name_space"
xmlns:gml="http://www.opengis.net/gml" xmlns:ogc="http://www.opengis.net/ogc"
xmlns:ows="http://www.opengis.net/ows" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.1.0"
xsi:schemaLocation="http://www.opengis.net/wfs https://devoas1.apps.th.gov.bc.ca/ogs-
geoV06/schemas/wfs/1.1.0/wfs.xsd">
  <wfs:TransactionSummary>
    <wfs:totalInserted>0</wfs:totalInserted>
    <wfs:totalUpdated>0</wfs:totalUpdated>
    <wfs:totalDeleted>1</wfs:totalDeleted>
  </wfs:TransactionSummary>
  <wfs:TransactionResults/>
  <wfs:InsertResults>
    <wfs:Feature>
      <ogc:FeatureId fid="none"/>
    </wfs:Feature>
  </wfs:InsertResults>
</wfs:TransactionResponse>
```

Appendix 8 – ITS Availability

1 Introduction

The following material is excerpted from section 3 of MoTI Information Management Branch's (IMB's) internal 'Infrastructure Design Guide' document (V.04 last updated 2020-04-23) and tailored for relevance to ITS hosting infrastructure.

2 ITS Availability

MoTI's IMB will determine the appropriate hosting infrastructure architecture based on the values provided by the Designer for each of the following availability measures: Uptime, Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

For each of these measures, the options are listed in increasing level of complexity. Please note that the effort and cost between the options increases exponentially, i.e., 1b. may be twice as expensive as 1a., but 1c. may be 10 times as expensive. Higher availability also requires additional staff for infrastructure and software maintenance. The objectives below are considered worst-case targets, i.e., while the system may be offline for up to 12 hours per month, generally the system will be offline for a much shorter time (1-2 hours).

1. **Uptime:** The ITS will regularly be unavailable for system maintenance, e.g., installing patches and updates. How much time in a given month does the ITS need to be available to users?
 - a) 98.3% (up to 12 hours per month offline): This is the standard service level for single-instance environments, and sufficient for systems that are only used during business hours. It can be improved through server load balancing and database mirroring.
 - b) 99% (up to 7 hours per month offline)
 - c) 99.9% (up to 43 minutes per month offline)
 - d) 99.99% (up to 4 minutes per month offline)

2. **RTO (Recovery Time Objective):** How long can system recovery take in the event of a disaster (i.e., the wide area network or the micro-data center becomes unavailable)?
 - a) Up to 8 weeks: This is the standard service level for the Ministry. Recovery would include procuring new servers, setting up the environment in an alternate location, and restoring data.
 - b) Up to 2 weeks: In this case, we pro-actively provision an off-site cold-standby environment which can be brought online and configured to support operations in the event of a disaster.
 - c) Up to 24 hours: This requires a separate failover (hot stand-by) environment which is continuously kept up-to-date and available.

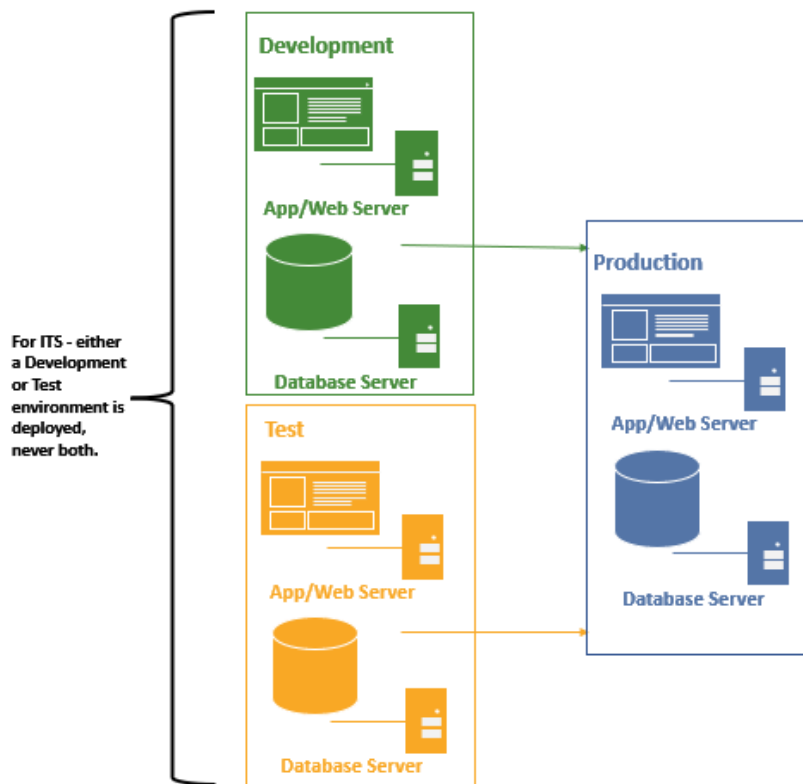
3. **RPO (Recovery Point Objective):** How old can the data be in event of a disaster (i.e., the wide area network or the micro-data center becomes unavailable)? Data that is older than the stated objective may be lost forever.
- Up to 48 hours: This is the standard service level for the Ministry.
 - Up to 24 hours
 - Up to 1 hour
 - Up to 5 minutes

2.1 Example 1

This example satisfies the following availability requirements:

- Uptime: 98.3% (up to 12 hours per month offline)
- RTO: up to 8 weeks
- RPO: Up to 48 hours

Please note that some servers (e.g., database servers) may be shared with other ITS. This decision is made at the discretion of MoTI IMB's Infrastructure Lead based on the technical hosting requirements of the ITS.

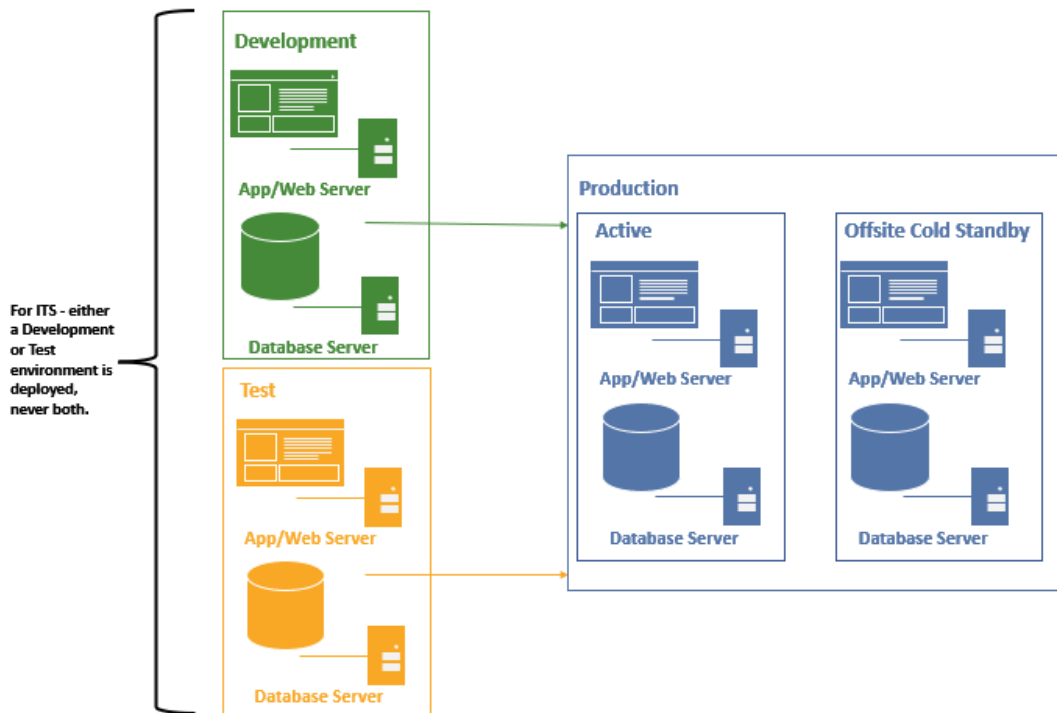


2.2 Example 2

This example satisfies the following availability requirements:

- Uptime: 99% (up to 7 hours per month offline)
- RTO: up to 2 weeks
- RPO: Up to 24 hours

Please note that some servers (e.g., database servers) may be shared with other ITS. This decision is made at the discretion of MoTI IMB's Infrastructure Lead based on the technical hosting requirements of the ITS.

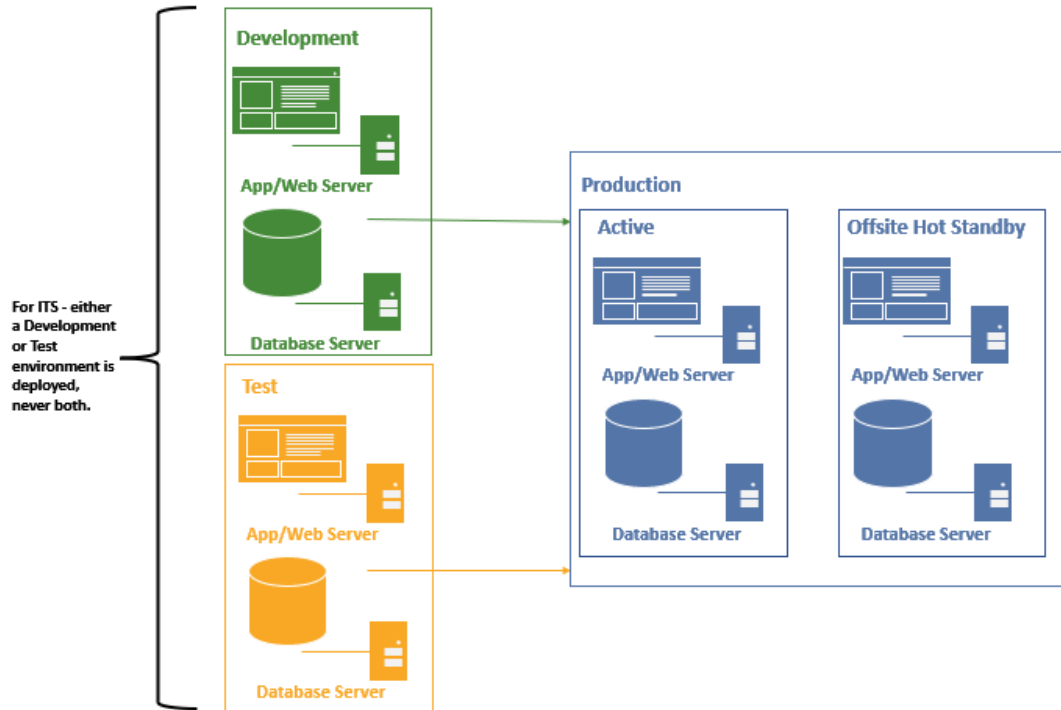


2.3 Example 3

This example satisfies the following availability requirements:

- Uptime: 99.9% (up to 43 minutes per month offline)
- RTO: up to 24 hours
- RPO: Up to 1 hour

Please note that some servers (e.g., database servers) may be shared with other ITS. This decision is made at the discretion of MoTI IMB's Infrastructure Lead based on the technical hosting requirements of the ITS.





Critical Systems Standard

Enterprise Design Services
Office of the CIO, Province of BC

Document Version: 3.0
Published: July 2019

1	DOCUMENT CONTROL	3
2	INTRODUCTION	4
3	PURPOSE	4
4	CONVENTIONS USED	4
4.1	SUPPORTING GUIDELINES	4
5	DEFINITIONS	5
5.1	MISSION CRITICAL FUNCTION	5
5.2	CRITICAL SYSTEM	5
5.3	MUST	5
5.4	SHOULD	5
6	ROLES	5
6.1	BUSINESS OWNER	5
6.2	SYSTEM OWNER	6
6.3	RESPONSE AND RECOVERY DIRECTOR	6
6.4	MINISTRY CRITICAL SYSTEMS COORDINATOR	7
6.5	OCIO CRITICAL SYSTEMS COORDINATOR	7
7	REGISTRATION	7
8	SYSTEM DESIGN AND SUPPORT DOCUMENTATION	7
9	SYSTEMS MANAGEMENT	8
9.1	NEW APPLICATION COMPLIANCE	8
9.2	CHANGE MANAGEMENT	8
9.3	PERFORMANCE BASELINE, MONITORING AND ALERTING	8
9.4	CAPACITY PLANNING	8
9.5	SERVICE PROVIDER SUPPORT MANAGEMENT	8
9.6	INCIDENT MANAGEMENT	8
9.7	DISASTER RECOVERY PLAN	8
10	IMPLEMENTATION	9
10.1	EFFECTIVE DATE	9
10.2	NON-COMPLIANCE	9
10.3	ANNUAL REVIEW	9

1 Document Control

Date	Author	Version	Change Reference
March, 2015	Derek Rutherford, Tim Gagne	1.0	Version 1
March, 2017	Scott Johnson	2.0	Extend scope to include new and changed systems
June 2019	Stuart Cayzer, Ruonan Lou, Scott Johnson	3.0	Increase focus on Mission Critical systems

2 Introduction

This new and improved Critical Systems Standard now aligns fully with our Core Policy and Procedures Manual, Chapter 16 (Business Continuity Management) by focusing on Mission Critical Systems, which are those required for the delivery of Mission Critical Business Functions.

As the IM and IT operating environment continues to increase in scale, complexity, and dependencies, the risk of disruptions to business services is higher. The effect of a loss of a mission critical service on individuals can bring hardship, and in some cases result in injury or even death. Note also that government is increasing its reliance on service providers (internal to government as well as external contractors). This increased complexity demands higher levels of vigilance in our security posture and improved coordination to be successful in delivering stable services to citizens.

Lessons learned from recent service interruptions in government have pointed to ways of improving how we recognize and more effectively deal with these kinds of disruptions. This standard addresses the immediate concerns from lessons we have recently learned and also lays the foundations for a program of continuous improvement.

3 Purpose

The purpose of this standard is to:

- Define a critical system;
- Identify key roles and responsibilities;
- Minimize the impact of a disruption to a critical system;
- Restore normal business operations as soon as possible; and
- Maintain the security of information systems and communications technologies, and the availability of supporting infrastructure and services.

4 Conventions used

Terms used that are written in all upper case are defined within this Standard e.g. BUSINESS OWNER is a role that is defined in section 6 Roles.

4.1 Supporting Guidelines

This standard is designed to be read in conjunction with the *Critical Systems' Guidelines* published [here](#). The guidelines describe proposed approaches that could meet the minimum requirements under this standard.

5 Definitions

5.1 Mission Critical Function

Defined in Core Policy, Chapter 16, and included here for ease of reference - Mission Critical functions are those that, should they not be performed, could lead to:

- Failure in meeting the legislated Emergency Program Act or any other Act
- Loss of life and/or safety
- Personal hardship to citizens
- Major damage to the environment
- Significant loss in revenue and/or assets.

5.2 Critical System

Any IM/IT service, system, or infrastructure component that is deemed necessary by the SYSTEM OWNER to deliver a MISSION CRITICAL FUNCTION, is a critical system for the purposes of this standard. The use of the word system is intended to have broad applicability and can include hardware and software implemented in numerous configurations i.e. on premise, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) whether operated under the direct control of government staff or through an outsourced service provider.

5.3 Must

The term "MUST" (when written in all upper case) is defined as an absolute requirement of this Standard.

5.4 Should

The term "SHOULD" (when written in all upper case) means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications MUST be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the Government Chief Information Officer (GCIO).

6 Roles

6.1 Business Owner

The BUSINESS OWNER MUST ensure that a Business Impact Analysis (BIA) is completed for each business unit or program area, as specified in Core Policy, Chapter 16.

The BIA MUST be reviewed and updated annually, as well as when changes to business operations and processes, organizational structure, critical dependencies or resources occur. Ministries are responsible for identifying and implementing operational triggers to ensure the BIA is current.

The BIA determines which business functions are Mission Critical.

6.2 System Owner

For all functions that have been deemed Mission Critical, the SYSTEM OWNER MUST identify all IM/IT services, systems, or infrastructure components that are necessary for the delivery of the Mission Critical function. These IM/IT services, systems, or infrastructure components MUST be declared as critical systems.

The SYSTEM OWNER role is accountable for the overall state of the system and MUST be authorized to allocate resources as appropriate to meet the obligations under this standard.

A *Critical System* MUST have a SYSTEM OWNER role assigned.

The SYSTEM OWNER MUST ensure that all critical systems for which they are accountable have:

- An up-to-date Security Threat and Risk Assessment (STRA);
- All roles required by this standard assigned, and will continue to be maintained;
- All system and contact details registered, and will be maintained in collaboration with the OCIO coordinator;
- System design documentation that is complete, accurate, up to date, and has a process in place to maintain currency and accuracy;
- A change management process;
- Performance monitoring and capacity planning baselines established and actively maintained, managed and monitored;
- A Major Incident Response and Recovery process, defined, maintained and tested at least annually;
- A Disaster and Recovery Plan defined, maintained and tested.
- Capacity Planning
- Service Provider Support Management

6.3 Response and Recovery Director

The RESPONSE AND RECOVERY DIRECTOR role defines the major incident response and recovery process and is responsible to manage, direct, and lead the actions of incident response and recovery for issues affecting normal business operating performance and availability as described in the *Critical Systems' Guidelines*.

A *Critical System* MUST have a RESPONSE AND RECOVERY DIRECTOR role and their alternate assigned.

The named Response and Recovery Director MUST have the authority to convene the necessary resources as required.

6.4 Ministry Critical Systems Coordinator

The MINISTRY CRITICAL SYSTEMS COORDINATOR role is the single point of administrative contact pertaining to the obligations under this standard.

Each Ministry **MUST** have a MINISTRY CRITICAL SYSTEMS COORDINATOR role assigned.

This coordinator will register each critical system with the OCIO CRITICAL SYSTEMS COORDINATOR

6.5 OCIO Critical Systems Coordinator

The OCIO CRITICAL SYSTEMS COORDINATOR role is the single point of administrative contact for all information flows between OCIO and MINISTRY CRITICAL SYSTEMS COORDINATORS.

The OCIO **MUST** have a CRITICAL SYSTEMS COORDINATOR role assigned.

The OCIO CRITICAL SYSTEMS COORDINATOR role **MUST**

maintain a register of all critical systems and

provide a quarterly report on the effectiveness of efforts made in the prior period towards achieving compliance, to:

- Ministry Chief Information Officers; and
- OCIO's CTO and ADM, Enterprise Services.

7 Registration

The OCIO CRITICAL SYSTEMS COORDINATOR **MUST** maintain a register of all critical systems.

MINISTRY CRITICAL SYSTEMS COORDINATORS **MUST** register each critical system with the OCIO CRITICAL SYSTEMS COORDINATOR. A registration **MUST** be completed in accordance with the guidance contained in the *Critical Systems' Guidelines*.

8 System Design and Support Documentation

For each critical system the SYSTEM OWNER **MUST** create and maintain as current, accurate and available, documentation for the *Critical Systems'* application; computing, data and network platform that **SHOULD** contain at minimum the elements as described in the *Critical Systems' Guidelines*.

9 Systems Management

9.1 New Application Compliance

All new systems developed or acquired, must be evaluated against the definition of a Critical System. Any new application whose BUSINESS OWNER determines that it will be a Critical System MUST ensure it is designed and built in compliance with the *Critical Systems Standard* prior to release into a production environment.

9.2 Change Management

The SYSTEM OWNER MUST ensure a process is in place that governs changes to a system and SHOULD ensure that such a change process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

9.3 Performance Baseline, Monitoring and Alerting

The SYSTEM OWNER MUST ensure a process is in place to manage system performance and SHOULD ensure that such a system performance process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

9.4 Capacity Planning

For each critical system the SYSTEM OWNER MUST ensure a process is in place to proactively manage system resource utilization and SHOULD review historical performance information to determine if any action is required.

9.5 Service Provider Support Management

For each critical system the SYSTEM OWNER MUST ensure a process is in place to proactively manage providers of services necessary to deliver the system and SHOULD ensure that such a service provider process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

9.6 Incident Management

The SYSTEM OWNER MUST ensure a process is in place to be able to recognize and recover from an incident that could impact business service availability and SHOULD ensure that such an incident management process, at minimum, meets the requirements outlined in the *Critical Systems' Guidelines*.

The SYSTEM OWNER MUST ensure that their organization has a defined incident management process. The incident management process SHOULD be repeatable and MUST be exercised prior to implementation of any new critical systems and at minimum annually thereafter, in accordance with the requirements outlined in the *Critical Systems' Guidelines*.

9.7 Disaster Recovery Plan

The SYSTEM OWNER MUST ensure that a tested Disaster Recovery Plan and skilled resources are in place to be able to recover from a disruptive event that has an unacceptable impact to a business service, and MUST ensure that such a disaster recovery processes, at minimum, meet the requirements outlined in the *Critical Systems' Guidelines*.

10 Implementation

10.1 Effective Date

This Standard is effective as of April 1, 2016.

10.2 Non-compliance

If a SYSTEM OWNER is unable to attest to compliance by the effective date, the SYSTEM OWNER (or delegate) MUST submit for endorsement a compliance assessment and roadmap as scheduled in the *Critical Systems' Guidelines*.

10.3 Annual Review

On each anniversary of the endorsement of their compliance roadmap, and on or before each target date from compliance, the SYSTEM OWNER MUST report the progress against the roadmap, any proposed revisions and an updated compliance assessment as described in the *Critical Systems' Guidelines*.

Critical Systems Guidelines

Enterprise Design Services Branch
Office of the Chief Information Officer
Province of British Columbia

Document Version 3.0

July, 2019

Table of Contents

1.0	Document Control	3
2.0	Introduction	4
3.0	Roles and Responsibilities	4
4.0	Critical System Registration	4
5.0	System Design and Support Documentation	5
5.1	Validity	5
5.2	Accurate and Current	6
5.3	Accessible	6
6.0	Systems Management	6
6.1	Change Management Process	6
6.2	Performance Baseline, Monitoring and Alerting	6
6.3	Service Provider Support Management Requirements.....	7
6.4	Incident Management Requirements	7
6.4.1	Defining the Major Incident Management Process	8
6.4.2	Convening the Team	8
6.4.3	Leading the Response and Recovery	8
6.5	Disaster Recovery Plan	9
6.6	Exercising Incident Management and Disaster Recovery.....	9
7.0	Compliance Assessment and Declaration	9
7.1	If declaring: 'No'	9
7.2	If declaring: 'Yes'	9
7.3	Independent Review and Attestation.....	9
Appendix A: Compliance Checklist		10

1.0 Document Control

Date	Author	Version	Change Reference
April, 2015	Tim Gagne	1.0	Initial version
December, 2015	Tim Gagne	1.1	Updates to Section 7 Compliance Attestation and Roadmap
January, 2016	Diana Rai	1.2	Linked Ministry Staff to their Ministry Critical Systems Coordinators
March, 2016	Scott Johnson	1.3	Updated 7.0, 7.1 and added 7.2
July, 2019	Stuart Cayzer, Theresa Parkin	3.0	Add Compliance Checklist, and synchronize versioning with the Critical Systems Standard

2.0 Introduction

These guidelines form part of the Critical Systems Standard Framework and are to be read in conjunction with the Critical Systems Standard (the Standard).

The following sections describe proposed approaches, actions, and documentation to meet the minimum requirements and obligations outlined under the Standard by:

- Aiding in the interpretation of the Standard, and,
- Outlining the minimum expectation of the specific requirements defined in the Standard.

3.0 Roles and Responsibilities

Current roles identified in support of the Standard include:

1. Business Owner;
2. System Owner;
3. Response and Recovery Director (and alternate);
4. Ministry Coordinator, Critical Systems Standard;
5. OCIO Coordinator, Critical Systems Standard.

The responsibilities for each of these roles are described fully in the Standard.

Recommendations on the assignment of the supporting roles:

- MCIO collaborate with Business Owners to appoint a single Ministry Critical Systems Coordinator (and, ideally, an alternate);
- MCIO collaborate with Business Owners to appoint, for each critical system, a Response and Recovery Director and alternate.

4.0 Critical System Registration

OCIO will maintain a Critical Systems Registry, as a single source of truth, identifying all registered critical systems.

The Ministry Critical Systems Coordinator is required to provide their contact details to the OCIO Critical Systems Coordinator, and maintain accurate information on their ministry's critical systems at all times, as follows:

- System name and business function description
- Name and contact details for:
 - Ministry Critical Systems Coordinator;
 - Business Owner;
 - System Owner;
 - System Response and Recovery Director;
 - System Response and Recovery Director alternate.

- Target Date for Compliance

5.0 System Design and Support Documentation

Each critical system's support documentation must describe:

- Designs incorporating business, system, technical and over-arching security;
- Corporate Infrastructure Services (e.g. identity management, payment, ..);
- The application platform;
- Communications infrastructure;
- Application platform interface;
- Communications infrastructure interface;
- Special qualities (e.g. security, application management, etc.);
- Physical components making up the system;
- The logical relationships/data and process flows;
- Each business process that is supported or potentially impacted by the system.
- For each software product:
 - Software title
 - Software version
 - Software functional description
 - Software vendor
 - SLA reference if applicable;
- For each hardware product:
 - Hardware component name
 - Hardware functional description
 - Hardware operating system version if applicable
 - Hardware vendor
 - SLA reference if applicable.

5.1 Validity

To keep support documents valid, it is recommended that at least the following control information is present in each document:

- Current document owner, and their organization;
- Update history, author, and author's organization;
- Last reviewed date, and who reviewed;
- Next Review Date.

5.2 Accurate and Current

A process should be put in place to ensure that support documents are annually reviewed and signed off as accurate and current.

5.3 Accessible

A copy of all support documents should be stored in a single location that is available to the team members and essential service support partners.

6.0 Systems Management

Above and beyond normal service desk or operation functions, the following requirements should apply in overseeing the health of a critical system.

6.1 Change Management Process

A procedure should be established to review and approve all proposed changes.

Change requests should include the following information:

- change requestor, approval chain;
- component(s) being changed;
- changes to be performed (include documented MOP - method of procedures);
- start time, end time, duration.

Change Management processes should also:

- Be performed initially on a test system that is reflective of the production environment;
- Be performed in identified production change windows;
- Log all changes and maintain history;
- For changes that require extra-ordinary services from OCIO or would benefit with a restriction on changes to infrastructure services or other dependent systems: coordinate with OCIO change management function - refer to [Request for Special Processing \(RSP\)](#) for engagement instructions;
- Update System Design and Support documentation following changes;
- Update problem log and close appropriate problems addressed in each change;
- Include internal event logging to support determination of who did what and when they did it.

6.2 Performance Baseline, Monitoring and Alerting

Understand what normal is:

- establish and record baseline metrics for normal business operating performance and availability;
- Establish performance and availability impact tolerance thresholds;
- Continuously monitor actual performance and keep history for trend analysis and capacity planning;
- Raise alerts pro-actively, and independent of user experiences and calls, when impact tolerance threshold is experienced.

6.3 Service Provider Support Management Requirements

The System Owner should ensure support agreements are in place for critical systems:

- Days of week and hours of service;
- Level of expertise expected;
- On-site requirement.

Service partner support specialists will rely on the support documentation to effectively assist in major incident response and recovery. To ensure effectiveness the System Owner should provide service partners the opportunity to attest that design support documents are complete and meaningful and current configuration or use of their services is supportable.

Unsupported configurations must be identified in a risk management plan along with mitigation strategy.

If there's privacy or exceptional security surrounding any system data, a process should be put in place that reviews and approves access.

6.4 Incident Management Requirements

Maintain the capability to recognize an incident that could impact availability of a critical system, by ensuring:

- Escalation of a major incident is clearly defined by the Response and Recovery Director;
- There is a single point of contact (help desk, an email inbox or a phone number) for users to raise incidents with the critical system and the hours of service match the criticality of the business function (e.g. if service is until 8pm, then single point of contact should be offered until 8pm);
- All incidents are recorded and history is maintained;
- Trouble tickets are generated, severity assigned, and alerts sent to designated support personnel;

- Incidents are reviewed daily, and action is taken to address any trends identified (problem management).

6.4.1 Defining the Major Incident Management Process

The Response and Recovery Director must define and maintain a process to respond to a major incident that is impacting business service performance or availability.

This process should at minimum:

- Define the Response and Recovery Team roles and responsibilities matrix;
- Assign primary and alternate names to the roles;
- Define the procedure to escalate a major incident, through the help or service desk, to the Recovery and Response Director;
- Establish authority to convene immediately the appropriate Response and Recovery Team members;
- Include a communications plan (channels, medium, timing, etc.) for all stakeholders who need to know the status of the response or recovery;
- Document procedures for handling vital documents generated during the response and recovery effort;
- Document procedures to ensure the names in the Response and Recovery Team file are up to date.

6.4.2 Convening the Team

Members of the response and recovery team must be capable of meeting the responsibilities defined in the roles and responsibilities matrix.

Training and succession plans should be identified by the Response and Recovery Director and committed to by the System Owner.

Where internal capabilities do not exist, the Response and Recovery Director should ensure that appropriate support agreements and funding are in place with service support partners.

6.4.3 Leading the Response and Recovery

Upon receiving an escalation of an incident to a major incident (as defined above), the Response and Recovery Director should lead the actions of the team and be the primary liaison with executives:

- Convene team members and communicate to their supervisors;
- Validate the impact is real;
- Execute the communications plan;
- Direct the actions from problem analysis to resolution;

- Lead recovery if required as documented in the Disaster Recovery Plan;
- Lead review of any process issues and identify lessons learned;
- Continuously improve the process.

6.5 Disaster Recovery Plan

The System Owner should ensure that a Disaster Recovery Plan exists, it has been tested within the past 12 months, and has been approved by the Business Owner.

6.6 Exercising Incident Management and Disaster Recovery

To ensure readiness, the Major Incident Management Process and Disaster Recovery Plan should be exercised before production implementation for new systems, and annually for existing systems.

7.0 Compliance Assessment and Declaration

As mentioned previously, it is the responsibility of the Ministry Critical Systems Coordinator to enter, and maintain, accurate information on the ministry's Critical Systems, in the Critical Systems Registry.

7.1 If declaring: 'No'

Enter your target date for compliance.

7.2 If declaring: 'Yes'

Notify the OCIO Critical Systems Coordinator, update the Critical Systems Registry to indicate that the system is compliant, and ensure that the target date for compliance is set to the date on which compliance was achieved (this will set the 1-year deadline for review to ensure ongoing compliance).

7.3 Independent Review and Attestation

The adequacy of controls must be verified by recent, rigorous independent review.

Rigorous, for the purpose of the Standard, means the reviewer must see evidence that the control is being met.

Independent means that the review should be done by someone not in the chain of system ownership or support. Cannot be the System Owner's Ministry Information Security Officer (MISO) - another ministry's MISO is acceptable.

Appendix A: Compliance Checklist

Ministry:	Critical System Name (as registered):
Reviewed by: <Print Name Here>	Review Date <dd-mmm-yyyy>:
Reviewer's Signature:	

System Owner: <Print Name Here>	Date <dd-mmm-yyyy> signed:
Signature:	

Business (Program) Owner: <Print Name Here>	Date <dd-mmm-yyyy> signed:
Signature:	

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
UP-TO-DATE STRA The SYSTEM OWNER MUST ensure that this system has an up-to-date STRA.			
Describe how you meet the requirement.			
Tell me/show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
CRITICAL SYSTEM REGISTRATION: The required information has been registered with the OCIO and the named persons are aware of their roles and responsibilities and feel capable of doing so: Click here for the full list.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

SYSTEM DESIGN AND SUPPORT DOCUMENTATION All required elements are available. Click here for the full list.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

SYSTEM DESIGN AND SUPPORT DOCUMENTATION VALIDITY: Required control information provided in each document. Click here for the full list.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
SYSTEM DESIGN AND SUPPORT DOCUMENTATION CURRENT and ACCURATE: Support documents are reviewed and signed off annually as accurate and current.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

SYSTEM DESIGN AND SUPPORT DOCUMENTATION ACCESSIBLE: Support documentation accessible to all supporting roles.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

CHANGE MANAGEMENT PROCESS: Process in place, and meets requirements. Click here for the full list.			
Describe how you have met the requirement.			
Tell /show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
PERFORMANCE BASELINE, MONITORING AND ALERTING: Process in place, and meets requirements. Click here for the full list.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			
CAPACITY PLANNING: Process in place, and meets requirements.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			
SERVICE PROVIDER SUPPORT MANAGEMENT: Process in place, and meets requirements. Click here for the full list.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
INCIDENT MANAGEMENT: Process in place, and meets requirements. Click here for the full list.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

MAJOR INCIDENT MANAGEMENT: Process in place, and meets requirements. • Click here for the full list.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

CONVENING THE TEAM Terms of Reference in place, and meets requirements. Click here for the full list.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
DISASTER RECOVERY PLAN:			

Controls	Evidence Good Y/N	Comments/Gaps	Compliance Target Date <dd-mmm-yyyy>
Plan in place, tested annually, and meets requirements. Click here for the full list.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

RESPONSE AND RECOVERY EXERCISED: Plan in place, tested annually, and meets requirements.			
Describe how you are meeting the requirement.			
Tell me/show me where I can find the supporting evidence.			

Appendix 11 – Hosted Environments

Table of Contents

1	Introduction	1
1.1	Ministry Hosted Environments for Custom Development	1
1.1.1	Environment Description(s)	1
1.1.2	Environment Indicators	2
1.2	Ministry Hosted Environments for Commercial Off The Shelf Software	4
1.3	Hosting Infrastructure Responsibilities	5

1 Introduction

The following material is excerpted (and tailored for relevance to ITS IM/IT hosted components) from section 2 of the internal **IMB Infrastructure Design Guide** document (V.04 last updated 2020-04-23). It is included to describe traditional IM/IT hosted environments that can be considered and delivered in support of a Ministry ITS.

1.1 Ministry Hosted Environments for Custom Development

1.1.1 Environment Description(s)

Environment: Training (Optional)

Short form: TRN

Description: This environment is used to conduct end user training. It is designed to assist employees in gaining the skills they need to perform work-related tasks. It is used for educational purposes and therefore should simulate the PRD environment. The infrastructure may be shared with DEV or TST if there is no impact on DEV or TST.

Environment: Development

Short form: DEV

Description: In this environment, the development team has full access to configure and customize ITS software. Developers deploy and debug code and conduct unit tests in this environment. Interfaces with other systems, data conversion scripts and reports are also deployed, configured, and customized if necessary in this environment.

Environment: Test

Short form: TST

Description: This environment is managed by the Ministry with support from and in collaboration with the ITS software vendor. All types of testing are executed in this environment (integration, functional, regression etc.) except for User Acceptance Testing (UAT). This environment is also used to ensure design models have been adhered to. This environment must have the appropriate test data in the data system to cover all test cases. Developers deliver code, database changes, scripts etc. to this

environment. Any Personally Identifying Information (PII) or Sensitive Personal Information (SPI) needs to be anonymized in this environment.

Environment: Pre-Production (Optional)

Short form: PRE

Description: Pre-Production is an exact duplicate of production, including data. This environment is used to achieve as little downtime as possible and is typically used for systems that have high availability requirements. You can release to PRE first, verify (preferably executing automated tests) and then switch PRE and PRD, then PRE becomes PRD and the cycle continues. When done right, the downtime during a deployment is negligible. It must be separated from DEV, or TST but parts of the infrastructure may be shared with PRD. This environment may be used for disaster recovery.

Pre-production is managed by the Ministry with support from the ITS software vendor as defined and detailed in a support and maintenance agreement for the ITS. In cases where a support and maintenance agreement requires that an ITS software vendor has privileged access to the environment, the vendor must adhere to the Ministry's respective privileged access policies and procedures.

Environment: Production

Short form: PRD

Description: Production is owned by the organization. Production is the live site, the services and information are exposed to external users. This infrastructure is completely separate from all other environments.

Production is managed by the Ministry with support from the ITS software vendor as defined and detailed in a support and maintenance agreement for the ITS. In cases where a support and maintenance agreement requires that an ITS software vendor has privileged access to the environment, the vendor must adhere to the Ministry's respective privileged access policies and procedures.

1.1.2 Environment Indicators

Distinguishing each environment on the UI using the corresponding color schema for menu ribbon:

Environment	HTML Color Code for Menu ¹
Development	Green (#448a38)
Test	Yellow (#f9a825)
Pre-production/Training/	Red (#8a3844)
Production	BC Gov Blue ²

¹ The active/selected menu item color is about 10% lighter than the main color. Using sass the active color is generated with the `lighten ($main-nav-color, 10%)` function.

² Depends on your template. Many projects are using the standard BCGov Bootstrap template found at <https://bcgov.github.io/bootstrap-theme/docs/reference/simple/>

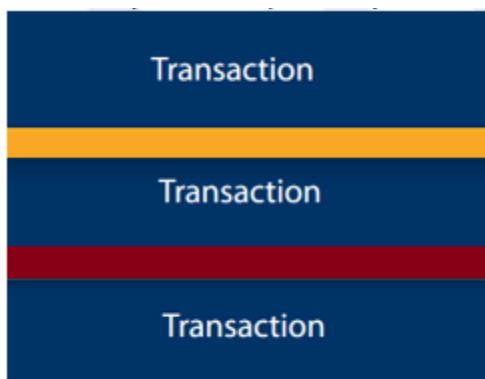
Environment	HTML Color Code for Menu ¹
Failover(s)	<i>Same as the corresponding environment</i>

- The examples of the above implementation could be seen in the following applications – HETS, School bus and HMCR
See example below (from top to bottom, same order as the table)



- In the event the menu is not separated from the application heading, add a colored ribbon in the non-production environments to distinguish them (example: Transaction)

See example below (from top to bottom – TST, PRE, PRD)



1.2 Ministry Hosted Environments for Commercial Off The Shelf Software

The Ministry will provide all hosting infrastructure and services for the selected ITS solution.

Available server configurations range from a 1-core, 4GB RAM virtual machine to a 32-core, 256GB RAM dedicated server; storage area network (SAN) storage is available in various speed and resiliency levels in 50GB increments. Physical access to the hosting facilities is restricted to individuals that are under contract to the Ministry or the B.C. Government to service these facilities and the physical hosting infrastructure supported therein. Remote access to file shares and databases can be accommodated via Virtual Private Networks as required to enable ITS software vendors to meet their contractual obligations to the Ministry.

Custom hardware components (e.g., hardware acceleration cards) can be accommodated, if the vendor can clearly demonstrate why the available hardware is not sufficient. Depending on the specific technologies chosen, the product may be partially or fully hosted on a shared server. To facilitate operation within this environment, the vendor should provide the following information:

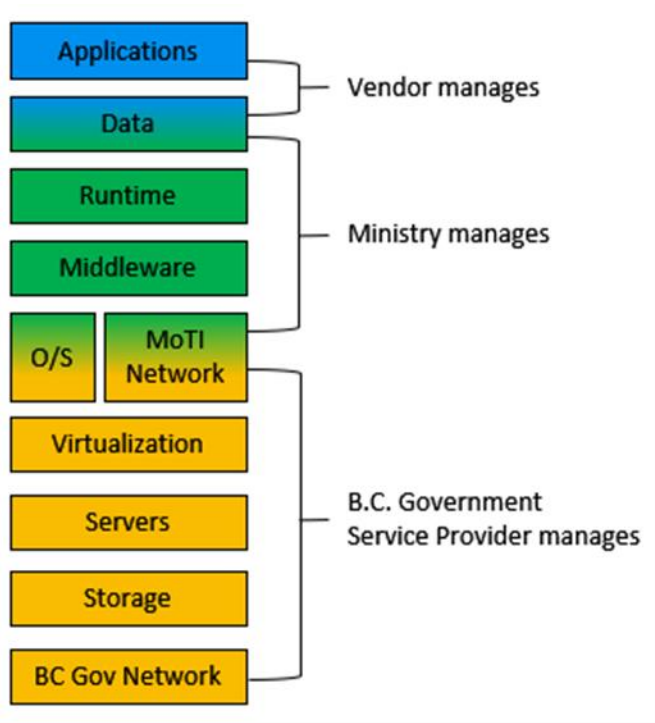
- a) CPU, RAM, disk space, disk I/O, network bandwidth, and IP address requirements.
- b) Storage requirements for all application servers and databases proposed.
- c) An architecture diagram with network communication requirements. The Ministry will set up firewall rules based on this deliverable. Firewall changes may require up to 2 weeks of lead time.
- d) Whether the application supports an inbound proxy in front of the application server.

To ensure sufficient resources are available to operate the future system, proposals should provide a detailed, itemized list of the required infrastructure.

The vendor should propose a solution that is designed to meet the availability requirements identified in the RFP. If the application is expected to remain online during standard maintenance, such as operating system patching, the vendor should suggest an architecture that can accommodate single server outages without affecting application availability. Outages caused by the Ministry-provided infrastructure will not count against application uptime, however the application should be resilient enough to recover automatically in most scenarios once the infrastructure becomes available again, such as after a brief network outage.

As Ministry staff will be responsible for deploying the application in all environments, the vendor will be required to supply a deployment guide when the application is delivered. Please see section 1.1 for environment definitions.

1.3 Hosting Infrastructure Responsibilities





Office of the Chief
Information Officer

ENTERPRISE IT SECURITY ARCHITECTURE SECURITY ZONES: NETWORK SECURITY ZONE STANDARDS

Architecture, Standards and Planning Branch

Office of the CIO ● Province of BC

People ● Collaboration ● Innovation

Version 2.0

July 20, 2012



Table of Contents

1	Foreword.....	1
2	Introduction	1
2.1	Classification.....	1
3	Scope	1
4	Normative references.....	2
5	Terms and Definitions	2
6	Requirements.....	4
7	General characteristics.....	4
7.1	Enterprise Security Model.....	4
7.1.1	Overview of Network Security Zones	5
7.1.2	Summary.....	6
7.2	Detailed Characteristics and Standard.....	7
7.2.1	Zone Constructs	7
7.2.2	Standard Elements	8
7.2.3	Inter-zone Connectivity	10
7.2.4	Intra-zone Connectivity	11
7.2.5	Enforcement.....	12
8	Evaluation criteria.....	13
8.1	Enquiry Scope	13
9	References	14
Annex A.	Standard for Network Security Zones.....	14



Date	Author	Version	Change Reference
10/25/2011	Christopher Lyons	3.0	Draft for ASRB review
11/08/2011	Christopher Lyons	3.1	Changes proposed by Ronald Warden
12/15/2011	Christopher Lyons	3.1	Removal of vendor references as per Malcolm McGregor.
12/23/2011	Christopher Lyons	3.1	Changes proposed by ISB
1/9/2012	Christopher Lyons	3.1	Changes proposed by David Steffy
1/12/2012	Christopher Lyons	3.1	Formatting
2/6/2012	Christopher Lyons	3.2	Replaced figure 2 diagram
2/15/2012	Christopher Lyons	3.2	Updated IP or port from zone B to Internet
4/25/2012	Christopher Lyons	3.3	Removed access from Zone B to Internet and B to SPAN
4/27/2012	Christopher Lyons	3.3	Updated Introduction
7/17/2012	Christopher Lyons	4.0	Minor updates throughout
9/25/2012	Christopher Lyons	4.1	Updated to include cases for zone B to Internet and update terms.
10/02/2012	Christopher Lyons	4.1	Modified Zone C to be only trusted device & trusted user

1 Foreword

Between 2005 and 2007 considerable work was conducted to develop an Enterprise IT Security Architecture (EITSA) as part of the Security Enhancement Project (SEP). The architectures described in the draft documentation were not considered mandatory for core government, and the EITSA was not formally published. The broad architectures described in the EITSA serve as the foundation of this standard, and also served as the mandatory security architecture for the SSBC Managed Services Environment with the STMS datacenter design. The EITSA was not published and therefore is not a publicly available document.

The Government of BC has traditionally invested heavily in perimeter security where firewalls and Intrusion Prevention Systems have been intended to provide the bulk of Government's data protection. Government collaboration with external partners has been carefully funnelled through 3rd Party Gateways with extensive security controls. The EITSA was written with the goal of moving Government towards a Defense In Depth posture where many layers of defense from the perimeter right down to the data encryption all play a role in protecting the enterprise Information Assets.

2 Introduction

This standard recommends dividing or segmenting the enterprise network into secure network segments or "Security Zones" as an important step in creating a secure layered network infrastructure that is consistent with moving security controls closer to the data that they are intended to protect.

The boundary controls employed to create and secure these zones and other associated network security services are included in this standard. The Zone model is consistent with the best practises of Defense in Depth.

In addition to the Network Security Zones standard, host-based firewalls, encryption, secure data protocols, data loss prevention, and data-level authentication are also considered critical to a long term successful information security strategy.

The main body of this document contains informative descriptions that support the implementation of this standard.

2.1 Classification

The proposed standard is classified as follows:

Table 1

Standard	Type	Nature	Review	Scope
Network Security Zones	Technical	Tactical	Annual	Enterprise IP networks, including those provided by ASD partners.

3 Scope

This document applies to government. It:



1. Specifies standard for the Network Security Zones; and
2. To the entire Government of BC enterprise network, including services delivered by ASD partners.

This document does not apply to:

1. Private and public entities which are not directly under the control or governance of the Government of BC; and
2. Existing legacy mainframe; and
3. Services that are provided by third parties and delivered across the Internet (public cloud services).

4 Normative references

International Standards

- ISO 27002:2005

OCIO IM/IT Standards Manual

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf

- Cryptographic Standards for Information Protection (section 6.10)
- Interim Standards for Information Systems Security and Network Connectivity (section 6.4)
- Standard for Information STRA Methodology, Process and Assessment tool (section 6.11)
- Physical Security Technical Standards
- Web Content Filtering (sections 1.1, 6.2 and 6.3)

Information Security Policy <http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf>

- Information Security Classification Framework

Information Management Standards

http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

- Ministries must ensure all government technology and information is managed in line with Government Core Policy Manual Chapter 12 Information Management and Information Technology Management,.

5 Terms and Definitions

For the purposes of this document, following acronyms apply.



Table 2

Acronym		Comments
ACL	Access Control List	
DLP	Data Loss Prevention	
DMZ	Demilitarized Zone	
EITSA	Enterprise Information Technology Security Architecture	
FQDN	Fully Qualified Domain Name	
IPS	Intrusion Prevention System	
ISCF	Information Security Classification Framework	
MPLS	Multi-protocol Label Switching	
NAT	Network Address Translation	
SAG	Secure Access Gateway	
SPI	Stateful Packet Inspection	
STRA	Security Threat Risk Assessment	
VLAN	Virtual Local Area Network	
VPN	Virtual Private Network	
VRF	Virtual Routing and Forwarding	
	Firewall Rules	A system of security rules that control by blocking or allowing communication between trusted and untrusted network segments or hosts.
	Information Asset	Any data created, processed and used by the Government of BC.
	Network Security Zone	A physically or logically isolated network consisting of network interfaces with similar security requirements or profiles.



6 Requirements

1. Information Assets classified in accordance with ISCF will determine the appropriate level of security measures needed to protect the asset.
2. Information Assets are periodically monitored to determine the effectiveness of the measures and controls in place with particular focus on those assets deemed High Security.
3. The Security Threat Risk Assessment (STRA) must be used by the Information Asset owner to evaluate the risk associated with a given service, or the information associated with a service. This standard is to be used in conjunction with the information security classification and security threat risk assessment.
4. Staff accessing the information through the network must complete all steps required in Core Policy and regulations required to have access to Government data.
5. All documentation to support the above four points have been completed, authorized and stored according to Core Policy and regulations.

7 General characteristics

7.1 Enterprise Security Model

The security controls employed by the BC Government have been divided into four logical groupings:

1. Boundary Layers (network segmentation, security zones, network firewalls, network IPS, anomaly detection, proxy/reverse proxy, network encryption, network access control, content filtering)
2. Trust Levels (device and user validation, user authorization, data level authentication)
3. Platform Hardening (host/application firewall, patch management, malware protection, data encryption, host IPS), and
4. Security Management (vulnerability management, asset management, security information management, review controls).

7.1.1 Overview of Network Security Zones

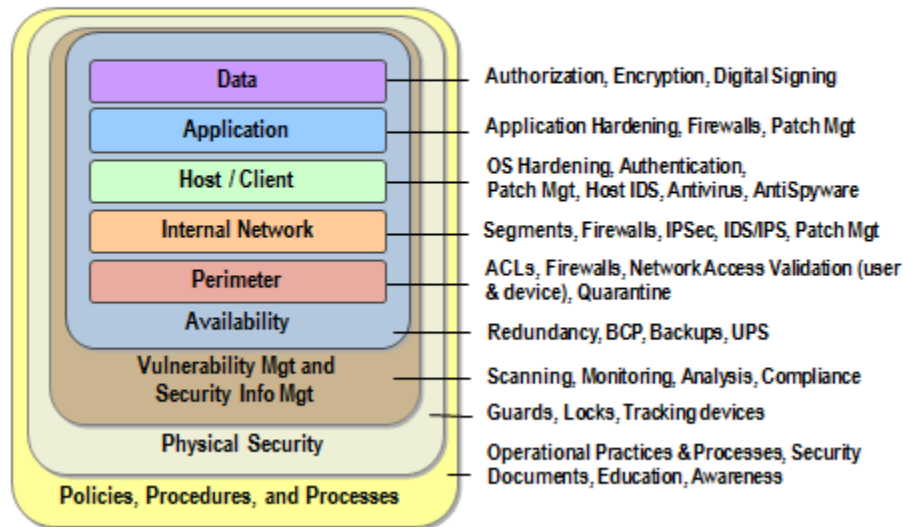


Figure 1

This Network Security Zone standard applies to the Perimeter and Internal Network controls as reflected in Figure 1 and utilizes network segmentation to create clearly defined Security Zones. The concept of Security Zones is an IT industry, widely accepted best practice for establishing security boundaries, control points and accountabilities. A Security Zone is a logical entity containing one or more types of services or entities. Security Zones group together those entities with similar security requirements and levels of risk. Further segmentation within the Zones is supported to allow each service and businesses program the level of security isolation they require.

Segmenting networks into well-defined Security Zones involves a number of different security controls working in concert. On a local switch, VLANs are used to isolate user groups with Virtual Routing Forwarding (VRF) instances providing policy enforcement. All routing between zones is done with firewalls and security is enhanced through the additional use of intrusion prevention systems (IPS) and anomaly detection for stronger policy enforcement. Over the wide area network, technologies like multi-protocol label switching (MPLS), and virtual private networks (VPN) are used to isolate traffic and provide geographic extension of different security zones. Datacenter to datacenter zone extensions must be encrypted when required by the data classification except in situations where dedicated private network facilities are used. Inter-zone security controls are discussed in subsequent sections of this document.

This standard defines several Zones and an associated operations management layer or plane. (See Figure 2, Security Zones: Connectivity) The architecture supports the classic network Zones such as the Demilitarized Zone (DMZ) and the Internet Zone. It also supports Zones internal to the government

network such as its shared ISP-like service called SPAN/BC, an Extranet Zone for connectivity with business partners of IT services. In addition, the Zone model provides internal Zones at its core; the Restricted High Security Zone (Zone A), the High Security Zone (Zone B), and the Trusted Client Zone (Zone C). Other Zones that are not reflected in figure 2 include Trusted User (BYOD) Zone, PCI Zone, Guest Zone (Internet only), Building Utility Services Zone, PLNet Zone, Pharmanet Zone, BPS Zone and a Collaboration Zone for edge servers and infrastructure associated with unified communications and collaboration. Lastly, the zone model supports a highly restricted and segmented operations management layer to provide the administrator access required to service the core infrastructure as well as the business applications.

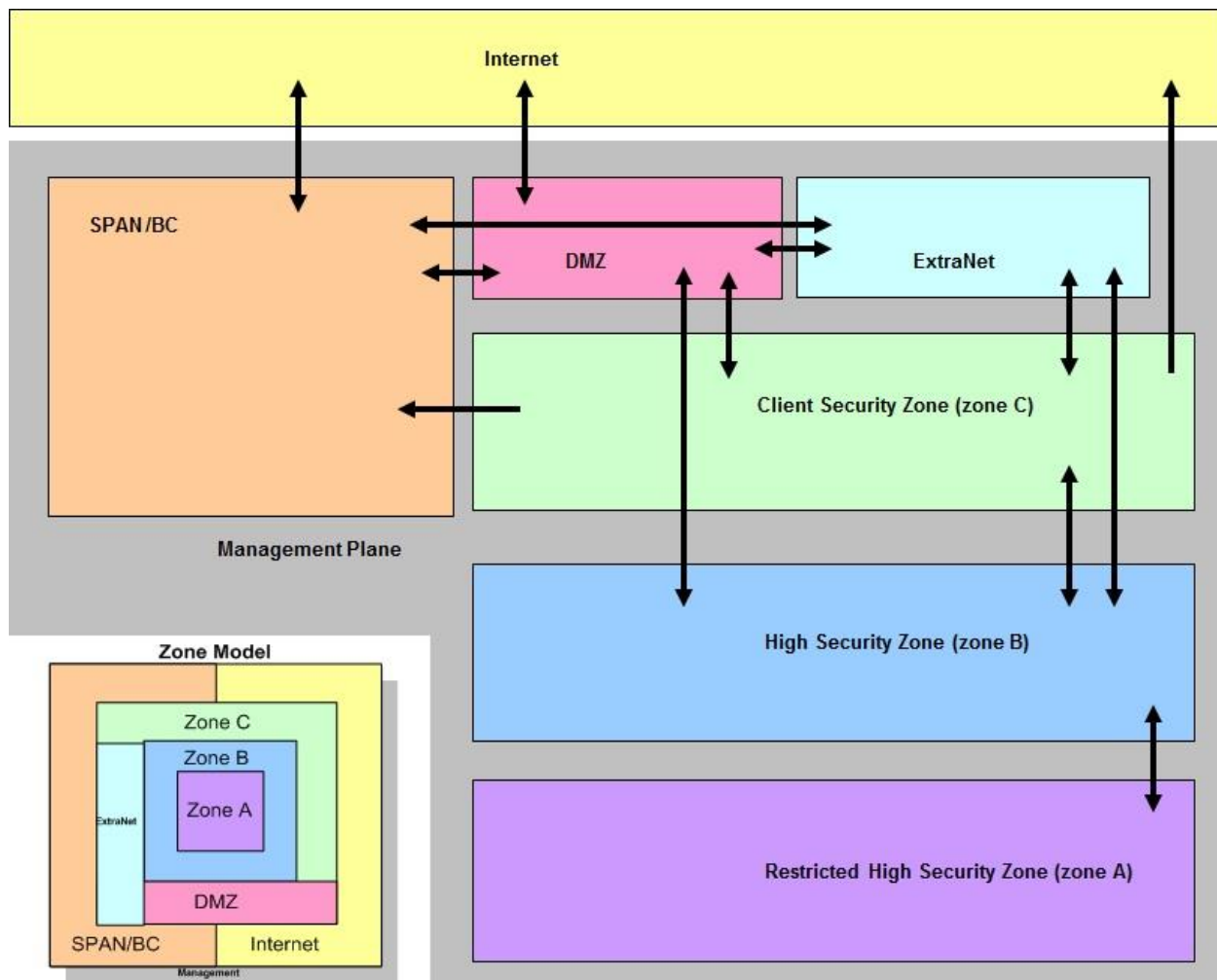


Figure 2 - Security Zones: Connectivity

The objective of the internal zones A, B and C are to provide increasing levels of security by limiting their visibility and connectivity to other zones and their associated devices.

7.1.2 Summary

The fundamental zone connectivity concepts for the security zones model are:



- Not all Zones are visible to all other Zones; only Security Zones adjacent to one another may initiate or service communication requests and as a result, there is no Security Zone “hopping”. E.g., desktops in the Trusted Client Zone cannot directly initiate a session with the application data stored in a server in the Restricted High Security Zone as they are not adjacent.
- Zone extensions (eg. Zone B in the Calgary datacentre to Zone B in the Kamloops datacentre) must be encrypted when required by the data classification framework except in situations where dedicated private network facilities are used.
- The session initiation between the security zones may or may not be bi-directional with an adjacent security zone. E.g., a desktop in the Trusted Client Zone can initiate a session with the Internet, but devices on the Internet cannot initiate a session with the Trusted Client Zone desktop.
- The datacenter **Management Plane** is physically separate from other Zones, and it is internally segmented. Each server’s dedicated network interface is on its own segmented network and interfaces on the Management Plane networks do not have visibility to each other.
- All traffic that transits a Security Zone boundary must pass firewall rules, IPS and anomaly detection.
- All Internet bound traffic sourced from Zone C, Trusted User Zone, Guest Zone or the PLNet Zone must pass through content filtering in accordance with the BC Government standard on Web Content Filtering.

7.2 Detailed Characteristics and Standard

7.2.1 Zone Constructs

7.2.1.1 Management Plane

There are multiple Management Planes used by the Government of BC and its ASD partners. This document is specifically concerned with the Management Plane in the datacenter.

In the datacenters the Management Plane:

- Is a construct that is used for performing backups and patch management.
- Is used for all server administration within datacenters.
- There is no direct access to the Management Plane.
- All access to the Management Plane is achieved through a dedicated Secure Access Gateway (SAG) service.
- IP addresses used in the Management Plane do not have Internet routing.

7.2.1.2 SPAN/BC

The Shared Public Access Network is an ISP-like service where public entities connect to government resources. SPAN is a network that hosts both trusted and un-trusted end-points.

7.2.1.3 DMZ

The DMZ is populated with proxies, web gateways, and other citizen facing interfaces.

Servers and application residing within the DMZ may be Internet accessible and require tighter host and application controls than Zone A and Zone B servers.

Internet facing applications must undergo an Application Vulnerability Scan prior to be placed in the DMZ.

Servers cannot be in IDIR domain if they are in the DMZ. Servers in the DMZ are in the .DMZ domain. A trust relationship exists between IDIR and the DMZ domains.

7.2.1.4 ExtraNet

The ExtraNet zone serves as a landing point for business partners who require connectivity to internal government services.

All ingress and egress traffic from the ExtraNet Zone must pass through a third party gateway equivalent infrastructure.

7.2.1.5 Trusted Client Zone (zone C)

Zone C is the Trusted Client Zone. All Zone C end-points are managed by Government and used by trusted users (IDIR).

7.2.1.6 Trusted User (BYOD) Zone

The Trusted User (BYOD) Zone is for end-user devices that are authenticated to the network with IDIR credentials.

7.2.1.7 High Security Zone (zone B)

Zone B is populated with applications, or databases with data that has a security classification of Low or Medium. High security data may reside in the High Security Zone upon completion of a Security Threat Risk Assessment and following risk acceptance by the information owner.

7.2.1.8 Restricted High Security Zone (zone A)

Zone A is populated with information, applications or databases with data that are classified as High security according to the Information Security Classification Framework (ISCF).

7.2.2 Standard Elements

7.2.2.1 Secure Access Gateway (SAG)

The Secure Access Gateway is a hardened Virtual Desktop or Terminal Services based service that is used to administer applications or data in the datacenter. The Secure Access Gateway should be used to administer applications or databases that reside on servers in the Restricted High Security zone and may be used to administer databases or applications in any datacenter zone.

The SAG service design requirements include:

Connections to the SAG must be made from Zone C or via a VPN that terminates in Zone C.

The SAG service is the best practice for administering applications and databases in Zone A.

The SAG service may be used to administer applications or databases in any zone that is adjacent to Zone B as show above in Figure 2.

SAG users must authenticate against IDIR.

Authentication must not pass through from the end-user localhost session to the SAG session.

The SAG service must have the capability to support multi-factor authentication.

The SAG service must log all connections and session details including failed connection attempts with accurate time stamps.

The desktop delivered by the SAG service must reside in Zone B and will be subject to all Zone B rules as defined in this standard.

The SAG must provide a mechanism to restrict user inter-zone and intra-zone access based on static IP address or VLAN assignment.

The desktop delivered by the BC SAG must follow a regular patching schedule, maintain up to date anti-virus protection, host-based firewall, and support session timeout.

Controls must be in place between the end-user localhost and the SAG desktop to restrict the ability to cut-and-paste or transfer files between the two environments. There must be no direct file transfer access from the user desktop to the SAG. Any file transfer must be in a secure and auditable manner.

The SAG must allow for client specific builds based on user requirements for specific management software.

Modifications to the SAG must not persist across sessions. Changes to the SAG client specific builds must be facilitated by the administrator of the SAG service.

7.2.2.2 Servers

Servers, both dedicated and virtual, can reside in only one non-management zone. A server may not exist in both the High Security Zone and the DMZ at the same time. Virtual Servers sharing a common Hardware or Virtual Operating System must reside on the same Zone.

7.2.2.3 Switches

Access and virtual access switches can reside in only one non-management zone.

A switch may not exist in both the High Security Zone and the DMZ at the same time.

Virtual Switches sharing a common Hardware or Virtual Operating System must reside on the same Zone.

Core and aggregation switches may reside in more than one zone.

7.2.2.4 Network Firewalls

Within the Government of B.C.'s security zone model, network firewalls are a key tool used to control the flow of communication between security zones. Additionally, firewalls may be employed to provide or support other functions such as network address translation (NAT), stateful packet inspection (SPI), device validation, and virtual private network (VPN) services.

7.2.2.5 Host Firewalls

Host firewalls must be configured on all servers that operate outside the SSBC datacenter and should optionally be configured on servers within the datacenter based on the sensitivity of applications and the particular threats presented to that server.

The host firewall on servers should be centrally managed, with the ability to monitor and report security events.

Firewall rules must support configuration based on source and destination IP address and port number for incoming and outbound traffic.

7.2.2.6 Network IDS/IPS

Within the architecture, network IDS/IPS are used to provide general network awareness, detection, notification, and blocking of attacks.

At a minimum, IDS/IPS must be used at the perimeter edges and key boundaries within the enterprise network.

A key boundary may be a physical location where all traffic is inspected, regardless of zone such as in the case of the SSBC datacentre, or the key boundaries may be based on network zones.

7.2.2.7 Proxy/Reverse Proxy

Within the architecture, proxy services are employed primarily in the DMZ to allow applications located within security zones to isolate themselves from untrusted clients or devices requesting their services.

A proxy service can be used to facilitate software updates and license validation for applications in zones A and B.

To prevent compromise of the security zone connectivity rules, proxies may also be employed to support single or two-tiered application that wish to leverage the High Security and Restricted High Security zones.

7.2.2.8 Network Encryption

As a minimum, encryption and its use must comply with the [Cryptographic Standards for Information Protection](#).

7.2.2.9 Access (Wired, Wireless, and Remote)

All devices requesting access to the network require validation. The minimum level of validation is dependent on the device and entry point or zone used to gain network access. Each Security Zone's "access" policy relates to the Zone's base security requirements and is strictly enforced.

The architecture provides support for network access via wired, wireless and remote services. Restrictions apply to some configurations of network access, as is required to support the enterprise Security Zones model. For example, access to the "High Security Zone (zone B)" from the Internet via remote services will not be supported. Those business solutions requiring such connectivity will need to leverage an alternative access solution like; web based proxy or Secure Access Gateway services.

7.2.3 Inter-zone Connectivity

Connectivity between zones is subject to principles of adjacency (no zone hopping), rules may be asymmetric, and intra-zone communications will in some cases be restricted. The following table contains the standard for access controls and the description of the minimum connectivity rules:



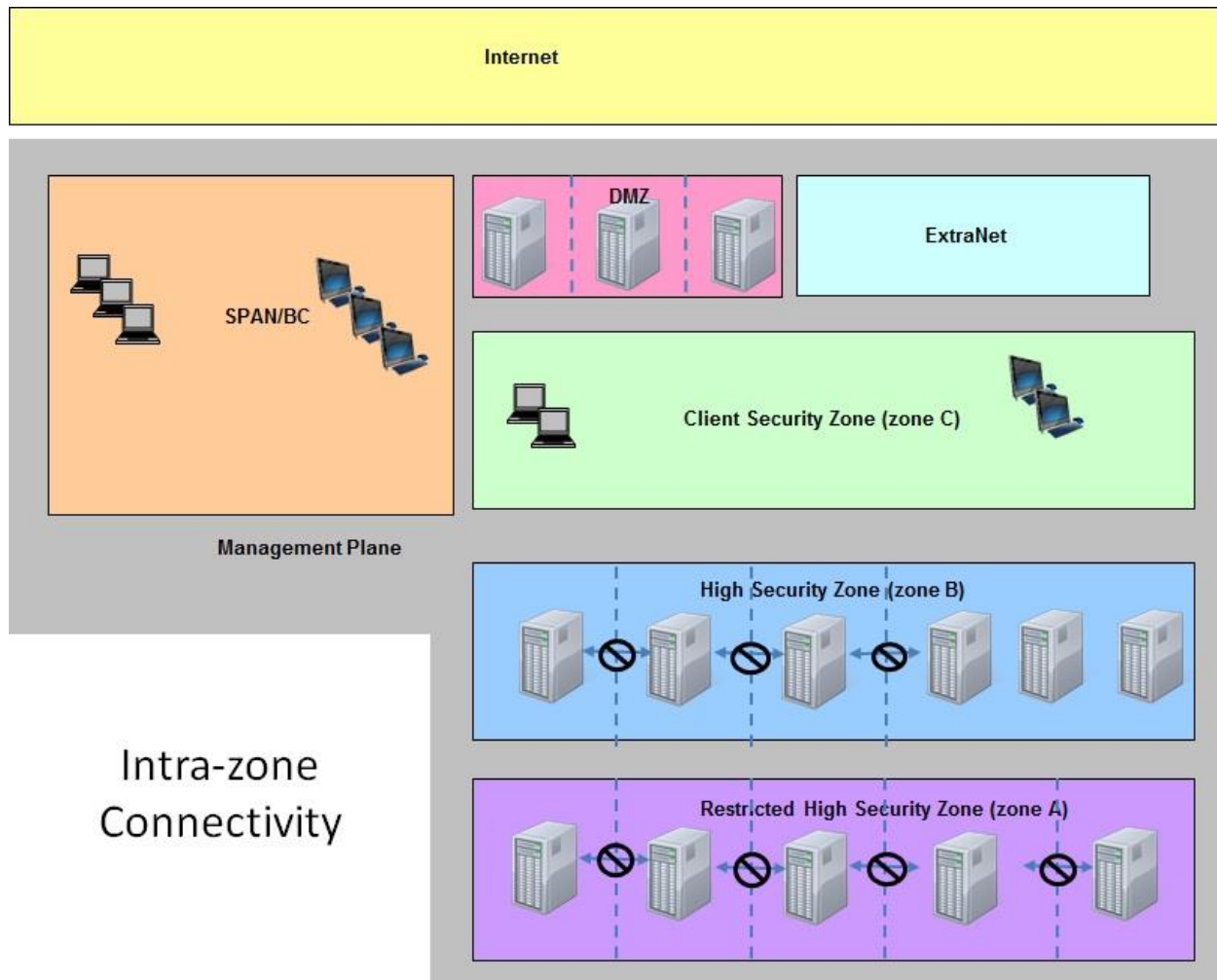
Table 3

From To	Restricted High Security (A)	High Security Zone (B)	Clients (C)	DMZ	ExtraNet	SPAN/BC	Internet
Restricted High Security (A)	Destination IP address AND Port #	Destination IP address AND Port #	No Access	No Access	No Access	No Access	No Access
High Security Zone (B)	Destination IP address AND Port #	Destination IP address OR Port #	Destination IP address OR Port #	Destination IP address AND Port #	Destination IP address AND Port #	No Access	No Access
Clients (C)	No Access	Destination IP address OR Port #	No Restrictions	Destination IP address OR Port #	Destination IP address OR Port #	No Restrictions	No Restrictions (except Internet Policies)
DMZ	No Access	Destination IP address AND Port #	Destination IP address OR Port #	Destination IP address AND Port #	Destination IP address OR Port #	No Restrictions (except Internet Policies)	No Restrictions (except Internet Policies)
ExtraNet	No Access	Destination IP address AND Port #	Destination IP address OR Port #	Destination IP address AND Port #	No Restrictions	Destination IP address OR Port #	No Access
SPAN/BC	No Access	No Access	No Access	Destination IP address OR Port #	Destination IP address OR Port #	No Restrictions	No Restrictions
Internet	No Access	No Access	No Access	Destination IP address OR Port #	No Access	No Restrictions	n/a
Mgmt	No Restrictions - Management functions only	No Restrictions - Management functions only	No Restrictions - Management functions only	No Restrictions - Management functions only	No Restrictions - Management functions only	No Access	No Access

Note that the table references port numbers, but some protocols do not use ports. In some cases a protocol may be defined if that protocol does not use ports. This table describes minimum rules for a specific source IP address (ie. server) within a Zone. Additional restrictions may be applied across and within Zone boundaries based on a business requirements and threat risk assessment.

7.2.4 Intra-Zone Connectivity

Within a given security zone, there are additional segments or partitions. The segmentation of networks within a zone may be accomplished through the use of VLANs. These segments are used, for example, to isolate different classes of hosts that have no requirement to interact with each other. This principle of least privilege helps to contain the damage in the event that any given system is compromised. Instead of VLANs, host based firewalls may be used to protect hosts within a common Zone. The following diagram provides a conceptual view of how the High Security and Restricted High Security zones could be partitioned:

**Figure 3**

For simplicity, figure 3 does not attempt to show supporting security elements such as firewalls, intrusion detection systems or content filters. Intra-zone communication between sub-zones is denied by default, and subject to the minimum security configuration outlined in Table 3.

Each partition within a zone is a separate VLAN or MPLS-VPN.

7.2.5 Enforcement

Information owners define the information security classification of the assets that they are responsible for. The information owner in conjunction with the application or database administrator determines the appropriate zone placement. HP-AS defines firewall rules as requested by administrators. The information asset owner for the destination of firewall rule request is the approver and also responsible for ensure that firewall requests comply with this standard. The Information Asset owner is responsible to ensure that a periodic validation of the configured firewall rule set is compared against the rules that have been requested for the application or database.

Zone B Access to the Internet

Some applications will require access to resources on the Internet. License validation and downloading application updates are examples where applications may require access to the Internet. Due to the dynamic nature of content distribution networks it may be difficult to identify specific IP addresses or even network ranges that need to be accessed by a specific application, therefore it is desirable to filter Internet traffic outbound from zone B based on URL. This may be accomplished by using the SSBC provided forward proxy service. In the event that an application requires Internet access and cannot be configured to use the forward proxy service, then the public IP address must be obscured using NAT.

- The default for zone B applications is No Access to the Internet.
- Applications that require access to the Internet from zone B should be deployed in such a way that the application owner leverages a proxy server in the DMZ.
- Access to the Internet for applications from zone B for applications that use HTTP or HTTPS may use the SSBC forward proxy service.
- In the event that an application is unable to use the SSBC proxy service and the application owner deems that it is impractical to host their own proxy service in the DMZ, then the application owner may request that SSBC grant an exception to allow the specified zone B application access to the Internet. The exception process differs from the exemption process.
- The exception request must include the name and IP address of the application. The name, telephone and email address of the application owner. Confirmation that the application requires Internet access and that the proxy service has been ruled out as an option and the reason for ruling out the proxy service as an option. Additionally the application owner must specify a destination port and IP address range that are required for their application.
- There will be no Zone B firewall rules that have a destination of any.
- In the event that an exception is made for a Zone B application the server's IP address will be NAT'd.

8 Evaluation criteria

8.1 Enquiry Scope

OCIO Information Security Branch, OCIO Architecture and Standards Branch, SSBC Network Services, SSBC Security Operations, SSBC Technology Solutions Division.

Annex A. Standard for Network Security Zones

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2012-10-18 Scheduled Review: Biannual Last Updated: 2012-10-18 Last Reviewed: 2012-10-11
	Type: Technical
X.0 Information Technology Security (CPPM 12.3.6)	
X.Y Network Security Zone standard	
Keywords: Network, datacenter	

Description of Standard

The strategic aim of this standard is to support the Government's goals through improvements to IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support Province's business needs of the future.

This standard governs the separation and protection of government data networks according to zones that are based on the classification of the information assets that the zones and associated security controls are intended to protect.

Where to Apply This Standard

This standard applies where there is a need to isolate and segment the government's networks and and/or for the graduated protection of government applications and the data that those applications process. The zone required in any given network application is determined by business requirements, Security Threat Risk Assessment and Privacy Impact Assessment.

Authority and Exemptions

This standard has been issued by the Office of the CIO in accordance with the Core Policy and Procedures Manual Chapter 12.3.6, Information Technology Security and the Information Security Policy.

If there are compelling business reasons why an organization is unable to comply with this architecture or standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

Information owners define the information security classification of the assets that they are responsible for. The information owner in conjunction with the application or database administrator determines the appropriate zone placement. HP-AS defines firewall rules as requested by administrators. The information asset owner for the destination of firewall rule request is the approver and also responsible for ensure that firewall requests comply with this standard. The Information Asset owner is

responsible to ensure that a periodic validation of the configured firewall rule set is compared against the rules that have been requested for the application or database.

Terms and Definitions

See section 5 of the full standard for Terms and Definitions.

References

The full Network Security Zones standard is available on the intranet at:

<insert link to standard>

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca

Contact

Architecture and Standards Branch, Office of the CIO

email: ASB.CIO@gov.bc.ca



ACCESS CONTROL SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.1

Published: August 2020

Table of Contents

I INTRODUCTION, SCOPE, BACKGROUND	3
II GLOSSARY, TERMS AND DEFINITIONS, LIST OF COMMONLY USED REFERENCES.....	3
1 ACCESS CONTROL	4
1.1 BUSINESS REQUIREMENTS OF ACCESS CONTROL	4
1.2 EMPLOYEE ACCESS MANAGEMENT.....	9
1.3 EMPLOYEE RESPONSIBILITIES.....	15
1.4 SYSTEM APPLICATION ACCESS CONTROL.....	16

I Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: [IM/IT Standards](#)).

II Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the “Glossary”, “Terms and definitions” and “List of commonly used references” sections of the Information Security Standard (version 2.0) (published here: [IM/IT Standards](#)) for the terms and definitions used in this standard.

1 Access Control

This chapter identifies the controls that restrict access to government information and information assets. Access control protects organizations from security threats such as internal and external intrusions. The controls are guided by legislation that protects particular types of information (e.g., personal and other types of confidential information) and by business requirements.

Access control policies provide the blueprint for the management of employee access, authorizations and control requirements for computer networks, operating systems, applications and information. This chapter identifies security best practices and responsibilities for administrators and employees.

1.1 Business requirements of access control

- 1.1.1 Access to information systems and services must be consistent with business needs and be based on security requirements.**
- a) Access control policy**
 - b) Access control policy management**
 - c) Review of access control policy**

Purpose: *To ensure that information and information systems are available for authorized use and protected from unauthorized use.*

1.1.1 a) Access control policy

Information Owners and Information Custodians are responsible for establishing, documenting and approving access control policies which must:

- Support and enable business requirements;
- Be based on requirements identified in Privacy Impact Assessments and Security Threat and Risk Assessments; and,
- Include classification of assets.

Access control policies must additionally:

- Consider both physical and logical access to assets;
- Apply the need-to-know and least privilege principles;
- Set default access privileges to deny-all prior to granting access;
- Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable;
- Have permissions assigned to roles rather than individual user identifiers; and,
- Access requirements should be determined at a functional, work unit level.

The access control policy must be communicated to employees as part of awareness training.

1.1.1 b) Access control policy management

Information Owners and Information Custodians are responsible for establishing processes to manage the access control policies, including:

- Ensuring the process is communicated to all employees;
- Documenting processes for employee registration and deregistration;

- Segregating roles and functions (i.e. access requests, access authorization, access administration);
- Defining rules for controlling access to privileged system functions;
- Identifying roles and/or functions which require multi-factor authentication; and,
- Identifying and justifying exceptional cases where there is a need for enhanced employee security screening for sensitive assets.

1.1.1 c) Review of access control policy

Information Owners and Information Custodians must conduct periodic reviews of the access control policies as part of an ongoing process for risk management, security, and privacy. Annual reviews are recommended. Reviews must be conducted:

- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes;
- When the threat environment changes or new vulnerabilities arise;
- Following significant government or Ministry re-organization as appropriate; and,
- For sensitive and business critical assets, reviews should be conducted more frequently than annually, based on the Security Threat and Risk Assessment.

Recommended Tests:

Note: 1.1.1 is reported on as part of the annual information security review.

- Demonstrate information sensitivity and classification is considered prior to granting access.
- Demonstrate segregation of duties for authorizing and administering.
- Demonstrate review of access logs.

1.1.2 Employees must only be provided access to the network services they have been specifically authorized to use.
--

a) Access to network services

b) Management controls and processes

c) Means for accessing networks and network services

Purpose: *To support the information system access control policy by limiting network access to authorized users of specific information systems.*

1.1.2 a) Access to network services

Information Custodians must enable network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system.

1.1.2 b) Management controls and processes

Information Custodians must document processes for management of network access, including:

- Documentation and review of implemented network access controls;
- Identification of threats, risks and mitigation factors associated with network services;
- Testing of network access controls to verify correct implementation; and,

- Assisting Information Owners to verify the principle of least privilege is used to minimize access, as specified in the access control policy.

1.1.2 c) Means for accessing networks and network services

Information Custodians must define and implement:

- Permitted network access methods for each network zone (e.g., direct connection, Virtual Private Network, Wi-Fi, remote desktop connection, desktop terminal services); and,
- Minimum security controls required for connection to networks (e.g., patch levels, anti-virus software, firewalls, user and system authentication requirements).

Recommended Tests:

Note: 1.1.2 is reported on as part of the annual information security review.

- Demonstrate systems network access controls are implemented and tested to prevent unauthorized access.
- Demonstrate network security controls are in place and up-to-date to prevent unauthorized access.

1.1.3 Remote access to government information systems must be subject to authentication.

a) Remote access to government networks or services

Purpose: *To identify and authenticate users and systems accessing the government network from remote locations.*

1.1.3 a) Remote access to government networks or services

Providers of remote network access services for individuals must:

- Perform a Security Threat and Risk Assessment for each remote access service to determine the authentication methods to be implemented. Factors to be considered include classification of network services, and information and information systems accessible from the remote access service;
- Require remote users to connect through government designated remote access services or security gateways (e.g., Virtual Private Network (VPN), Desktop Terminal Services (DTS), Outlook Web Access);
- Require user identification and authorization prior to permitting each remote network connection; and,
- Require multifactor authentication when accessing sensitive information from untrusted networks (eg. the Internet).

Providers of remote network access services for interconnection of networks must:

- Perform a Security Threat and Risk Assessment for each remote network interconnection to determine the user and system authentication methods to be implemented. Factors to be considered include:
 - classification of network services, information, and information systems accessible from the remote access service, and,
 - the strength of security controls implemented in the remote network;
- Obtain prior approval to interconnect networks from Information Owners of every information system accessible from the remotely connected networks; and,
- Require remote network interconnections to connect through government designated remote

access services or security gateways (e.g., Virtual Private Network, Third Party Network Gateway).

Recommended Tests:

Note: 1.1.3 is not reported on as part of the annual information security review.

- Demonstrate an approval been obtained from Information Owners prior to interconnecting networks.

1.1.4 Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment. a) Authentication of connections

Purpose: *To increase assurance of system identification where required by system sensitivity or classification.*

1.1.4 a) Authentication of connections

Information Owners must use automatic equipment identification if the requirement is identified by a Security Threat and Risk Assessment. Factors to consider include:

- The sensitivity and classification of information that may be accessed or stored;
- The physical security of information, information technology assets and location;
- Unauthorized information access by people at the location, either inadvertent or deliberate; and,
- Remote access threats if remote access is utilized.

When Information Owners identify a requirement for connection to a network or information system from a specific location or equipment, the connection may be authenticated using automated equipment. Activities include:

- An identifier must be in, or attached to, the equipment;
- The identifier indicates that the equipment is permitted to connect to specified networks or information systems and must be maintained in the asset inventory;
- The equipment identifier must be inspected, and sessions should be logged to verify that the identifier is being correctly used for access; and,
- Connections must be monitored to detect anomalies, such as unusual session times, overly long sessions, or increased frequency of use.

Good physical security is required to complement the use of equipment identifiers. Reliance should not be placed solely on automated equipment for authentication. The equipment should be secured from tampering by locating it inside a secure facility or ensuring it is under the direct supervision of an individual.

1.1.5 Physical and logical access to diagnostic ports must be securely controlled. a) Protection of diagnostic ports

Purpose: *To prevent unauthorized use of maintenance or diagnostic facilities.*

1.1.5 a) Protection of diagnostic ports

To prevent bypassing of information system access controls, Information Custodians must implement access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed and kept active for the minimum time required.

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized by agreements, contracts and conditions of use.

Use of diagnostic ports must be logged and monitored for suspicious activity.

Recommended Tests:

Note: 1.1.5 is not reported on as part of the annual information security review.

- Demonstrate controls.

1.1.6 The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system.

a) Logical and physical network connection control

b) Wireless networks

Purpose: *To control network connection in support of the access control policy and limit opportunity for unauthorized access.*

1.1.6 a) Logical and physical network connection control

Information Custodians must restrict the ability of users to physically and logically connect to networks according to the access control policy defined by Information Owners. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

Direct network connections to information systems must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to segregate it from direct network connections by employee workstations.

1.1.6 b) Wireless networks

Information Custodians must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a Security Threat and Risk Assessment.

Recommended Tests:

Note: 1.1.6 is not reported on as part of the annual information security review.

- Demonstrate that network access is granted following the requirements for logical and physical separation.

1.1.7 Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system.
a) Network address control
b) Control of routing information

Purpose: *To control network routing to prevent unauthorized access or bypassing of security control points.*

1.1.7 a) Network address control

Information Custodians must implement mechanisms to prevent unauthorized changes to network routing and traffic flow (e.g., through use of router access control lists).

Security gateways must be considered for network access control points, in accordance with information system security classification requirements. Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

1.1.7 b) Control of routing information

Information Custodians must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).

Recommended Tests:

Note: 1.1.7 is not reported on as part of the annual information security review.

- Demonstrate network access control points.

1.2 Employee access management

1.2.1 There must be a formal employee registration and de-registration process for granting access to all information systems.
a) Registration
b) De-registration

Purpose: *To ensure that all access actions are traceable to an identifiable individual or process.*

1.2.1 a) Registration

Information Owners and Information Custodians are responsible for managing access to the assets under their control and must implement registration processes which:

- Require approval for all access rights;
- Ensure access requests are approved by the Supervisor of the employee requesting access;
- Ensure the reasons for requesting access are consistent with job responsibilities;
- Maintain records of access right approvals;

- Ensure employees understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- Ensure access rights are consistent with the data uses documented in the approved Privacy Impact Assessment;
- Ensure accesses are traceable to an identifiable individual or process;
- Ensure each employee is assigned a single unique identifier for accessing information systems (See Exceptions section below);
- Ensure the responsibilities for authorizing access are segregated from the responsibilities for granting access;
- Restrict access by using predefined role permissions;
- Provide secure and separate transmission of the user identifier and password to the employee; and,
- In exceptional cases, where warranted by the classification of the asset and supported by a Security Threat and Risk Assessment, ensure enhanced employee security screening or background checks are completed prior to authorizing access.

1.2.1 b) De-registration

Information Owners and Information Custodians must formally assign responsibilities and implement processes to:

- Remove access privileges for employees no longer with the organization within 5 working days;
- Promptly review access rights whenever an employee changes duties and responsibilities;
- Promptly review access rights whenever the employee's branch or department is involved in significant reorganization;
- Review access privileges for employees on extended absence or temporary assignments within 10 working days of the change of status;
- Remove access privileges for employees terminated for cause concurrent with notification to the individual; and,
- Quarterly check for and remove inactive or redundant user identifiers.

Authority and Exceptions:

Individual employees may have multiple identifiers when:

- Required to meet limitations of technology (e.g., IDIR, MVS).
- Required to meet unique business requirements provided the rationale is documented and approved by the Information Owner or Information Custodian as appropriate.

Recommended Tests:

Note: 1.2.1 is reported on as part of the annual information security review.

- Demonstrate unique IDs are issued to employees and are documented.
- Demonstrate that exemption requests for shared IDs are current and are monitored.

1.2.2 A formal employee access provisioning process must be implemented to assign or revoke access rights for all user types to all systems and services.

Purpose: *To ensure authorized user access and to prevent unauthorized user access to systems and services.*

1.2.2 a) Access provisioning process

Information Owners and Information Custodians must implement a formal employee access provisioning process. The provisioning process for assigning or revoking access rights granted to user IDs must include:

- Obtaining authorization from the owner of the information system or service for the use of the information system or service. Separate approval for access rights from management may also be appropriate;
- Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties;
- Ensuring that access rights are not activated (e.g., by service providers) before authorization procedures are completed;
- Maintaining records of access rights granted to a user ID to access information systems and services;
- Adapting access rights of employees who have changed roles or jobs and immediately removing or blocking access rights of employees who have left the organization; and,
- Periodically reviewing access rights with owners of the information systems or services.

Guidelines:

Employee access roles should be established based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews are more easily managed at the level of such roles than at the level of particular rights. Consideration should be given to including clauses in employees' contracts and service contracts that specify sanctions if unauthorized access is attempted by employees.

Recommended Tests:

Note: 1.2.2 is reported on as part of the annual information security review.

- Demonstrate access is authorized by appropriate authorities prior to providing access and that authorization is specific to access rights.
- Demonstrate owners and/or their designate grant access based on business requirements.
- Demonstrate access is role based versus user based.

1.2.3 The allocation and use of system privileges must be restricted and controlled.
a) Managing, restricting and controlling the allocation and use of system privileges
b) Managing the issuance of privileged user credentials

Purpose: *To prevent unauthorized access to multi-user information systems.*

1.2.3 a) Managing, restricting and controlling the allocation and use of system privileges

Information Owners and Information Custodians are responsible for authorizing system privileges and must:

- Identify and document the system privileges associated with each information system or service;
- Ensure the process for requesting and approving access to system privileges includes Supervisor approval(s) prior to granting of system privileges;
- Ensure processes are implemented to remove system privileges from employees concurrent with changes in job status (e.g., transfer, promotion, termination);

- Limit access to the fewest number of employees needed to operate or maintain the system or service;
- Ensure the access rights granted are limited to and consistent with employee job functions and responsibilities;
- Maintain a record of employees granted access to system privileges;
- Ensure use of system privileges is recorded in audit logs which are unalterable by the privileged user;
- Implement processes for ongoing compliance checking of the use of system privileges; and,
- Implement processes for regular review of authorizations in place to confirm that access is still needed and that the least number of users needed have access.

User identifiers with system privileges must only be used for performing privileged functions and not used to perform regular activities. User identifiers established to perform regular activities must not be used to perform privileged functions.

Guidelines:

- The design of information systems should include processes for performing regular maintenance activities which avoid the requirement of system privileges.
- Whenever possible system routines should be used to execute system privileges rather than granting system privileges to individual employees.
- System acquisition and development should encourage use of programs which minimize the need for employees to operate with system privileges.

Privileged users should:

- Not read the data of an information asset unless authorized;
- Be able to alter user permissions for an information asset; and,
- Be permitted to view, but not alter, user activity logs as part of security safeguards.

1.2.3 b) Managing the issuance and revocation of privileged user credentials

The issuance of privileged user credentials must have two levels of approval. Use of system privileges should require use of multi-factor authentication.

Recommended Tests:

Note: 1.2.3 is reported on as part of the annual information security review.

- Demonstrate privileged users' access is regularly reviewed to ensure access rights are in line with business requirements.
- Demonstrate that logs are regularly reviewed for privileged user activity.
- Demonstrate that when employees no longer require privileged access, it is removed.

1.2.4 The issuance and revocation of authentication credentials must be controlled through a formal management process.

a) Managing the issuance of authentication credentials

Purpose: *To define the formal management processes for issuing passwords.*

1.2.4 a) Managing the issuance and revocation of authentication credentials

Ministries must formally designate individuals who have the authority to issue and reset passwords. The following applies:

- Passwords must only be issued to employees whose identity is confirmed prior to issuance;
- Individuals with the authority to reset passwords must transmit new or reset passwords to the employee in a secure manner (e.g., using encryption, using a secondary channel);
- Whenever technically possible, temporary passwords must be unique to each individual and must not be easily guessable;
- Passwords must never be stored in an unprotected form;
- Default passwords provided by technology vendors must be changed to a password compliant with government standards during the installation of the technology (hardware or software); and,
- The revocation of authentication credentials must follow a formal process.

Recommended Tests:

Note: 1.2.4 is reported on as part of the annual information security review.

- Demonstrate that passwords are never stored or transmitted in clear text.
- Demonstrate employees are made aware to never divulge their password.
- Demonstrate that vendor provided equipment and software default passwords are changed upon implementation.

1.2.5 Information Owners must formally review employee access rights at regular intervals.
a) Circumstances and criteria for formal access right review
b) Procedure for formal access right review

Purpose: *To ensure that access rights only exist for users with a defined "need to know".*

1.2.5 a) Circumstances and criteria for formal access rights review

Information Owners and Information Custodians must implement formal processes for the regular review of access rights. Access rights must be reviewed:

- Annually;
- More frequently for high value information assets and privileged users;
- When an employee's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect an employee's need to access information assets;
- As part of a major re-organization, or the introduction of new technology or applications; and,
- When Information Owners change the access control policy.

1.2.5 b) Procedure for formal access rights review

Review of access rights must include the following:

- Confirmation that access rights are based on the need-to-know and least privilege principles;
- Confirmation that all members of the group/role have a need-to-know;
- Reviews and verification of access control lists dated and signed by the reviewer and kept for audit purposes; and,
- Confirmation that changes to access rights are logged and auditable.

Access control logs and reports are government records and must be retained and disposed of in accordance with approved record management schedules.

Recommended Tests:

Note: 1.2.5 is reported on as part of the annual information security review.

- Demonstrate a regular review of all employee access rights are based on business requirements.
- Demonstrate reviews of access privileges for employees that have changed roles within the organization.
- Demonstrate changes to user access rights are logged.

1.2.6 The access rights of employees to information systems must be removed upon termination of employment and reviewed upon change of employment.
a) Change of employment status
b) Action upon termination or change of employment
c) Reduction of access rights

Purpose: *To ensure physical and logical access rights to information systems and information processing facilities are managed in relation to the security responsibilities of the job requirements.*

1.2.6 a) Change of employment status

Supervisors must review access to information systems and information processing facilities when employees change employment, including:

- When employees assume new roles and responsibilities;
- During restructuring of positional or organizational roles and responsibilities;
- When employees commence long-term leave; and,
- Updating directories, documentation and systems.

1.2.6 b) Action upon termination or change of employment

Supervisors must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment by:

- Removing or modifying physical and logical access;
- Recovering or revoking access devices, cards and keys; and,
- Updating directories, documentation and systems.

1.2.6 c) Reduction of access rights

Supervisors must ensure access to information systems and information processing facilities is reduced or removed before the employment terminates or changes, based upon the evaluation of risk factors such as:

- Whether the termination or change is initiated by the employee/contractor or by a Supervisor;
- The reason for termination;
- The current responsibilities of the employee/contractor; and,
- The value of the assets currently accessible.

Recommended Tests:

Note: 1.2.6 is reported on as part of the annual information security review.

- Demonstrate review of access to information systems and information processing facilities is conducted when employees change employment.
- Demonstrate access to information systems and information processing facilities is immediately removed upon termination of employment.

1.3 Employee responsibilities

1.3.1 Employees must follow security best practices in the selection and use of passwords.

- a) Selection of passwords
- b) Password change
- c) Privileged accounts
- d) Protection and use of passwords

Purpose: *To maintain the integrity of the unique identifier (user id) by ensuring employees follow security best practices.*

1.3.1 a) Selection of passwords

When selecting passwords employees must:

- Select complex passwords, i.e., a mixture of characters as specified in the Standard;
- Keep authentication information confidential;
- Avoid recording authentication information; and,
- Avoid using the same password for multiple accounts.

The effectiveness of access control measures is strengthened when employees adopt security best practices for selecting passwords.

1.3.1 b) Password change

Passwords must be changed:

- During installation of hardware or software which is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If compromise has taken place or is suspected the incident must be reported in accordance with the Information Incident Management Process; and,
- In compliance with password change instructions issued by an automated process (e.g., password life-cycle replacement) or an appropriate authority.

1.3.1 c) Privileged accounts

Privileged accounts have wider and more powerful access rights to information assets. In addition to 1.3.1 a) and b), employees authorized to create or who hold privileged accounts must use passwords which are at least 15 characters where technically feasible.

1.3.1 d) Protection and use of passwords

Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing passwords;
- Permitting anyone to view the password as it is being entered;
- Writing down a password;
- Storing other personal identifiers, access codes, tokens or passwords in the same container;
- Keeping a file of passwords on any computer system, including mobile devices, unless that file is encrypted according to the Cryptographic Standards for Information Protection;
- Employing any automatic or scripted logon processes for personal identifiers; and,
- Using personal identifiers, access codes, or passwords associated with government accounts for non-government purposes.

Where a business need is defined to keep written records of passwords, a request for an exemption must be submitted to the Chief Information Security Officer.

Standards:

The Complex Password Standard for government systems requires that passwords must:

- Contain a minimum of 8 characters;
- Contain characters from three of the following categories:
 - English upper-case characters (A to Z),
 - English lower-case characters (a to z),
 - numerals (0 to 9), and,
 - non-alphanumeric keyboard symbols (e.g., ! \$ # %); and,
- Not contain the username or any proper names of the employee.

For example, the complex password "T#ocitpi7" is derived from the phrase "The number of clowns in the parade is seven". Complexity can be further increased by substituting numbers for vowels.

For mobile devices connecting to the government messaging server, the following password rules apply:

- Passwords must contain a minimum of 6 characters;
- Controls should be in place to prevent the use of overly simple passwords; and,
- The use of a combination of numbers, symbols, upper- and lower-case characters is recommended to increase the password strength.

Guidelines:

Never divulge your password to anyone. Legitimate IT technical support employees such as systems administrators, helpdesk and security will not ask employees for their passwords.

Authority and Exceptions:

Exception is granted to RACF and VM Secure due to technical product limitations.

Recommended Tests:

Note: 1.3.1 is reported on as part of the annual information security review.

- Demonstrate password requirements are communicated to employees.
- Demonstrate an awareness program identifying employee password responsibilities.
- Demonstrate additional controls on privileged accounts.

1.4 System application access control

- 1.4.1 Access to information systems functions and information must be restricted in accordance with the access control policy.**
- a) Information access controls
 - b) System configuration
 - c) Publicly accessible information

Purpose: *To restrict access to application systems functions and information to authorized individuals or systems.*

1.4.1 a) Information access controls

Information Owners and Information Custodians are responsible for ensuring the implementation of the access control policy for their business applications. Every information system must have an access control policy that specifies access permissions for information and system functions. The access control policy must identify the information and system functions accessible by various classes of users.

The application and information section of the access control policy must specify:

- The information to be controlled;
- The system functions to be controlled; and,
- The roles authorized to access the resources and information and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

1.4.1 b) System configuration

Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.

System utilities or functions that can bypass user access controls must be specified in the access control policy. Access to these utilities and functions must be restricted.

1.4.1 c) Publicly accessible information

Information that is publicly accessible must be segregated from non-public information.

Recommended Tests:

Note: 1.4.1 is reported on as part of the annual information security review.

- Demonstrate access controls are implemented for application system functions.
- Demonstrate access control policies restrict access to powerful utilities and functions (e.g., role-based access controls).
- Demonstrate access control policies segregate public information from non-public information.

1.4.2 Information systems managing data of a sensitive nature must have an isolated dedicated computing environment.
a) Segregation of sensitive information systems

Purpose: *To ensure that sensitive information systems are segregated from non-sensitive information systems and are not compromised by sharing information technology resources with non-sensitive information systems.*

1.4.2 a) Segregation of sensitive information systems

Information Owners and Information Custodians must conduct a Security Threat and Risk Assessment to determine the information system classification level. The information system classification level determines which network security zone the information system must reside in.

Security zones must be established using physical or logical methods, which may include separate network segments, separate servers, firewalls, access control lists and proxy servers.

Recommended Tests:

Note: 1.4.2 is reported on as part of the annual information security review.

- Demonstrate the information system classification level has been determined.
- Demonstrate physical or logical security zones have been created.

1.4.3 Access to information systems must use a secure logon process.
a) Information displayed during logon
b) Unsuccessful logon attempts
c) Password transmission

Purpose: *To ensure access to information systems is limited to authorized users and processes.*

1.4.3 a) Information displayed during logon

Information Owners must ensure that Information Custodians configure logon processes to minimize the opportunity for unauthorized access, which includes:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

1.4.3 b) Unsuccessful logon attempts

Information Owners must ensure that Information Custodians configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure, and if exceeded, the system should terminate the logon; and,
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

1.4.3 c) Password transmission

Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

Standards:

After three consecutive failed logon attempts for an account the logon process must:

- Lock the account and require Administrator intervention; or,
- Lock the account for 15 minutes and then allow a further three logon attempts.

Guidelines:

A general warning should be displayed that the information system is accessed only by authorized users.

The logon procedure should permit users to monitor the security of their account by displaying the following information on completion of a successful logon:

- Date and time of the previous successful logon; and,
- Details of any unsuccessful logon attempts since the last successful logon.

Recommended Tests:

Note: 1.4.3 is reported on as part of the annual information security review.

- Demonstrate critical business systems that process confidential/sensitive information within the Ministry (e.g., financial, personal information) are segregated appropriately by network zones, VLAN's.
- Demonstrate shared user identifiers are not used, as their use impedes investigation as to responsibility when multiple persons utilize the same credentials, and if for operational reasons there are shared identifiers an exemption must be obtained.
- Demonstrate successful and unsuccessful log on attempts are logged.
- Demonstrate that there is both a time maximum and minimum for logon attempts.

1.4.4 All employees must be issued a unique identifier for their use only and an approved authentication technique must be used to substantiate the identity of the user.

- a) Allocation of unique identifier**
- b) Authentication of identity**
- c) Shared user identifiers**

Purpose: *To ensure that access to information systems requires use of unique authenticated user identifiers.*

1.4.4 a) Allocation of unique identifier

Information Owners must ensure employees are issued unique user identifiers (user ids) for their use only, except as specified in 1.4.4 c). The documented and approved process for allocating and managing unique identifiers must include:

- A single point of contact to:
 - manage the assignment and issuance of user identifiers,
 - ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and,
 - record user status (e.g., employee, contractor);
- Identification of those individuals or positions authorized to request new user identifiers;
- Confirmation that the user has been informed of appropriate use policies;
- Automated linkages with the employee's management system (i.e., CHIPS) to identify transfers, terminations and extended leave actions to initiate the suspension or cancellation of user identifiers;
- Linkages with contract management offices and/or contract managers to identify and maintain the status of identifiers issued to contractors; and,
- Conducting annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

1.4.4 b) Authentication of identity

Information Owners must ensure that user identifiers are authenticated by an approved authentication mechanism.

User identifiers authenticated by means other than a password must use a mechanism approved by the Office of the Government Chief Information Officer.

1.4.4 c) Shared user identifiers

In exceptional circumstances, where there is a clear business benefit identified by the Information Owner or Information Custodian, the use of a positional user identifier for a group of users or a specific job can be used, provided:

- Positional user identifiers are not used for privileged users; and,
- The Supervisor responsible for the position using the positional user identifier:
 - Maintains a record of the name of the individual, the user identifier, and the start and end date of use, and,
 - Deactivates the user identifier when not in use by requesting a password reset.

Guidelines:

Processes for issuing and managing information system user identifiers should be coordinated with those used for issuing and managing other identification credentials (e.g., building passes, user identifiers for telecommunications services provided to an individual).

Recommended Tests:

Note: 1.4.4 is not reported on as part of the annual information security review.

- Demonstrate annual reviews of all user identifiers conducted.
- Demonstrate notices of employee change received by user administrators within 5 working days.

1.4.5 A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.
a) Enforcing quality password rules

Purpose: *To support the operating system access control policy through use of password management systems to enforce the password standard.*

1.4.5 a) Enforcing quality password rules

Information Owners and Information Custodians must ensure password management systems:

- Enforce the use of individual user identifiers and passwords;
- Support selection and change of passwords using the Complex Password Standard (see 1.3.1);
- Enforce change of temporary passwords at first logon and after password reset by an Administrator;
- Enforce regular user password change, including advance warning of impending expiry;
- Prevent re-use of passwords for a specified number of times;
- Prevent passwords from being viewed on-screen;
- Store password files separately from application system data;
- Ensure password management systems are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in protected (e.g., encrypted) form.

The password management system standard for government systems requires that users must be:

- Prevented from re-using the same password within 12 months; and,
- Provided with notification at least 10 days before their password will need to be changed.

Authority and Exceptions:

- Exception granted to RACF due to technical product limitations.
- Exemptions may be approved under specific criteria for non-expiring password usage. The Non-Expiring Password Acceptance Form is available from SSBC Client Resource Centre.

Recommended Tests:

Note: 1.4.5 is reported on as part of the annual information security review.

- Demonstrate systems not integrated with government's Active Directory (IDIR/BCeID authentication) need to determine if they are compliant with password integrity.
- Demonstrate passwords are not stored in clear text.
- Demonstrate systems found not compliant due to technical product limitations request an OCIO Policy / IM/IT Standards exemption record as evidence.
- Demonstrate user identifiers are authenticated by an approved authentication mechanism.

1.4.6 Use of system utility programs must be restricted and tightly controlled.
--

a) Restriction and control of system utility programs
--

Purpose: *To restrict and tightly control the use of utility programs, which may be used to override system and application controls.*

1.4.6 a) Restriction and control of system utility programs

Information Owners and Information Custodians must limit use of system utility programs by:

- Defining and documenting authorization levels;
- Restricting the number of users with access to system utility programs;
- Annually reviewing the status of users with permissions to use system utility programs;
- Ensuring that the use of system utilities maintains segregation of duties;
- Requiring a secure logon process to be used to access system utilities;
- Ensuring that all system utility programs are identified and usage logged;
- Segregating system utilities from application software where possible; and,
- Removing or disabling unnecessary and obsolete system utilities and system software.

Guidelines:

Use of system utility programs should be limited to privileged users. Use of system privileges should require use of multiple factors of authentication.

Recommended Tests:

Note: 1.4.6 is reported on as part of the annual information security review.

- Demonstrate regular reviews of users authorized to access system utility programs.
- Demonstrate the segregation of duties for system utilities.
- Demonstrate logs are maintained and regularly reviewed for system utility programs.

1.4.7 Inactive sessions must be shut down after a defined period of inactivity.
--

a) Session time-out

Purpose: *To ensure unattended information system sessions are automatically terminated.*

1.4.7 a) Session time-out

Information Owners and Information Custodians must define and implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity.

Government information systems must have session time-outs managed by operating system access, application or government infrastructure controls.

Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity commensurate with the:

- Risks related to the security zone;
- Classification of the information being handled; and,
- Risks related to the use of the equipment by multiple users.

The session must be terminated or require re-authentication after a period of no more than 15 minutes of inactivity.

Recommended Tests:

Note: 1.4.7 is not reported on as part of the annual information security review.

- Demonstrate the maximum period of inactivity set to 15 minutes or less.

1.4.8 Restrictions on connection times must be used to provide additional security for high value applications.
--

a) Limiting access hours

b) Limiting connection duration
--

Purpose: *To limit opportunities for inappropriate and unauthorized access to high value applications by restricting access hours and connection duration.*

1.4.8 a) Limiting access hours

Information Owners and Information Custodians must restrict access hours for high value applications.

Restricting operating hours includes:

- Limiting access to pre-determined times (e.g., when Ministry support employees are available); and,
- Establishing restrictions for access from high risk public or external locations which are outside the control of the Ministry.

1.4.8 b) Limiting connection duration

Information Owners and Information Custodians must limit the duration of connection times for high value applications. Restricting connection duration includes:

- Limiting session length; and,
- Requiring re-authentication of the user when a session has been inactive for a pre-defined period of time.

Recommended Tests:

Note: 1.4.8 is not reported on as part of the annual information security review.

1.4.9 Access control must be maintained for program source libraries. a) Protection of program source libraries
--

Purpose: *To protect information systems from unauthorized access or modification.*

1.4.9 a) Protection of program source libraries

Information Owners and Information Custodians must implement procedures to control access to program source code for information systems to ensure that:

- Program source code is isolated and stored separately from operational information systems;
- Privileged users' access is defined and monitored;
- A change control process is implemented to manage updating of program source libraries and associated items;
- Program source code contained on any media must be protected; and,
- Accesses and changes to program source libraries are logged.

Recommended Tests:

Note: 1.4.9 is reported on as part of the annual information security review.

- Demonstrate that source code is not kept on production systems.
- Demonstrate that access to source code libraries is controlled and logged (e.g., reports from software development tools on code check-in and check-out).
- Demonstrate program source code is stored separately from operation information systems.
- Demonstrate program source code and program source libraries are managed according to established procedures.
- Demonstrate that access to all program source libraries is logged and regularly reviewed.



DATABASE SECURITY STANDARD FOR INFORMATION PROTECTION

Information Security Branch

Office of the Chief Information Officer | Province of BC

Document Version 1.0

Published: April 4, 2018

Replaces: None

Introduction

This document contains standards for the protection of confidential, personal, and sensitive, information in databases (or “database management systems”). This Standard was developed in collaboration with ministries, endorsed by the Architecture and Standards Review Board, and approved by the Government Chief Information Officer.

Applicability

This Standard applies to database systems used for BC Government services, and will establish the baseline security controls for a secure database system.

This Standard identifies a minimum set of database system security controls. Privacy Impact Assessments (PIA) and Security Threat and Risk Assessments (STRA) may identify additional database security requirements.

Compliance Schedule

A compliance schedule will be developed in cooperation with the ministries, endorsed by the Architecture and Standards Review Board and approved by the Government Chief Information Officer.

For new database systems:

Controls in the standard are requirements for the procurement and/or implementation of new database systems. Where a new database system cannot reasonably be made compliant with this Standard but does not pose an unacceptable security risk and does not contravene Office of the Chief Information Officer (OCIO) strategic objectives, then an exemption may be requested through the OCIO.

For existing database systems:

Upon review, existing database systems may be found to pose unacceptable security risks. An existing database system must be brought into compliance with this Standard if it poses an unacceptable security risk. For existing database systems which do not pose an unacceptable security risk, ministries are encouraged to weigh resourcing of retroactive compliance efforts against resourcing other applicable, compensating, security controls.

Glossary

Critical (system) - Any IM/IT service, system, or infrastructure component that is deemed necessary by the SYSTEM OWNER to deliver a MISSION CRITICAL, or BUSINESS PRIORITY function, is a critical system for the purposes of this Standard.

Data Custodian – Person accountable for operational policy, definitions, rules, standards, structure, content, use and disposal for data under their responsibility.

Data Steward – Assumes some responsibilities of Data Custodian, but is not accountable for the data.

Database system(s) - A collection of organized information in a regular structure, in a machine-readable format accessible by a computer. Also: "Database Management System (DBMS)" or simply "database".

Environment - A term describing the setting where a part of the software lifecycle occurs, i.e. Development Environment, Testing Environment, Production Environment, etc.

Information - Data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision making.

Least privilege - A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

MISO - Ministry Information Security Officer : The single point of contact for information security issues and related concerns in the ministry. For more information about the MISO role, refer to [Link](#). For a list of all MISOs, refer to this [Link](#).

MPO - Ministry Privacy Officer: The single point of contact for privacy issues and related concerns in the Ministry. For more information about MPOs role, refer to this link. For a list of all MPOs, refer to MPO Directory.

OCIO - Office of the Chief Information Officer (OCIO) leads strategy, policy and standards for telecommunications, information technology, and the management of the IM/IT investment portfolio for the Province.

PIA - Privacy Impact Assessment, an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Production Database - Information that is persistently stored and used to conduct business processes. It must be accurate, documented and managed on an on-going basis to ensure its value to the organization.

Reasonable - Fair and moderate, not excessive, to a degree dictated by sensible evaluation of the factors impacting a decision.

Segregation of duties - The concept of sharing responsibilities for processes across more than one party. Segregation of duties reduces opportunity for fraud or malicious use by ensuring that there are checks in place for the conduct of critical operations. For example, segregation of duties can be applied to prevent fraud by making the party who reviews database use logs unable to modify those logs.

Service Owner - the Single Point of Contact who is accountable for all aspects of a service throughout the service life cycle.

Service Provider - a person or an organization retained under contract to perform services for the Government of British Columbia.

STRA - Security Threat Risk Assessment, a tool for understanding the various threats to IT systems, determining the level of risk these systems are exposed to, and recommending the appropriate level of protection.

Suspicious or abnormal activities - Defined by the Information Owner and Information Custodians, and are activities that for one reason or another are unusual and may indicate fraud or unauthorized access.

Note to Readers

This Standard is ordered to follow a typical system development life cycle, from initiation to disposition of a database system.

Terminology

The term “MUST” is defined as an absolute requirement of the specification. “SHOULD” means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications must be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the ADM of the information owner. For the purposes of this Standard “information owner” is defined in the Province’s Information Security Policy.

Standard/Controls:**Database System Planning, Acquisition & Requirements**

1. Ministries and Service Owners must identify information security requirements for new database systems or enhancements to existing database systems. These information security requirements must include confidentiality, availability, integrity and access requirements.
2. Ministries and Service Owners must manage security risks related to production databases.
3. Ministries and Service Owners must ensure that data in production databases is classified from a security perspective and protected based on that security classification.
4. Ministries must identify critical production databases. Ministries must ensure that a tested Disaster Recovery Plan and skilled resources are in place to be able to recover from a disruptive event that has an unacceptable impact to critical production databases.
5. Ministries and Service Owners must work with Ministry Privacy Officer(s) to ensure that reasonable security controls are in place to protect personally identifiable information within databases.
6. Ministries and Service Owners must determine the use of encryption for data in transit and at rest based on the classification of the database information and the risk of unauthorized access.

-
7. Responsibilities must be separated so that no single person or team is entirely responsible for operations of production databases and security measures, controls, and management.
 8. Formal user authorization process must be in place for granting and revoking access to production databases as defined by business requirements.
 9. Ministries and Service Owners must ensure that employees accessing production databases have completed information security and privacy training.
 10. Ministries and Service Owners must ensure that production databases' environments are isolated from non-production environments.
 11. Use of production data in non-production environments is only permitted based on business needs with appropriate security controls in place.
 12. Service Providers and Contractors accessing information within databases must comply with non-disclosure agreements (NDAs) and contracts governing their service provision.

Design, Development & Testing

13. Where reasonable, Ministries and Service Owners must ensure that production databases are configured to capture, record and alert on key data and database activities including, but not limited to:
 - view access to confidential or personal information;
 - data manipulation activities (e.g. insert, delete & change);
 - security activities (e.g. creation/deletion of users);
 - high-risk database activities (e.g. turn audit on/off); and
 - suspicious or abnormal activities.
14. Production databases requiring password authentication must utilize authentication lookup against approved BC Government authentication services (i.e. BCeID and IDIR) system. An exemption must be requested when this authentication is not possible.
15. Ministries and Service Owners must conduct regular database vulnerability assessments to identify, analyze and manage security risks related to critical and high risk database vulnerabilities.

-
16. Ministries and Service Owners must develop, document, maintain and implement security operating procedures and responsibilities for production databases.
 17. Ministries and Service Owners must ensure changes to database systems follow the organization's Change Management processes, including changes being tested and authorized before implementation in production systems.
 18. Ministries, Service Owners and Service Providers must ensure that a tested up to date Disaster Recovery Plan (DRP) and skilled resources are in place to meet business objectives.

Implementation, Operations & Disposition

19. Service Providers and Service Owners must develop and maintain documentation for production databases that is necessary for ongoing support/operations and future changes/upgrades.
20. Ministries and Service Providers must apply database patches on a regular and timely basis commensurate with the criticality of the database.
21. Copy or transfer of bulk data in production databases outside production databases and outside current operating procedures must be formally documented by the Ministry and restricted to specific business situations.
22. The Ministry and Service Owners must monitor and audit production databases to ensure privileged database users maintain appropriate database and access management controls including segregation of duties.
23. A formal review of users and their access permissions to databases containing production data must be performed by the Ministry or Service Owner on an annual basis.

CRYPTOGRAPHIC STANDARDS FOR INFORMATION PROTECTION

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● Collaboration ● Innovation

Document Version 1.7

Replaces: Version 1.6

Cryptographic Standards for Information Protection

Table of Contents

Document Control.....	3
Introduction.....	5
Applicability	5
Compliance Schedule.....	5
Notes to users.....	6
Terminology.....	6
Shared Services BC (SSBC) Support for Cryptographic Standards.....	6
Topics Not Included.....	6
1. ALGORITHMS AND KEY SIZES.....	7
1.1 Public Key Algorithm.....	7
1.2 Block Cipher Algorithm	8
1.3 Hashing Algorithms.....	9
2. DIGITAL CERTIFICATES.....	10
2.1 Multi-factor Authentication	10
2.2 Issuance of User Certificates	12
2.3 Issuance of Server Certificates.....	14
2.4 Certificate Status Checking.....	16
2.5 Multi-use SSL Certificates.....	18
3. INFORMATION IN TRANSIT	20
3.1 Web Protocol	20
3.2 SSH (for Administration Purposes)	23
3.3 File Transfer Protocol with Security.....	25
3.4 Web Service SOAP Security	27
4. INFORMATION AT REST	29
4.1 Windows Full Disk Encryption	29
4.2 Windows File Encryption	31
4.3 USB Flash Drives	33
4.4 Backup Data.....	35
4.5 Extracted Data on Portable Media	37
4.6 Document Signing	39
4.7 Portable External Hard Drives.....	41
4.8 OS X Full Disk Encryption.....	43
5. MESSAGING	45
5.1 Email.....	45
APPENDICES	47
APPENDIX A: Compliance Schedule for Web Service SOAP Security	47
APPENDIX B: Compliance Schedule for Cryptographic Standards	48

DOCUMENT CONTROL

Date	Author	Version	Change Reference
Oct 9, 2008	Lee & Walker	DRAFT	Initial draft presented to ASRB
Dec 11, 2008	Lee & Walker	DRAFT	Final DRAFT endorsed by ASRB
Dec 23 2008	Lee & Walker	1.0	Approved by CIO
June 9, 2009	Lee & Walker	1.1	Update
July 8, 2010	Lee & Walker	1.2	Update
Aug 12, 2011	Lee & Walker	1.3	Update
Aug 19, 2012	Lee & Walker	1.4	Update
Jan 02, 2015	R. Walker	1.5	Additions, Updates & Maintenance
Dec 19, 2016	R. Walker	1.6	Multi-Use Digital Certificates & Maintenance
Feb 28, 2017	R. Walker	1.7	Issuing Authority for User Certificates

Version 1.7 (Feb 2017) highlights:

- REVISED: Section 2.2 Issuance of User Certificates

Version 1.6 (Nov 2016) highlights:

- NEW: Section 2.5 Multi-Use Digital Certificates
- VALIDATED: URL's

Version 1.5 (Mar 2015) highlights:

- REVISED: Section 3.1 Web Protocol
- UPDATES: All Sections, verified URL's.
- NEW: Section 4.8 Whole disk encryption for Macs
- REVISED: Front Cover Refreshed

Version 1.4 (Aug 2012) highlights:

- NEW: Chapter 1: Algorithms and Key Sizes
- REMOVED: (Old) Section 1.4 Length of Public Keys.
- REVISED: Section 3.3 File Transfer Protocol with Security.
- REVISED: Section 4.3 USB Flash Drives.

Version 1.3 (Aug 2011) highlights:

- NEW: Section 3.7 Portable External Hard Drives.
- REVISED: Section 1.5 Certificate Status Checking (removed some guidance).
- REVISED: Some wording changes for improved clarity.
- Some formatting improvements.

Version 1.2 (July 2010) highlights: (Cont'd)

- NEW: Section 1.5 Certificate Status Checking.
- REVISED: Section 1.3 Issuance of Server Certificates.
 - The standard has been reworded for improved clarity – the scope & intent are unchanged
 - The context has been reworded for improved clarity around applicability.
- All references to WTS have been changes to Shared Services BC.

The “**Changed:**” date reflects only changes thought to be of possible material impact.

Version 1.1 (June 2009) highlights:

- New: Appendix A: Compliance Schedule for Web Service SOAP Security.
- Moved to: Appendix B: Compliance Schedule for Cryptographic Standards.
- Minor changes to parameters prescribed in SOAP security specification.

Version 1.0 (Jan. 2009) highlights:

- Approved and Published

INTRODUCTION

This document contains a family of standards for the cryptographic protection of information. These are standards of the Government of British Columbia, approved by the Chief Information Officer (CIO).

APPLICABILITY

For many of standards in this document the question of applicability rests with the information owner. In these cases, applicability may be determined by the following steps:

Step 1: A set of business requirements is gathered and documented.

Step 2: A Privacy Impact Assessment is performed and documented.

Step 3: A Security and Threat Risk Assessment is performed and documented.

Step 4: Based on a review of 1-3 above, determine if cryptographic controls are required.

Step 5: If controls are required use this family of standards for further planning.

Each standard in this family provides further information on applicability.

COMPLIANCE SCHEDULE

The compliance schedule for these standards is located in the Appendix.

NOTES TO USERS

Terminology

The term “MUST” is defined as an absolute requirement of the specification.

“SHOULD” (when in upper case) means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications must be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the ADM of the information owner. For the purposes of these standards “information owner” is defined in the Province’s Information Security Policy.

Shared Services BC (SSBC) Support for Cryptographic Standards

This document assumes the availability of certain products and services from Shared Services BC (SSBC). SSBC will be providing support for the January 2009 Cryptographic Standards as the infrastructure evolves and will be balancing service enhancements with the need to carefully manage rates. Full compliance (as per Compliance Timelines section) across SSBC services will be a multi-year undertaking.

Topics Not Included

There are some subject areas which, for various reasons, could not be accommodated in the time available to develop these standards. At some future point, more topics will be addressed.

Some topics NOT currently covered:

- Cryptographic controls applied by database management systems for the purposes of protecting back-up data
- Virtual private network systems
- Server side disk encryption: Windows, Linux, MVS, UNIX.
- Cryptographic controls for Directory Access Protocol
- Protection of activation data for digital certificate request fulfilment

1. ALGORITHMS AND KEY SIZES	Effective: 2012-08-19 Reviewed: 2014-08-19
<u>1.1 Public Key Algorithm</u>	Changed: 2012-08-19

Purpose

This standard provides guidance on controls used for the protection of information and systems.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Algorithms and key size are critical aspects of cryptographic information protection. This section is intended to help implementers make informed decisions in the absence of specific directives elsewhere in this family of standards.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where public key cryptography is being applied in circumstances not covered by any other standard in this family, implementers **MUST** use one of the following choices:

1. RSA based cryptography
 - 1.1 The RSA key size **MUST** be no less than 1024 bits.
 - 1.2 The RSA key size **SHOULD** be 2048 bits.
2. Elliptic curve cryptography (ECC).
 - 2.1 ECC curve and key parameters **MUST** be selected from among those recommended in FIPS 186-3, APPENDIX D.
 - 2.2 The bit length of ' n ' specified in Table D-1 **MUST** be no less than 224.

Additional Guidance

SHOULD and **MUST** are defined in the section **NOTES TO USERS**.

References

NIST - FIPS 186-4 Digital Signature Standard (DSS) (APPENDIX D)
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

1. ALGORITHMS AND KEY SIZES	Effective: 2012-08-19 Reviewed: 2014-08-19
<u>1.2 Block Cipher Algorithm</u>	Changed: 2012-08-19

Purpose

This standard provides guidance on controls used for the protection of information and systems.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Algorithms and key size are critical aspects of cryptographic information protection. This section is intended to help implementers make informed decisions in the absence of specific directives elsewhere in this family of standards.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where a block cypher is being applied in circumstances not covered by any other standard in this family, implementers **MUST** use the following:

1. Advanced Encryption Standard (AES), NIST - FIPS 197
 - 1.1 The AES key size **MUST** be no less than 256 bits.

Additional Guidance

None.

References

NIST - FIPS 197 Advanced Encryption Standard (AES)
<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

1. ALGORITHMS AND KEY SIZES	Effective: 2012-08-19 Reviewed: 2014-08-19
<u>1.3 Hashing Algorithms</u>	Changed: 2012-08-19

Purpose

This standard provides guidance on controls used for the protection of information and systems.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Hash functions, also known as message digest functions, can play a critical role in protection of information. This section is intended to help implementers make informed decisions in the absence of specific directives elsewhere in this family of standards.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where a hash function is being applied in circumstances not covered by any other standard in this family, implementers SHOULD use the following:

1. Secure Hash Algorithm as specified in NIST - FIPS PUB 180-3
 - 1.2 The block size MUST be no less than 256 bits (i.e. SHA-256).

Additional Guidance

SHOULD and MUST are defined in the section **NOTES TO USERS**.

Where the technology is available legacy systems should migrate to SHA-256.

References

NIST - FIPS PUB 180-3 Secure Hash Standard (SHS)
<http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4>

2. DIGITAL CERTIFICATES	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>2.1 Multi-factor Authentication</u>	Changed: 2012-08-19

Purpose

This section specifies the government's standard for user multi-factor authentication. Multi-factor authentication lowers the risk of unauthorized access to protected government information assets.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

One aspect of protecting information is ensuring that only authorized persons can access it. User ID and password are commonly used for this purpose. The effectiveness of user authentication depends on the confidence in the identity of the person requesting access. Confidence can be improved by using multi-factor authentication (MFA). MFA is an effective means to ensure the authenticity of the person making such a request.

By specifying an X.509 digital certificate protected on a tamper-resistant device this standard mandates a uniform, standardized approach for two-factor authentication. Solutions requiring more than two factors may be granted as an exception by the OCIO. The main target of this standard is government information systems. However, the approach taken will enable benefits in other areas. Digital certificates can be used for controlling building access, performing digital signatures and supporting non-repudiation.

This standard applies where there is a need for multi-factor authentication for system users.

The need for multi-factor authentication is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where multi-factor authentication is required it **MUST** be implemented as follows:

One authentication factor **MUST** be based on a X.509 certificate stored on a tamper-resistant device that meets FIPS 140-2 Level 2 and is issued under a government approved registration process. The tamper-proof device **MUST** also meet the requirements of ISO 7816-1

Identification Cards – Integrated Circuit Cards Part 2: Cards with Contacts – Dimensions and Locations of Contacts.

The X.509 certificate attributes MUST conform to the Identity Information Management Standards for the province.

Additional Guidance

- The issuance of user certificates is covered in Section 2.2.
- The above authentication standard should be integrated with WEB single sign-on, VPN, email, and other standard government services.

References

OCIO – Information Security Policy 6.6.1 Network security configuration control
OCIO – Information Security Policy 6.9.1 Electronic commerce
OCIO – Information Security Policy 6.10.3 Protection of information system logging facilities
OCIO – Information Security Policy 7.1.1 Access control policy management
OCIO – Information Security Policy 7.2.2 Allocation and use of system privileges
OCIO – Information Security Policy 7.5.4 Control of system utility programs
OCIO – Information Security Policy 8.3 Cryptographic controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Liberty Alliance – Strong Authentication

http://www.projectliberty.org/liberty/strategic_initiatives/strong_authentication

Multi-factor authentication methods will be compatible with the province's recommendations for a building access solution. The following identification card (i.e. smartcard) standards have been included for reference:

- ISO 7810
- ISO 7811
- ISO 7812
- ISO 7813
- ISO 7816
- ISO 4909
- NIST - FIPS 201-1

NIST - FIPS 140-2 Security Requirements for Cryptographic Modules

<http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

2. DIGITAL CERTIFICATES	Effective: 2009-01-14 Reviewed: 2017-02-29
<u>2.2 Issuance of User Certificates</u>	Changed: 2017-02-29

Purpose

This standard specifies how digital certificates (for end-users) will be issued by Province of British Columbia to employees, business partners and optionally to the broader public sector.

This standard helps protect the Province's information and technology assets. The desired outcome is to preserve the privacy of sensitive information and to position the Province's IM/IT infrastructure to meet evolving business needs.

This standard provides specific guidance for the application of security policy.

Context

In early 2016 a Digital Certificate Service (DCS) was launched by the Office of the Government Chief Information Officer (OCIO). This new service contains all the public key infrastructure, policies and procedures needed for issuing and managing digital certificates for end-users. It provides foundational infrastructure to further secure the Province's information assets and communications.

A Digital certificate is a credential that is issued by an authority in accordance with a strictly defined process, much like a driver's license. The issuing authority is responsible for the policies and procedures required to ensure the integrity of the system. The type of certificates issued by the DCS are for end-users, such as employees or partners of the Province.

The requirement to apply cryptographic controls (e.g. user certificate) is determined by a Privacy Impact Assessment, a Security Threat and Risk Assessment, or the business requirements.

Scope

This standard applies to end-user certificates issued in the name of (i.e. representing) the Province of British Columbia. This standard does not apply to, or restrict, user certificates issued by partners (e.g. other governments, external agencies) to the Province for accessing external services.

Standard

- 1.1 The Digital Certificate Service of the OCIO is the exclusive issuing authority for end-user certificates bearing the name "Province of British Columbia".
- 1.2 User certificates bearing the name "Province of British Columbia" issued by or on behalf of the Province MUST be obtained through the Digital Certificate Service.
- 1.3 Subscribers MUST follow the certificate management policies and procedures set forth by the OCIO DCS.

Additional Guidance

- A subscriber is a program area, ministry or agency that adopts the use of user certificates.
- This standard will be updated as new or additional certificate authorities are authorized.

References

OCIO – Information Security Policy 8.3 Cryptographic controls

OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509-201210-I/en>

2. DIGITAL CERTIFICATES	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>2.3 Issuance of Server Certificates</u>	Changed: 2011-08-11

Purpose

This section specifies the government's standard for the issuance of digital certificates for server systems. This standard provides a unifying direction for all ministries and agencies that require digital certificates.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Digital certificates play an important role in the protection of information. This standard specifies the way X.509 certificates for servers will be issued.

A server is a system or device connected to a network that offers services to clients. While providing a service, a server may itself request a service from another system, thus acting in the role of client. If a certificate is being used to identify a system (in either roles of server or client) then this standard applies.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

The following requirement governs all parties whose internet domain name is managed by Shared Services BC:

Where an X.509 certificate is required for system authentication it **MUST** be obtained through Shared Services BC.

Additional Guidance

- None.

References

OCIO – Information Security Policy 8.3 Cryptographic controls

OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509-201210-I/en>

2. DIGITAL CERTIFICATES	Effective: 2010-01-26 Reviewed: 2014-08-19
<u>2.4 Certificate Status Checking</u>	Changed: 2010-04-30

Purpose

This section specifies government requirements for checking the status of X.509 digital certificates.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

X.509 certificates play a role in providing assurance for the authenticity of an assertion. Assertions are such things as: a digital signature on a contract or the user-ID used for a logon request. Every certificate has an associated status. A certificate's status is important. For example if a certificate's status is "REVOKED" that certificate is no longer valid as a proof of identity for signing a document or logging on to a system.

This standard specifies the steps that should be taken to check the status of a X.509 certificate. It is intended to cover all uses of X.509 certificates, e.g. signing and authentication.

Standard

When an X.509 certificate is used to make an assertion the status of the certificate SHOULD be checked, subject to availability, by one of the following methods:

1. Online Certificate Status Protocol (OCSP) as defined in RFC 2560.
2. Certificate Revocation List (CRL) as defined in RFC 5280.

Additional Guidance

- Shared Services BC will provide certificate status information, via OCSP for certificates issued by the Public Works and Government Services Canada (PWGSC) Certificate Authority of the Government of Canada.
- Government systems validating PWGSC certificates should obtain certificate status information from Shared Services BC.

References

OCIO – Information Security Policy 8.3 Cryptographic controls

OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
<http://tools.ietf.org/html/rfc6277>

IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List
(CRL) Profile
<http://tools.ietf.org/html/rfc6818>

2. DIGITAL CERTIFICATES	Effective: 2016-11-17 Reviewed: TBD
<u>2.5 Multi-use SSL Certificates</u>	Changed: 2016-11-17

Purpose

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure and better positioned to support future business needs.

Context

SSL Certificates are important because they underpin citizen trust in government's online services. Certificates are also important because they help ensure the trustworthy administration of the Province's data centers.

The Province employs many SSL certificates, some of which are of a type known as "multi-use".

Multi-use certificates involve wider, more serious security considerations than regular SSL certificates. For example, multi-use certificates can be used to establish trust outside of the original context. Consequently, they can inconspicuously introduce risks to other provincial services and users (i.e. beyond the original business area). Because this risk is inconspicuous, it undermines risk management and good security practice.

Therefore, multi-use certificates should only be used after a careful security analysis. The term "multi-use" encompasses 2 kinds of SSL certificates: wildcard and multi-domain. (Multi-domain certificates are also known as SAN or UC certificates.)

This standard sets conditions on multi-use SSL certificates for domains owned or operated on behalf of the Province of BC.

Standard

Part 1 of 2: **Multi-domain certificates**

Part 1 applies to Multi-domain X.509 certificates that DO NOT contain a hostname with an embedded '' character.*

- 1.1 New deployments of multi-domain certificates **MUST** be appraised in a Security Threat and Risk Assessment (STRA).

Part 2 of 2: **Wildcard certificates**

A wildcard certificate is any kind of X.509 certificate containing a hostname (for server identity) that has an embedded wildcard character '' in it.*

- 2.1 The use of *.gov.bc.ca is prohibited. *(cont'd)*

- 2.2 Existing certificates using “*.gov.bc.ca” MUST be removed from service upon reaching their expiry date.
 - a. In special circumstances an OCIO exemption may be applied for.
- 2.1 New deployments of wildcard certificates MUST be appraised in a Security Threat and Risk Assessment (STRA).
 - a. The STRA MUST address risks related to using a wildcard certificate.
 - b. Common risks, as well as business risks, must be considered.
- 2.3 A wildcard application form must be submitted for review.
Note: this form is available from the OCIO's Information Security Branch.
 - a. The STRA must accompany the application form.
 - b. The requesting Ministry must agree to implement the STRA's recommendations for mitigating common risks. (i.e. risks impacting other parties)
 - c. The business owner must acknowledge the business risks identified in the STRA.

Additional Guidance

- 1. A certificate that has been appraised under an existing, valid STRA (as per 1.1 or 2.3) does not require a new STRA for the routine renewal of that certificate.
- 2. This standard does not prohibit wildcard certificates for sub-domains.
- 3. The term “**business owner**” refers to the Assistant Deputy Minister of the business line.
- 4. The term “**risk**” means the potential for loss.
- 5. A **business risk** is a potential for loss that is limited to the line of business.
- 6. A **common risk** is a potential for loss that extends beyond the line of business.
- 7. For this standard, the definition of a **Wildcard** certificate is any type of certificate (i.e. including multi-domain certificates) that contains one or more hostnames (for server identity) that contain a wildcard character ‘*’.
- 8. **Multi-domain** certificates are also known as: Unified Communications Certificates (UC) and Subject Alternate Name Certificates (SAN).

References

OCIO – Information Security Policy 8.3 Cryptographic controls

OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Understanding Multi-Use Certificates

<http://wiki.apache.org/httpd/UnderstandingMultiUseSSLCertificates>

RFC 2818 HTTP Over TLS

<https://tools.ietf.org/html/rfc2818>

3. INFORMATION IN TRANSIT	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>3.1 Web Protocol</u>	Changed: 2015-05-28

Purpose

This standard provides direction for all ministries and agencies having requirements for secure web communications based on hypertext transfer protocol (HTTP). It specifies the standard for protecting personal and sensitive information communicated over the HTTP protocol.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens and will make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Over the past decade various industry standards have been proposed to help secure web (i.e. HTTP) communications. As time passed and shortcomings emerged these standards have been improved. This government-wide standard is meant to ensure that the most current, reliable protocols are being used to protect information.

This standard applies where there is a need to apply cryptographic controls to secure HTTP.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required for HTTP, they MUST be implemented as follows:

PART 1 of 3: CERTIFICATES

- 1.1 An X.509 certificate MUST be used for performing server authentication.
- 1.2 Public facing sites using HTTPS SHOULD use an Extended Validation (EV) Certificate.

PART 2 of 3: TRANSPORT LAYER

- 2.1. HTTPS MUST be used with TLS 1.1 or above - subject to availability.
- 2.2. Web servers supporting TLS 1.1 or above MUST disable ALL versions of SSL.
- 2.3. Sites not supporting TLS 1.1 or above MUST decommission SSL by Jan. 1, 2016.

PART 3 of 3: ENCRYPTION

- 3.1. HTTPS MUST be used with AES.
- 3.2. The AES key length MUST not be less than 128 bits.
- 3.3. Web servers supporting HTTPS MUST disable RC4.
- 3.4. Perfect forward secrecy SHOULD be used where available.

Additional Guidance

- Regular scans for HTTPS vulnerabilities are recommended.
- Support for forward secrecy is recommended where higher security is required and performance requirements allow.
- The software implementing HTTPS should be patched on a timely basis.
- Server certificates must conform to sections 2.3 and 1.1 of this standard.
- All reasonable measures should be taken to protect the server's private key.
- For applications requiring high assurance, client side certificates for mutual authentication should be used.
- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

References

OCIO – Information Security Policy 6.6.1 Secured path
OCIO – Information Security Policy 7.4.2 Remote access to government networks or services
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls
OCIO – Information Security Policy 7.7.2 Teleworking security

Wikipedia – Forward Secrecy

http://en.wikipedia.org/wiki/Forward_secrecy

IETF – The Transport Layer Security (TLS) Protocol Version 1.2

<http://tools.ietf.org/html/rfc5246>

Industry forum for EV certificates

<http://www.cabforum.org/>

Guidelines for the Issuance and Management of Extended Validation Certificates

<https://cabforum.org/documents/>

IETF – Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T – Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509-201210-I/en>

NIST – FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

3. INFORMATION IN TRANSIT	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>3.2 SSH (for Administration Purposes)</u>	Changed: 2009-01-14

Purpose

This standard provides direction for all ministries and agencies responsible for the administration of remote systems and network attached devices. It specifies the standard for protecting sensitive telecommunications by providing confidentiality and authentication.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

All devices and systems attached to a network must be administered. Because of the distributed nature of networks the administration function is usually performed remotely. This raises a need for authentication and information protection.

This standard applies in situations where a command line is used for performing remote administration of a system or device.

Standard

Command line administration of remote systems and devices **MUST** be done by employing SSH Version 2 or higher. The encryption algorithm used **MUST** be AES with a minimum key length of 256 bits. Mutual authentication **MUST** be used between user and server.

Additional Guidance

- Server certificates must conform to sections 2.3 and 1.1 of this standard.
- All reasonable measures should be taken to protect the server's private key.
- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

References

OCIO – Information Security Policy 6.6.1 Secured path

OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls

IETF – The Secure Shell (SSH) Authentication Protocol

<http://tools.ietf.org/html/rfc4252>

IETF – Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T – Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509-201210-I/en>

NIST – FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

3. INFORMATION IN TRANSIT	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>3.3 File Transfer Protocol with Security</u>	Changed: 2012-08-19

Purpose

This standard provides direction for all ministries and agencies having requirements for secure file transfer based on File Transfer Protocol (FTP). It specifies the standard for protecting personal and sensitive information communicated via FTP by providing confidentiality and authentication.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

File Transfer Protocol (FTP) is a commonly used utility for transferring files between computers. The FTP protocol is insecure. Over the past decade various standards have been proposed to improve the security of FTP. This standard is meant to help ensure that FTP is deployed securely.

This standard applies where there is a need to apply cryptographic controls to secure FTP.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

FTP-based file transfers that require cryptographic controls **MUST** employ one of the following two choices:

1. SSH File Transfer Protocol Version 2 (commonly referred to as SFTP)
 - 1.1. The encryption algorithm used **MUST** be AES with a minimum key length of 256 bits.
 - 1.2. If server certificates are used, they **SHOULD** conform to section 2.3 of this standard.
 - 1.3. If client certificates are used, they **SHOULD** conform to sections 2.1 and 2.2 of this standard.
 - 1.4. If data with an information security classification **MEDIUM** or above will be handled, both client and server authentication based on public key cryptography **MUST** be used.
2. FTP over TLS/SSL (commonly referred to as FTPS)

- 2.1 The encryption algorithm used **MUST** be AES with a minimum key length of 256 bits.
- 2.2 Both control and data channels **MUST** be encrypted.
- 2.3 Server certificates **MUST** conform to section 2.3 of this standard.
- 2.4 Where client certificates are used, they **MUST** conform to section 2.1 and 2.2 of this standard.
- 2.5 If data with an information security classification **MEDIUM** or above will be handled, both client and server authentication based on public key cryptography **MUST** be used.

Additional Guidance

- Anonymous login should be disabled on the server side.
- All reasonable measures should be taken to protect the server's private key.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 6.6.1 Secured path
OCIO – Information Security Policy 6.8.1 Electronic information exchange
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls

IETF - File Transfer Protocol
<http://tools.ietf.org/html/rfc959>

NIST - FIPS 197 Advanced Encryption Standard (AES)
<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

IETF - SSH File Transfer Protocol
<http://tools.ietf.org/html/draft-ietf-secsh-filexfer-13>

IETF - The Secure Shell (SSH) Protocol Architecture
<http://tools.ietf.org/html/rfc4251>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
<https://www.itu.int/rec/T-REC-X.509-201210-I/en>

3. INFORMATION IN TRANSIT	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>3.4 Web Service SOAP Security</u>	Changed: 2009-06-09

Purpose

This standard provides direction for all ministries and agencies using or planning to use secure SOAP Web Service interactions. It specifies the standard for protecting personal and sensitive information communicated via SOAP messages by providing confidentiality and authentication.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

SOAP, formerly known as the Simple Object Access Protocol, is a protocol for exchanging structured information between computer systems. The main purpose of the SOAP specification is to define structured message exchange. The specification does not attempt to define a security model. Instead SOAP foresees “security” as being defined elsewhere. This approach, while justifiable, has resulted in a host of deployments using incompatible security solutions. This hampers interoperability.

By specifying a single security model this specification aims to:

- Better position us to support business objectives
- Increase security robustness
- Reduce non-essential complexity
- Improve interoperability

This standard applies where there is a need to apply cryptographic controls to secure SOAP with Web Services.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they **MUST** be implemented as follows:

SOAP Web services that require cryptographic controls **MUST** be compliant with WS-I Basic Security Profile 1.0 with the following provisions:

Transport layer implementations must comply with one of the following two choices:

- TLS implementations **SHOULD** implement TLS_RSA_WITH_AES_128_CBC_SHA
- SSL implementations **SHOULD** implement SSL_RSA_WITH_AES_128_CBC_SHA

Cryptographic modules implementing the above **SHOULD** be validated to FIPS 140-2.

Additional Guidance

- A SOAP message supporting the authentication of a user would be an example use case for this standard.

References

OCIO – Information Security Policy 6.6.1 Secured path

OCIO – Information Security Policy 6.8.1 Electronic information exchange

OCIO – Information Security Policy 6.9.2 On-line transaction security

OCIO – Information Security Policy 6.9.3 Internet site security

OCIO – Information Security Policy 7.2.3 Authentication credential management

OCIO – Information Security Policy 8.1.1 Security requirements of information systems

WS-I - Security Challenges, Threats and Countermeasures

<http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf>

WS-I - Basic Security Profile

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

4. INFORMATION AT REST	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>4.1 Windows Full Disk Encryption</u>	Changed: 2009-01-14

Purpose

This standard provides direction for all ministries and agencies responsible for information stored in hard drives on computer systems. It specifies the standard for protecting information on hard drives.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Access to information stored on computers is largely dependent on controls provided by the operating system. This information is stored on a hard disk. In some circumstances, operating systems protections can be bypassed leaving the hard disk vulnerable. This raises a need for another level of protection for the drive itself. This protection can be achieved by using hard drive encryption. Even if a computer is lost or stolen encryption provides protection against unauthorized disclosure of information.

The integrity of cryptographic systems depends on preserving secrecy. Thus, it follows that cryptographic keys must be managed securely throughout their lifetime. The typical events in the lifecycle of a cryptographic key include (but are not limited to): generation, distribution, storage, access (e.g. backup, archive, recovery) and destruction.

This standard pertains to the encryption of logical disk volumes under the control of Microsoft Windows Vista or above running on non-server systems.

Standard

Hard disks under the control of Windows Vista or its successors **MUST** be encrypted. Cryptographic operations **MUST** be performed with Trusted Platform Module (TPM) 1.2 or higher compliant hardware. The encryption algorithm used **MUST** be AES with a minimum key length of 256 bits.

Key management **MUST** be documented and performed in accordance with the following requirements:

- Key Storage
 - The master encryption key shall reside within the TPM hardware and **MUST** not leave the TPM for the master key's service life.
- Key Recovery

- The key recovery password MUST be protected by at least two levels of independent access controls and limited to an audience of personnel authorized for the task of information recovery.
- Logging Transactions
 - All access to the key recovery passwords MUST be recorded in an audit trail.

Information owners MUST ensure that information custodians produce documentation for the above.

Additional Guidance

- Strong protection measures should be taken to protect the key recovery password.
- The master encryption key should reside in the TPM at all times.
- Shared Services BC has chosen to meet the above requirements with a service offering based on BitLocker.
- BitLocker should be deployed in advanced mode with hibernation.
- The BIOS boot order should not be changeable by the user.

References

OCIO – Information Security Policy 5.2.5 Equipment security controls

OCIO – Information Security Policy 6.7.1 Portable storage devices – mandatory controls

OCIO – Information Security Policy 6.7.3 Media handling procedures

OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Microsoft - BitLocker Drive Encryption

<http://social.TechNet.microsoft.com/Search/en-US?query=bitlocker&ac=3>

Trusted Platform Module (TPM) Specifications

<https://www.trustedcomputinggroup.org/specs/TPM/>

NIST - FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

4. INFORMATION AT REST	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>4.2 Windows File Encryption</u>	Changed: 2009-01-14

Purpose

This section specifies the standard for protecting information stored in individual files.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Within a program area business circumstances will arise under which it is necessary to take additional steps to protect individual files. This protection can be achieved through the use of file encryption.

This standard applies where there is a need to apply cryptographic controls to secure files under the control of a Windows operating system. These controls supplement the basic operating system controls and are intended for end users to apply on a discretionary basis.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

Discretionary file encryption controls MUST be provided by Shared Services BC as a single government-wide solution meeting the following requirements:

- The solution MUST integrate seamlessly with existing government PKI and infrastructure.
- The solution MUST provide individual user and group permission-based access controls.
- The solution MUST be capable of remote administration.
- Files MUST be encrypted with AES 256.
- The file encryption process MUST be automated and transparent to the end-user.
- The solution MUST integrate seamlessly and securely with all currently supported Windows files system types.

Key management MUST be documented and performed in accordance with the following requirements:

- Key Recovery

- File encryption keys MUST be recoverable.
- Key Backup
 - The file encryption key MUST be backed up on a central server.
 - When a file encryption key is backed up the key MUST be encrypted.
 - A documented process MUST be established to access the backed up keys.
- Logging Transactions
 - All access to the backed-up key MUST be recorded in an audit trail.

Information owners MUST ensure that information custodians produce documentation for the above.

Additional Guidance

- Client certificates must conform to section 1.1 of this standard: Multi-factor Authentication and to section 1.2: Issuance of User Certificates.
- All reasonable measures should be taken to protect PKI private keys.
- Extra care should be taken to protect recovery keys.

References

OCIO – Information Security Policy 6.7.4 Protection of systems documentation
OCIO – Information Security Policy 8.3.1 Acceptable use of cryptography
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Microsoft – Using Encrypted File System (EFS)
<http://technet.microsoft.com/en-us/library/bb457116.aspx>

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
<https://www.itu.int/rec/T-REC-X.509>

NIST - FIPS 197 Advanced Encryption Standard (AES)
<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

4. INFORMATION AT REST	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>4.3 USB Flash Drives</u>	Changed: 2012-08-19

Purpose

This section specifies the standard for protecting information stored on USB flash drives.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Business circumstances arise under which it is necessary to store files on a USB flash drive (i.e., a form of portable storage device). Steps must be taken to protect files stored on this device. This protection can be achieved by using file encryption.

This standard applies to all USB flash drives used to store government information.

Standard

Only USB flash drives obtained through Shared Services BC may be used for storing government information.

Part 1 of 2: MANDATORY REQUIREMENTS, for all flash drives:

- 1.1 USB flash drives **MUST** be certified by NIST to FIPS 140-2 Level 2 or above.
- 1.2 All user writeable partitions on the drive **MUST** be fully encrypted.
- 1.3 The encryption algorithm **MUST** be AES, i.e. FIPS 192.
- 1.4 The AES encryption key **MUST** be a **MINIMUM** of 256 bits long.
- 1.5 The device **MUST** lockdown after consecutive failed login attempts.
- 1.6 The number of failed login attempts **MUST** not exceed 12.
- 1.7 The USB flash drive **MUST** enforce the use of a complex password.

Part 2 of 2: CONDITIONAL REQUIREMENTS, applicable when handling information with a security classification of “HIGH”.

- 2.1 USB flash drives **MUST** be certified by NIST to FIPS 140-2 Level 3.

Additional Guidance

- None

References

OCIO – Information Security Policy 6.7.1 Portable storage devices – mandatory controls
OCIO – Information Security Policy 6.7.3 Media handling procedures
OCIO – Information Security Policy 7.3.1 Selection of Passwords
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Microsoft – Using Encrypted File System (EFS)

<http://technet.microsoft.com/en-us/library/bb457116.aspx>

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509>

NIST - FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

NIST - FIPS 140-2 Security Requirements for Cryptographic Modules

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

4. INFORMATION AT REST	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>4.4 Backup Data</u>	Changed: 2009-01-14

Purpose

This standard provides direction for ministries and agencies responsible for performing the systematic backup of data. It specifies the standard for the protection of information stored on external backup media.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

The term “backup” refers to the process of making copies of data to protect against data loss.

Backup systems vary widely across different hardware platforms, operating environments and vendor solutions. This specification provides a system-independent set of requirements.

This standard applies where there is a need to apply cryptographic controls to secure information that is systematically being backed up to external media.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

Backup data that requires encryption MUST be encrypted with AES.

A minimum key length of 256 bits MUST be used.

Key management MUST be documented and performed in accordance with the following requirements:

- Key Recovery
 - Encryption keys MUST be recoverable.
- Logging Transactions
 - All access to the backed up data MUST be recorded in an audit trail.

Information owners MUST ensure that information custodians produce documentation for the above.

Additional Guidance

- Periodic verification of backed up data should be performed.
- External media may be interpreted to mean a sibling disk system.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media

OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - The Secure Shell (SSH) Authentication Protocol

<http://tools.ietf.org/html/rfc4252>

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509>

NIST - FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

4. INFORMATION AT REST	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>4.5 Extracted Data on Portable Media</u>	Changed: 2009-01-14

Purpose

This standard provides direction for ministries and agencies performing the extraction of data onto portable media.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

The term “extracted data” normally refers to a data set comprised of selected records extracted from a source data set. Extracted data is used for decision support, research, agency reporting or other business related purpose. For this specification “extracted data” is meant to include any computer file being transferred from a source system onto portable media. A common scenario is where extracted data is stored on portable media for transfer between parties, a provider and consumers.

There are foreseeable risks associated with handling and transporting extracted data on portable media. These risks require that measures be taken to protect confidentiality.

Section 7.7.1 of the B.C. Government’s Information Security Policy (ISP) requires the “encryption of stored data” when placed on a portable storage device.

This standard specifies how the ISP Section 7.7.1 encryption requirement is to be implemented.

Standard

Extracted data placed on portable media **MUST** be encrypted with AES.

A minimum key length of 256 bits **MUST** be used.

Key management **MUST** be documented and performed in accordance with the following requirements:

- Key Exchange
 - Encryption keys **MUST** be handled in a manner that does not put extracted data at risk of disclosure when the media is lost or misplaced.
 - Encryption keys **MUST** never be transported together with the media.

Additional Guidance

- Key exchange using public key infrastructure is recommended.

- Information temporarily stored on a portable storage device should be transferred to the government network as soon as practicable and then deleted from the portable storage device.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - The Secure Shell (SSH) Authentication Protocol

<http://tools.ietf.org/html/rfc4252>

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<https://www.itu.int/rec/T-REC-X.509>

NIST - FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

4. INFORMATION AT REST	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>4.6 Document Signing</u>	Changed: 2009-01-14

Purpose

This standard provides direction for ministries and agencies with requirements for the digital signing of documents.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Digital signatures ensure the authenticity of the author and the integrity of the content of a document.

This standard applies where there is a need to apply cryptographic controls to ensure the authenticity and integrity of a document.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

The signing of digital documents MUST be based on X.509 certificates. The signing key pair MUST be distinct from the encryption key pair. The signing key MUST not be recoverable.

When the signing key is lost, stolen or compromised, the user MUST report the incident so that the key can be revoked.

When a user's signing key is revoked and the user is eligible to possess a key, a new key MUST be generated for the user.

When a user is no longer eligible to possess a signing key due to the employment status change, the manager MUST report the change so that the key can be revoked.

Additional Guidance

- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
<https://www.itu.int/rec/T-REC-X.509>

NIST - FIPS 186 DSS Digital Signature Standard
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

4. INFORMATION AT REST	Effective: 2011-04-25 Reviewed: 2014-08-19
<u>4.7 Portable External Hard Drives</u>	Changed: 2011-04-25

Purpose

This section specifies the encryption standard for protecting information stored on portable external hard disk drives and portable external solid state drives (SSD).

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Business circumstances arise under which it is necessary to store files on a portable, external hard disk drive. The Information Security Policy requires that steps be taken to protect files stored on portable storage devices regardless of the security classification of the stored information. The use of encryption is a requirement under this policy.

This standard applies to portable, external hard disk drives and solid state drives used to store information for or on behalf of the Province of British Columbia.

StandardPart 1 of 2: MINIMUM REQUIREMENTS:

- 1.1 All information stored on a drive **MUST** be encrypted using AES encryption.
- 1.2 The AES encryption key **MUST** be a **MINIMUM** of 256 bits long.
- 1.3 All user writeable partitions on the drive **MUST** be fully encrypted.

Part 2 of 2: CONDITIONAL REQUIREMENTS, when handling information with a security classification of "HIGH":

- 2.1 All information stored on a drive **MUST** be encrypted using an AES hardware encryption module that conforms to **FIPS 140-2 Level 3**. (This clause overrides clause 1.1.)
- 2.2 The cryptographic modules implementing FIPS 140-2 Level 3 **MUST** have a FIPS 140-2 Validation Certificate.

Additional Guidance

- Part 1 permits software based encryption, part 2 allows only hardware based encryption.
- See references for a list of validated FIPS 140-2 cryptographic modules.

- A drive or drive array that is stationary by design (i.e. designed to be used at a single, fixed, secure location) and is thus not at risk of being lost, misplaced or stolen is not considered portable.
- Where an STRA is deemed necessary for the safe use of a portable storage device, the STRA should assess the need for a credential recovery process to ensure ongoing user/owner access to the information stored on the device.
- A credential can be in a form of a key or a password with or without a username.
- Where a credential recovery process is required it should incorporate the following:
 1. The credential should be handled and protected like a secret.
 2. Access to and distribution of the credential should be limited to authorized persons based on a need-to-know principle.
 3. The information owner (e.g. ministry) should not need to depend on the device user for the recovery of the credential, unless the risk is deemed acceptable by the owner.

References

1. Information Security Classification Framework
<http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-classification-framework>
2. NIST Cryptographic Module Validation Program
<http://csrc.nist.gov/groups/STM/cmvp/index.html>
3. Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>
4. NIST - FIPS 197 Advanced Encryption Standard (AES)
<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
5. NIST - FIPS 140-2 Security Requirements for Cryptographic Modules
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
6. OCIO - Information Security Policy Home Page
<http://www.cio.gov.bc.ca/information-security-policy/>
7. OCIO – Information Security Policy 6.7.1 Portable storage devices – Mandatory Controls
8. OCIO – Information Security Policy 6.7.3 Media Handling Procedures
9. OCIO – Information Security Policy 7.7.1 Mobile Computing & Teleworking – Controls
10. OCIO – Information Security Policy 11.1.6 Regulation of Cryptographic Controls

4. INFORMATION AT REST	Effective: 2015-05-28 Reviewed: 2015-05-28
<u>4.8 OS X Full Disk Encryption</u>	Changed: 2015-05-28

Purpose

This standard specifies the configuration to be used for protect information residing on Apple Mac computers.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure and better positioned to meet future business needs.

Context

The ability to protect information stored on computer hard drives depends on controls provided by the operating system. In some circumstances, operating systems controls can be bypassed leaving the information on the hard disk vulnerable to disclosure. This raises the need for an additional means of information protection. Whole disk encryption provides this protection. It is the best defense against unauthorized disclosure in the event a computer is lost or stolen.

Whole disk encryption depends on a password and secret key. If the user-password is forgotten or the secret key becomes corrupted the information on the disk may be unrecoverable. Thus, it is necessary to ensure the information on an encrypted disk is recoverable, independent of the end user.

To protect information, cryptographic keys must be managed securely throughout their lifetime. The typical events in the lifecycle of a cryptographic key include (but are not limited to): generation, distribution, storage, access (e.g. backup, archive, recovery) and destruction.

This standard is not mandatory for stationary OS X computers located in secure facilities.

Standard**Part 1 of 2: Encryption**

Objective: To protect the information on a lost or stolen device from unauthorized exposure.

1. OSX versions below release 10.7 SHOULD be upgraded to 10.7 or above.
2. Hard disks under the control of OSX 10.7 or above MUST be encrypted.
3. The disk encryption algorithm used MUST be XTS-AES-128 (per: NIST 800-38E).

(Continued...)

Part 2 of 2: Institutional recovery

Objective: To provide the Province with the ability to recover encrypted information.

1. Encrypted drive contents **MUST** be recoverable independently of the end-user.
2. A recovery key (or master password or equivalent) **MUST** be kept in escrow.
3. Escrowed keys **MUST** reside on infrastructure controlled by the Province of BC.
4. Access to escrowed keys **MUST** be recorded in an audit trail.

Additional Guidance

- Apple's FileVault 2 meets the requirements of this standard.

References

OCIO – Information Security Policy 5.2.5 Equipment security controls
OCIO – Information Security Policy 6.7.1 Portable storage devices – mandatory controls
OCIO – Information Security Policy 6.7.3 Media handling procedures
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

NIST 800-38E: Recommendation for Block Cipher Modes of Operation:
The XTS-AES Mode for Confidentiality on Storage Devices
<http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf>

NIST - FIPS 197 Advanced Encryption Standard (AES)
<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

5. MESSAGING	Effective: 2009-01-14 Reviewed: 2014-08-19
<u>5.1 Email</u>	Changed: 2009-01-14

Purpose

This standard specifies the security controls for the protection and authenticity of email messages.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Many routine government business matters are conducted through email messaging. These messages may contain sensitive information. It is important to know, with confidence, that the sender identity is authentic. Furthermore, it is important to protect these messages while in transit. Industry standards have been developed for the authenticity and protection of email messages.

This standard applies where there is a need to apply cryptographic controls to secure email messages.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they **MUST** be implemented as follows:

The authentication, integrity, non-repudiation of origin and confidentiality of email messages **MUST** be protected by an S/MIME version 3.1 or above based solution.

Secure email solution for government **MUST** be provided by Shared Services BC as a centrally managed government-wide solution.

The solution **MUST** seamlessly integrate with the government's email messaging system, operating systems, and the government's public key infrastructure.

Certificates for digital signature and encryption **MUST** be distinct.

Additional Guidance

- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.
- SHOULD and MUST are defined in the section **NOTES TO USERS**.

References

OCIO – Information Security Policy 6.8.1 Electronic information exchange

OCIO – Information Security Policy 6.8.4 Exchanges of information – general requirements

OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls

IETF - S/MIME Version 3.1 Message Specification (RFC 3851)

<http://www.ietf.org/rfc/rfc3851.txt>

IETF - S/MIME Version 3.1 Certificate Handling (RFC 3850)

<http://www.ietf.org/rfc/rfc3850.txt>

IETF - X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities (RFC 4262)

<http://www.ietf.org/rfc/rfc4262.txt>

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

<http://tools.ietf.org/html/rfc4210>

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks

<http://www.itu.int/rec/T-REC-X.509>

NIST - FIPS 197 Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

APPENDICES

APPENDIX A: Compliance Schedule for Web Service SOAP Security

The following schedule has been developed in cooperation with the ministries, endorsed by the Architecture and Standards Review Board and approved by the government Chief Information Officer.

- 1) Shared service and inter-organizational¹ SOAP provider interfaces must be upgraded to comply with the standard and be released into production by December 10, 2010.
- 2) Shared service and inter-organizational SOAP consumer interfaces must be upgraded to comply with the standard no later than 12 months after the publication of the corresponding provider interface.
- 3) All new SOAP interfaces (provider and consumer²) to be released into production must comply with the standard starting from December 10, 2009.
- 4) Legacy SOAP interfaces (provider and consumer) not covered above should be brought into compliance on a best effort basis, unless they pose a security risk³ or collide with an OCIO objective.

¹ The term "inter-organizational" includes ministry-to-ministry, ministry-to-agency, ministry-to-service provider, etc.

² This is Subject to the availability of provider interfaces.

³ Interfaces that pose a security risk should be dealt with on a priority basis.

APPENDIX B: Compliance Schedule for Cryptographic Standards

The following schedule has been developed in cooperation with the ministries, endorsed by the Architecture and Standards Review Board and approved by the government Chief Information Officer.

Appendix B applies for all standards except Web Service SOAP Security. The compliance schedule for Web Service SOAP Security is covered in Appendix A.

For existing systems:

An existing system should be brought into compliance only if it poses an unacceptable security risk or if for some other reason non-compliance raises a tangible issue. Bringing existing systems into compliance simply for the sake of compliance is not advocated.

For new systems:

The standard should be factored in as a requirement for the procurement of new systems.

Where a new system cannot reasonably be made compliant and if that does not pose an unacceptable security risk and does not collide with OCIO strategic objectives then an exception may be obtained through the Office of the Government Chief Information Officer.