



Office of the Chief Information Officer
Ministry of Citizens' Services

Information Management / Information Technology Standards Manual

Last Updated:	2012-02
Version:	2.10

Document Security

The information security classification of this document has been established as **Low**. It has been specifically created and organized with the expectation of general availability to the public, but should be protected from unauthorized manipulation.

Terms of Use

The contents of this Information Management/Information Technology (IM/IT) Architecture and Standards Manual are expected to change as the evaluation, review and approval process of standards progresses, i.e., it should be considered a working document. The current version of this document will be posted on the website of the Office of Chief Information Officer (www.cio.gov.bc.ca).

Standards Compliance

The format of this document is based on templates provided by the Project Management Office, Ministry of Health, and adapted by Architecture and Standards, the Office of the Chief Information Officer, B.C. Ministry of Labour and Citizens' Services.

Full List of Changes to IM/IT A/S Manual

Date	Author	Vers.	Change Description
2007-08-17	Colin Stafford	-0.7	Initial drafts of document use for internal discussion and review purposes.
2007-09-21	Bel Zajic	1.0	Finalized, converted to PDF and sent for approval. Updated manual to reflect feedback in the approval process, finalized and converted to PDF.
2007-10-16	Bel Zajic	1.1	Updated hyperlink to information security policy.
2008-01-21	Colin Stafford, Darko Petrusic	1.2	Added Sections 1.1, 5.2, 5.6, 5.7, 6.6 to 6.10; refreshed 4.1, 5.1, 6.3, glossary; minor word-smithing, updating of links.
2008-03-11	Colin Stafford	1.3	Included feedback from Robert Walker, Information Security Branch (ISB); rewrote Sections 5.2, 6.10; confirmed URLs
2008-03-29	Colin Stafford	1.4	Revised introduction to reflect new CIO web page.
2008-04-10	Colin Stafford	1.5	Updated 5.5; incorporated additional feedback from ISB in Section 6; removed VoIP standard (6.9) at request of ISB.
2008-05-07	Lloyd Loisel	1.6	Added Preface to reflect Strategic Initiatives and Infrastructure.
2008-05-18	Colin Stafford	1.7	Updated IM/IT Policy Framework, web linkages; minor wordsmithing, reformatting; removed draft Preface.
2008-06-18	Colin Stafford	1.8	Changed 6.6 to Process Standard; removed draft Section 5.6; updated web linkages. Created version for government intranet use (Ver 1.8b).
2008-11-10	Jason Smeraka	1.9	Added: 5.8 N2N Security Standard
2008-12-08	Jason Smeraka	2.0	Added: 3.10 Raster Standard 5.9 Pharmanet WLAN Standard
2009-02	Jason Smeraka	2.1	IMIT AS Manual Annual Review Added: 3.5 - Date Time Standard (Revised) 5.9 - Govt-wide WLAN Standard (Supersedes 5.9 Pharmanet) 5.10 - WLAN Architecture 5.11 - STRA Standard for WLAN implementation 6.10 - Cryptographic Standards for Information Protection (NEW)

Date	Author	Vers.	Change Description
2009-06	Jason Smeraka	2.2	Updated: 6.10 Cryptographic –Appendix A: Implementation Schedule Added: Exemptions, Updates, Omissions – information on exemptions 4.3 Multi-Function ID Card Standard Obsolete: 3.1 Data Admin Standard 3.2 Data Management Roles/Responsibilities
2010-02	Jason Smeraka	2.3	Updated: 5.1 User Interface Standards and Guidelines...
2010-03	Bel Zajic	2.4	Updated: Web Link updates and general assessment
2010-05	Bel Zajic	2.5	Updated: 3.11 Open Data Physical Dataset Format Standard.
2010-09	Chris Lyons Patricia Wiebe Robert Walker	2.6	Updated: 6.10 Cryptographic Standards for Information Protection Added: 2.1 Development Standards for Information Systems and Services 4.4 Identity Assurance Standard 4.5 Evidence of Identity Standard 4.6 Electronic Credential and Authentication Standard 4.7 (Reserved) 4.8 Claims Information Standard 4.9 Claims Technology Standard 5.12 Unified Communication Federation Standard 5.13 Technical Architecture for Unified Communication Federation 6.11 Standard for Information Security Threat and Risk Assessment (STRA)
2010-11-05	Seanna McDonald	2.7	Added: 3.12 Physical Address and Geocoding Standards – Conceptual Model 5.9.1 Secure Wireless Local Area Network Connectivity Standard Supplement
2011-08-23	Seanna McDonald	2.8	Added: 6.10 Cryptographic Standards for Information Protection
2011-12-06	Wendy Fox-Jensen	2.9	Added: 3.13 ECM Content Metadata Standard
2012-02-01	Wendy Fox-Jensen	2.10	Added: 5.14 Tools for Collaboration with External Business Entities
2012-03-16	Wendy Fox-Jensen	2.10	Updated: 3.12 New URL for Physical Address and Geocoding Standards Conceptual Model

Table of Contents

INTRODUCTION	6
Purpose of the Document.....	6
Authority	6
Types of Standards.....	8
Format.....	9
Exemptions, Updates, Omissions, and Suggestions.....	9
Glossary	9
Contact	9
1.0 APPROPRIATE USE OF GOVERNMENT RESOURCES (CPPM 12.3.1).....	10
1.1 Use of Websense® for Internet Filtering.....	10
2.0 INFORMATION AND TECHNOLOGY PLANNING (CPPM 12.3.2).....	12
2.1 Development Standards for Information Systems and Services.....	12
3.0 INFORMATION MANAGEMENT (CPPM 12.3.3).....	14
3.1 Data Administration Standards	14
3.2 Data Management Roles and Responsibilities.....	16
3.3 Mailing and Delivery Address Data Standards.....	18
3.4 Standard for Developing Digital Data Specifications Standards Documents	20
3.5 BC Government IM/IT Display Date and Time Standard.....	22
3.6 Government IRM Glossary Standards and Procedures	24
3.7 Oracle® as Preferred Government Database Standard.....	26
3.8 Enterprise Document and Records Management	28
3.9 Aboriginal Administrative Data.....	30
3.10 Common Raster Cell Origin, Shape and Sizes Standard for the Government of BC	32
3.11 Open Data Physical Dataset Format Standard.....	34
3.12 Physical Address and Geocoding Standards – Conceptual Model	37
3.13 ECM - Content Metadata Standard.....	39
ADDITIONAL INFORMATION	42
4.0 IDENTITY MANAGEMENT (CPPM 12.3.4).....	43
4.1 Secure Electronic Transactions – OBSOLETE/SUPERSEDED	43
4.2 Single Identifier for Transacting with Government Electronically.....	45
4.3 Standard for Multi-Function Identity Card: Physical Characteristics and Graphical Topography.....	47
4.4 Identity Assurance Standard.....	50
4.5 Evidence of Identity Standard.....	52
4.6 Electronic Credential and Authentication Standard.....	54
4.8 Claims Information Standard.....	56
4.9 Claims Technology Standard.....	58
5.0 INFORMATION TECHNOLOGY MANAGEMENT (CPPM 12.3.5).....	60
5.1 User Interface Standards and Guidelines for the Internet.....	60
5.2 User Interface Standards and Guidelines for the Government Intranet.....	63
5.3 Wireless Internet Access and Wireless Hotspots	65
5.4 Connection of Multi-Function Devices (MFDs) to SPAN/BC Network.....	67
5.5 Use of webMethods® as Integration Broker Standard	70
5.6 SSBC Workstation Services Supported Hardware Products.....	72

5.7	SSBC Workstation Services Supported Software Products	74
5.8	Network to Network Connectivity	76
5.9	Technical Security Standard for Wireless Local Area Networks	79
5.9.1	Technical Security Standard for Wireless Local Area Networks - Supplement	82
5.10	High Level Architecture for Wireless Local Area Networks.....	85
5.11	Security Threat and Risk Analysis Standard for Implementing Wireless Local Area Networks	89
5.12	Unified Communication Federation Standard.....	99
5.13	Technical Architecture for Unified Communication Federation.....	101
5.14	Tools for Collaboration with External Business Entities.....	104
6.0	INFORMATION TECHNOLOGY SECURITY (CPPM 12.3.6).....	106
6.1	Use of Employee Desktop Computers as Servers	106
6.2	Web Traffic Filtering	108
6.3	Internet Filtering of Well Known Ports	110
6.4	Interim Standards for Information Systems Security and Network Connectivity.....	112
6.5	Use of Portable Storage Devices on Government-managed Personal Computers – OBSOLETE/SUPERSEDED.....	114
6.6	IT Asset Disposal.....	116
6.7	Password Standard	118
6.8	Use of Non-government Managed Laptops by Contractors.....	120
6.9	Data Encryption and Minimum Key Length Standards – OBSOLETE/SUPERSEDED... ..	122
6.10	Cryptographic Standards for Information Protection	124
6.11	Standard for Information Security Threat and Risk Assessment Methodology, Process and Assessment Tool.....	126
	APPENDIX A: GLOSSARY	130
	APPENDIX B: IM/IT STANDARDS CHANGE MANAGEMENT PROCESS.....	131
	APPENDIX C: STANDARDS ABSTRACT TEMPLATE	132
	APPENDIX D: ARCHITECTURE ABSTRACT TEMPLATE	133

INTRODUCTION

The Province of British Columbia (Province) is the custodian of extensive information holdings and relies upon its information assets for fiscal, policy and program delivery initiatives. The Office of the Chief Information Officer (OCIO) has adopted an Enterprise Architecture (EA) program which establishes a framework for managing information assets. The Enterprise Architecture program is intended to:

- ensure quality and safety of information,
- optimize value for money in IM/IT investments,
- enable business transformation, and
- maximize the ability to deal with change.

The publication of the IM/IT Architecture & Standards Manual supports the achievement of the EA program.

Purpose of the Document

The purpose of this document is to serve as an authoritative and practical compendium of existing and proposed IM/IT architectures and standards. Standards are established norms or requirements that help clarify, guide and control IM/IT processes and activities. They help create a common language with which systems people and business people can communicate about the relationship between business needs and technology solutions.

Every entry in this document is described by means of a consistent, searchable template that will:

- offer guidance in the applicability of each standard,
- supply contact information associated with each standard,
- report on the current validity of each standard, and;
- provide linkages to related documentation.

Authority

The IM/IT Architecture & Standards Manual is issued under the authority of the Government Chief Information Officer (GCIO). The CIO sets government direction and standards for IM/IT, guiding the development of a coordinated whole-of-government approach. The CIO works with ministries and their programs to achieve their service objectives while promoting corporate or government objectives.

The CIO is also responsible for IT components of the Province's *Core Policy and Procedures Manual* (CPPM). This manual contains government-wide policies for managing information, communications, material, transportation, contracts and expenses. It is located at: www.fin.gov.bc.ca/ocq/fmb/manuals/CPM.

Within the CPPM, the CIO is directly responsible for *Chapter 12 – Information Management and Technology Management Policies*.

The CIO maintains four manuals that support the current *CPPM* Chapter 12:

1. *Chapter 12 IM/IT Supplemental Manual*
(<http://www.cio.gov.bc.ca/local/cio/about/documents/cpm12.pdf>).
2. *Freedom of Information and Protection of Privacy Policy and Procedures Manual*
(http://www.cio.gov.bc.ca/cio/priv_leg).
3. *Information Security Policy*
(www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page).

The Policy Framework, shown below in Figure 1, shows how the various IM/IT responsibilities are related.



Figure 1 – IM/IT Policy Framework

In addition, there is a Risk Management Branch (RMB) publication entitled *Security Standards and Guidelines* that is referenced in the *Information Security Policy* document listed above. This RMB guidebook, which provides information for ministries that are developing a security management program, is located on the government intranet and requires an IDIR user id to access.

Also related to IM/IT Standards is the *Recorded Information Management Manual* (www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/rim_manual) which is maintained by the Information Access Office of the Ministry of Citizens' Services.

Types of Standards

Overview

In formal terms, a standard is an established, measurable, achievable and understandable statement or set of criteria that describes a desired level of performance against which actual performance can be compared. While a policy tells us what to do, a standard is a tool that allows us to measure, monitor and compare actual performance against a benchmark.

A standard must be applied across government to all IM/IT domains including data administration, applications, technical infrastructure, security and privacy.

There are four types of standards that have been designated by the OCIO:

1. **Technical Standard** – these are detailed, unique standards that have developed in response to government IM/IT policies. Technical standards are intended to be replicable, transferable, and adaptable across ministries and other government agencies. Examples of these include address data standards or specifications for a single identifier for transacting with government electronically.
2. **Product Standard** – an IM/IT product or specific technology oriented standard that facilitates the task of planning for enhancements and acquisitions within the government's broad information systems environment. As a definitive list of the numerous technologies either employed or under evaluation by Shared Services B.C., product standards are critical in establishing conformity, interoperability and interchangeability. Examples of these include a government-wide standard for document and record management, and the list of core products for government workstations.
3. **Process Standard** - an established, mandatory business practice that supports IM/IT projects and existing systems to improve the outcome, diminish risks, and increase reliability. Examples include the Privacy Impact Assessment template, or the Information Sharing Agreement template.
4. **Reference Standard** – an IM/IT industry standard (either a national or international formal or de facto standard) that has been adopted for use by the Province of B.C. A Reference Standard may be adopted either as stand-alone or as a precursor to a customized standard or policy document. Examples include the ISO 17799:2005 standard for information security management (on which the *Information Security Policy Manual* is based) or the 1024 bit RSA standard for public key encryption.

Format

The format of this manual reflects the Core Policies and Procedures Manual (CPPM) Chapter 12 policies which are posted on the Office of the Comptroller General website. For each section of Chapter 12, this IM/IT Architecture & Standards Manual identifies:

- the corresponding section of CPPM Chapter 12 policies,
- the name of the architecture or standard, a full description and where it is used,
- the authority behind the architecture or standard plus exceptions, metrics, enforcement and references to additional material in other documents or to key websites for the benefit of users, and
- additional information explaining, for example, governance and any known customization necessary to meet business needs of ministries.

Exemptions, Updates, Omissions, and Suggestions

The IM/IT Architecture & Standards Manual is reviewed annually, and as required to ensure accuracy and applicability by the Architecture and Standards Branch (ASB), OCIO. Suggested modifications are welcome.

The OCIO recognizes that “one size does not fit all” on all architectures and standards. There will be cases where published architectures and standards either do not meet specific business needs or may be inconsistent with emerging national, international and industry standards. The ASB must be consulted well before any procurement or implementation decision is made if published standards may not be appropriate for business needs.

Exemptions from existing architectures and standards can be requested. A guide to the exemption process along with the exemption form can be found on our website at:

<http://www.cio.gov.bc.ca/cio/standards/asdlc/exemptions.page>.

Glossary

The OCIO is developing a Consolidated IM/IT Glossary (see Figure 1 above) that will be made available through the OCIO website (www.cio.gov.bc.ca). At this time an Information Resource Management (IRM) Glossary is available on the OCIO website, although its target audience is primarily data administration.

This IM/IT Architecture & Standards Manual includes a working Glossary plus references to other known terminology directories, including the IRM Glossary.

Contact

For inquiries regarding the IM/IT Architecture & Standards Manual, please contact:

Executive Director, Architecture and Standards Branch, OCIO

Phone: 250-952-6970 Email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2006-11-15 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
	Type: Product Standard
1.0 APPROPRIATE USE OF GOVERNMENT RESOURCES (CPPM 12.3.1)	
1.1 Use of Websense® for Internet Filtering	
Keywords:	

Description of Standard

This standard defines the use of Websense® for Internet use filtering and tracking within ministries and government agencies.

Where to Apply This Standard

The Websense® solution has been implemented by SSBC in order to provide a monitoring capability for appropriate business web content between the Internet and the government network.

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.1, *Appropriate Use of Government Information*. Specifically, the policy states that users of government information technology must not:

- obtain files from unauthorized or questionable non-government sources (e.g., racist material, pornography, file swapping sites);
- access Internet sites that might bring the public service into disrepute or harm government's reputation, such as those that carry offensive material;
- access radio stations or video clips (typically referred to as "streaming" audio or video) over the Internet, unless the access is work-related and authorized;
- download non-work related files, such as Freeware, Shareware, movie or music files;

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. Policies related to the appropriate use of government resources can be found within the Core Policy and Procedures Manual:
www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1231
and in the IM/IT Chapter 12 Supplemental Manual at:
www.cio.gov.bc.ca/local/cio/about/documents/cpm12.pdf.
2. The *Websense® Exemption Request* form is located on an internal BC Government website. For more information please contact:
Corporate Planning & Policy
Information Security Branch, OCIO
email: CITZCIOSecurity@gov.bc.ca

Additional Information

The Information Security Branch, OCIO, is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Information Security Branch, OCIO
email: CITZCIOSecurity@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2010-06-17 Scheduled Review: Annual Last Updated: 2010-07-06 Last Reviewed: 2010-07-06
	Type: Non-Technical
Office of the Chief Information Officer Province of British Columbia	
2.0 INFORMATION AND TECHNOLOGY PLANNING (CPPM 12.3.2)	
2.1 Development Standards for Information Systems and Services	
Keywords: Development, Procurement, Software, Services	

Description of Standard

This family of standards governs specific areas of activity coincident with developing or procuring an information system or service. Topics include: requirements management.

The strategic aim of this standard is to support the Government's goals through improvements to capabilities in the area of systems and services development.

Where to Apply This Standard

This standard applies when an information system or service is being developed, modified or procured by, or on behalf of, the Province of British Columbia.

Authority and Exemptions

This standard has been issued by the GCIO in accordance with CPPM Chapter 12.3.2, Information and Technology Planning.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

Compliance is based on self regulation in conjunction with the principles of risk management.

Shared Services B.C. Compliance

There is no infrastructure required from SSBC to support this standard.

Terms and Definitions

Terms and definitions are defined within the standard.

References

1. Core Policy:
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm
2. Development Standards for Information Systems and Services:
www.cio.gov.bc.ca/local/cio/standards/documents/standards/development_standards.pdf

Additional Information

The OCIO is the owner of this standard.

Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 1998-02-12 Scheduled Review: Annual Last Updated: 2009-01 Last Reviewed: 2009-01
	Type: Technical Standard
3.0 INFORMATION MANAGEMENT (CPPM 12.3.3)	
3.1 Data Administration Standards	
Keywords:	

Description of Standard

This set of standards arose from a set of recommendations generated by the Data Administration Framework Task Force (DAFTF), the predecessor of the Data Administration Forum (DAF) under the auspices of the Government Chief Information Officer (CIO).

The Data Administration Standards were established to set minimum criteria for data management that apply to all data within government. The intent is to encourage all ministries to follow best practices in information management, while making a minimum set of standards mandatory. For example, this document specifies that each ministry should have “data element naming standards” and describes in general what they are. However, it may not actually specify detailed standards, because some ministries may not have the support infrastructure developed that could action those standards *at that level of detail*.

Where to Apply This Standard

The standards outlined in this document are meant to:

- Assist any government ministry or agency that is launching or overseeing a Data Administration function. DAF expects that those ministries with existing Data Administration functions will already have data administration standards in place that, at minimum, meet those outlined here.
- Serve as a reference to all internal (government) and external (contracted) resources involved in the management of data or the development and/or maintenance of systems which act on government data.

Authority and Exemptions

DAF published these standards with the consent of the Advisory Council on Information Management (ACIM). Although the standards identified in this document have been specifically focused on the baseline needs of government, there is no standard for modeling at this time. However, modeling should be undertaken for all systems development projects to ensure that the activities the business performs are well understood.

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

The standards outlined in this document apply to all ministries. The intention of DAF is to advertise and promote these standards as being mandatory in all government ministries. That said, DAF does not currently have the resources to enforce standards compliance. To begin to effectively manage information, a ministry should implement these standards as a minimum, through a ministry data administration function.

Terms and Definitions

There are a number of data administration terms and definitions in this standards document related to:

- the minimum requirements for data model metadata; and
- the basic components of a data model including entity type, attribute type and relationship type.

These are included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in References.

References

1. The location of the Data Administration Standards document is at:
www.cio.gov.bc.ca/local/cio/standards/documents/standards/data_administration_standards.pdf.
2. The B.C. Government Information Resource Management Glossary is currently under review.

Additional Information

The Data Administration Forum is the owner of these standards. Its website is located at www.cio.gov.bc.ca/cio/standards/daf.page.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2010-11-18 Scheduled Review: Annual Last Updated: Last Reviewed: 2010-09
	Type: Process Standard
3.0 Information Management (CPPM 12.3.3)	
3.2 Data Management Roles and Responsibilities	
Keywords:	

Description of Standard

The purpose of this standard is to define the roles and responsibilities necessary for data management within government.

This standard was developed by the Standards Subcommittee of the Data Architecture Advisory Committee (DAAC) under the auspices of the Government Chief Information Officer (CIO).

Where to Apply This Standard

The standards outlined in this document are meant to:

- Assist any government ministry or agency that is launching or overseeing a Data Administration function.
- Serves as a reference to all internal (government) and external (contracted) resources involved in the management of data or the development or maintenance of systems which act on government data. In particular, these guidelines can be used by Data Administrators as part of the education and communication process for improving information management in their organization.

Authority and Exemptions

DAAC published these standards with the consent of the Advisory Council on Information Management (ACIM). This standard strives to establish common names for the roles, and a common set of responsibilities where no roles exist or where the names for roles vary across ministries.

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

The standards outlined in this document apply to all ministries. The intention of DAAC is to advertise and promote this standard as being mandatory in all government ministries. That said DAAC does not currently have the resources to enforce standards compliance. To begin to effectively manage information, a ministry should implement this standard as a minimum, through a ministry data administration function.

Terms and Definitions

This standard contains a *Data Management Roles & Responsibilities Matrix* that summarizes the role definitions and gives a general assessment of some existing issues related to those roles within government.

In addition, many of the data administration terms and definitions in this standard are included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in References.

References

3. The location of the Data Management Roles and Responsibilities document is at: www.cio.gov.bc.ca/local/cio/standards/documents/standards/data_mgt_roles_responsibilities_guidelines.pdf.
4. The B.C. Government Information Resource Management Glossary is currently under review.

Additional Information

The Data Architecture Advisory Committee is the owner of these standards. Its website is located at www.cio.gov.bc.ca/cio/standards/daac.page.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2000-11 Scheduled Review: Annual Last Updated: 2009-01 Last Reviewed: 2009-01
	Type: Technical Standard
3.0 Information Management (CPPM 12.3.3)	
3.3 Mailing and Delivery Address Data Standards	
Keywords:	

Description of Standard

These standards define the metadata about mailing and delivery addresses, i.e., the elements of an address (storage structure standards) and the metadata for ways in which an address is structured for output or presentation.

Additional data requirements such as those for tracking historical changes to addresses, for physical implementation (such as how to store accent characters) and for business area specific needs, are not identified.

Where to Apply This Standard

These standards are meant to assist any B.C. government ministry or agency capture, maintain and validate mailing and delivery addresses.

Authority and Exceptions

The Data Administration Forum (DAF) published these standards with the consent of the Advisory Council on Information Management (ACIM). Mailing and delivery address data standards ensure that address information is consistent and shareable within the B.C. Government.

Metrics and Exemptions

The standards outlined in this document apply to all ministries. DAF's intention is to advertise and promote these standards as being mandatory in all government ministries. That said, DAF does not currently have the resources to enforce standards compliance. To begin to effectively manage information, a ministry should implement these standards as a minimum, through a ministry data administration function.

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.

Terms and Definitions

There are a number of data administration terms and definitions in this document related to mailing and delivery addresses. These are included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in References.

References

1. The location of the Mailing and Delivery Address Data Standards document is at: http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/address_data_standards.pdf.
2. The B.C. Government Information Resource Management Glossary is currently under review.
3. The Integrated Land Management Bureau (formerly Geographic Data BC) is mandated to define data standards for *physical addresses* and to capture and maintain physical address data for the whole of the B.C. government. It is located at: ilmbwww.gov.bc.ca.

Additional Information

The Data Administration Forum is the owner of these standards. Its website is located at www.cio.gov.bc.ca/cio/standards/daac.page.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 1998-02-05 Scheduled Review: Annual Last Updated: Last Reviewed:
	Type: Technical Standard
3.0 Information Management (CPPM 12.3.3)	
3.4 Standard for Developing Digital Data Specifications Standards Documents	
Keywords:	

Description of Standard

The purpose of this standard is to define the digital form and structure of resource inventory digital data as managed by the Province of B.C. It defines:

- standards for describing thematic content
- standards for physical data specification
- geo-referencing standards
- quality assurance guidelines and
- recommendations for cartographic representation of the data.

This standard also recommends or prescribes methods for digital data capture, quality assurance and graphic data representation, as well as project metadata related to digital capture.

Where to Apply This Standard

These standards are technical in nature, and are intended for a specialist audience of persons compiling, managing and using a digital resource inventory dataset.

Consequently, they will be useful to:

- ministry staff or contractors involved in collecting resource inventory data;
- managers charged with overseeing data-collection projects;
- custodians and data administrators maintaining resource inventory datasets; and
- end-users seeking to apply resource inventory data to resource management and land-use issues.

Authority and Exemptions

These standards are part of a series of related documents produced by the Resources Inventory Standards Committee (RISC), Integrated Land Management Bureau (ILMB). They are intended to ensure BC government agencies are providing resource information that meets recognized standards for quality and consistency.

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

This set of standards will be used by contractors and government staff involved directly with collecting resource inventory data for specific technical guidance on the form and structure of the data sets they prepare. Managers of such data-collection projects will use these standards to evaluate whether resource inventory projects have been properly conducted.

Terms and Definitions

There are a large number of technical data definitions and geo-referencing terminology in this document. Unfortunately, there is no immediately accessible Glossary attached to the set of standards. For further information, contact the ILMB, listed below.

References

1. The location of the Standard for Developing Digital Data Specification Standards Document is: <http://ilmbwww.gov.bc.ca/risc/pubs/other/standardfordevelopdigitaldata>.
2. The Integrated Land Management Bureau (Resource Information Standards Committee) is located at: <http://ilmbwww.gov.bc.ca/risc>.

Additional Information

The ILMB (Resource Information Standards Committee) is the owner of this government-wide standard. Its website is shown above in References.

The ILMB has also produced two internal documents to provide information on the corporate data model framework and guidance on modeling techniques and standards specific to data models. These documents are as follows:

1. *Corporate Data Model Framework*:
<http://ilmbwww.gov.bc.ca/risc/pubs/other/corporateframework>.
2. *Corporate Data Modeling Standards and Guidelines*:
<http://ilmbwww.gov.bc.ca/risc/pubs/other/corporatestandards>.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 1997-12-19 Scheduled Review: Annual Last Updated: 2009-01-28 Last Reviewed: 2009-01
	Type: Technical Standard
3.0 Information Management (CPPM 12.3.3)	
3.5 BC Government IM/IT Display Date and Time Standard	
Keywords: standard, date, time, display, alphanumeric, format	

Description of Standard

This standard outlines the acceptable IM/IT display date and time formats for use by the Government of British Columbia. The majority of these standards are based on the principles of the International Standards Organization (ISO) 8601 standard with 3 exceptions for alphanumeric date formats (5.10. to 5.12.). These exceptions have been included as standards with the understanding that their use is limited to specific purposes as outlined in the document and, that they may be removed in future versions. The principles of ISO 8601 include:

- Dates and times **MUST** be unambiguous and use 4-digit years and 24 hr clock
- Both dates and times **SHOULD** be displayed in order of significance
- Both dates and times **SHOULD** be displayed in order of significance:
 - **For Date:** Year-Month-Day (YYYY-MM-DD), for
 - **Time:** Hour-Minute-Second-Partial Second (HH:MM:SS:FF).
 - **Date/Time together:** (Order: YYYY-MM-DD-HH:MM:SS:FF)
- For Date: Year (YYYY)-Month (MM)-Day(DD), for Time: Hour(HH 24 Hour)-Minute(MM)-Second(SS)-Partial Second (FF). This also applies when displaying date and time together (Order: Year to Partial Seconds)
- Date and time values **MUST** have a fixed number of digits and should be padded with leading zeros (2008-03-01 not 2008-3-1)
- If no time zone is included assume local time of the user. Otherwise use UTC time zone offsets
- Use of alphanumeric date formats is not recommended due to language compatibility issues

Where to Apply This Standard

The scope of use for this standard is all computer generated display date and time formats; the exception being Provincial correspondence which is NOT covered by the standard. The document also includes guidelines for other non-conforming formats and text-based dates/times stored in databases. These guidelines have been included at the request of stakeholders to limit the impact of non-conforming formats. Using formats for the guideline sections will require an exemption.

Authority and Exemptions

These standards have been updated by the Architecture and Standards Branch and, at the recommendation of the Architecture and Standards Board (ASRB), approved by the Government Chief Information Officer (GCIO). Therefore, these are government-wide standards and must be followed when displaying date and/or time in an IM/IT context.

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

The standards outlined in this document apply to a) all government ministries and, b) all external stakeholders wanting to share information with the provincial government. Compliance to these standards will be managed by the GCIO, Architecture and Standards Branch with the compliance framework yet to be determined.

Terms and Definitions

Any data administration terms and definitions in this document related to date formats are included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in References.

References

1. The location of the Display Date and Time Standard is located at:
www.cio.gov.bc.ca/local/cio/standards/documents/standards/date_time_display_standards.pdf.
2. The *B.C. Government Information Resource Management (IRM) Glossary* is currently under review.

Additional Information

Additional information management standards are available at:
www.cio.gov.bc.ca/cio/standards/daf.page.

Contact

Architecture and Standards Branch, OCIO

email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2001-06-19 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Process Standard</p>
<p>3.0 Information Management (CPPM 12.3.3)</p>	
<p>3.6 Government IRM Glossary Standards and Procedures</p>	
<p>Keywords:</p>	

Description of Standard

This standard defines:

- The process by which the B.C. Government standard *Information Resource Management (IRM) Glossary* of terms will be maintained.
- The format that is to be used for the glossary content.

Where to Apply This Standard

The *IRM Glossary* is a government-wide glossary of terms for Information Resource Management (IRM) and is intended to be the one source for IRM terms in government. Consequently, this standard is meant to define the process for anyone with the B.C. government or agency who wishes to update or enhance the Glossary.

Authority and Exemptions

The Data Administration Forum (DAF) published this standard with the consent of the Advisory Council on Information Management (ACIM). Compliance with this standard ensures that changes to this government-wide Glossary are properly managed.

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

The standard outlined in this document applies to all ministries. DAF's intention is to advertise and promote this standard as being mandatory in all government ministries. That said, DAF does not currently have the resources to enforce standards compliance. In order to effectively manage the Glossary, a ministry must adopt this standard, preferable through an internal data administration function.

Terms and Definitions

Any data administration terms and definitions in this document related to date formats are included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in References.

References

1. The *Government IRM Glossary Standards and Procedures* is currently under review.
2. The *B.C. Government Information Resource Management Glossary* is currently under review.

Additional Information

The Data Administration Forum is the owner of this standard. Its website is located at www.cio.gov.bc.ca/cio/standards/daf.page.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2002-03-12 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
	Type: Product Standard
3.0 Information Management (CPPM 12.3.3)	
3.7 Oracle® as Preferred Government Database Standard	
Keywords:	

Description of Standard

This standard establishes the use of Oracle® as the preferred application database manager within the B.C. government.

Where to Apply This Standard

This standard defines the conditions under which Oracle® is to be used when implementing new applications where databases (physical or logical) are required, or for all new government-wide and inter ministry database applications.

Authority and Exemptions

With the expiry of the Oracle® Network Server License Agreement (NSL) in April 2001, the Government Chief Information Officer (CIO) issued an update on the status of Oracle® within government since its mandatory use was no longer contractually required.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory component throughout government. However, in order to effectively manage the use of Oracle®, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any database administration terms and definitions in this document related to date formats are included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in References.

References

1. The location of the CIO memo supporting the *Oracle® as Preferred Government Database Standard* is:
www.cio.gov.bc.ca/local/cio/standards/documents/standards/oracle_update_memo_20020312.pdf.
2. The *B.C. Government Information Resource Management Glossary* is currently under review.
3. Information on the use of Oracle® as the *mandatory* database (between April 1, 1996, and March 31, 2002) including the process for requesting an exemption, can be found in a Technology Architecture Forum (TAF) presentation dated September 15, 1998. This document is available on request, to obtain a copy please contact the Architecture and Standards Branch.

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2003-06 Scheduled Review: Annual Last Updated: 2009-01 Last Reviewed: 2009-01
	Type: Product Standard
3.0 Information Management (CPPM 12.3.3)	
3.8 Enterprise Document and Records Management	
Keywords: TRIM, Document, Records Management	

Description of Standard

This standard establishes Hewlett Packard's TRIM as the Province's standard system for document and records management (both physical and electronic).

Where to Apply this Standard

The TRIM system is intended for use by ministries that have a requirement either to implement new document and/or records management software or to migrate from existing software to a new system. The TRIM system is also appropriate for ministries that are considering making substantial investments in additional development or installations of records management systems already in use (i.e., efforts beyond those required to maintain existing records management operations).

Authority and Exemptions

In October 2001 the B.C. government issued a Request for Proposal (RFP) for an Enterprise Document and Records Management System (EDRMS). The RFP sought an integrated software solution for managing documents and records, regardless of media, from creation to final disposition. A memorandum was issued by the Government Chief Information Officer (CIO) which stated that TRIM had been confirmed as the government standard system for document and records management.

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

EDS Canada was awarded a contract in March 2002 to provide Tower Software's TRIM system for deployment across government (30,000 desktops). In 2008 both EDS Canada and Tower Software were acquired by Hewlett Packard. The Ministry of Labour and Citizens' Services is working with Hewlett Packard, in conjunction with ministry Records Officers, to configure and administer TRIM to support government records management standards and business processes.

Implementation of a standard EDRMS toolset will enable government to manage its electronic and physical documents in a more consistent, effective and secure manner. This toolset will provide an essential electronic record keeping infrastructure, thereby reducing litigation risks, supporting information sharing and knowledge retention, and enabling improved information access and management. A baseline product configuration has been established to ensure required consistency across government.

Terms and Definitions

Any database administration terms and definitions in this document related to date formats will be included in the B.C. Government Information Resource Management (IRM) Glossary listed below in References.

References

1. The location of the CIO memo supporting the Tower Software's TRIM as the B.C. government standard for enterprise document and record management is: www.cio.gov.bc.ca/local/cio/standards/documents/standards/edrms_trim_memo_20030327.pdf.
2. The B.C. Government Information Resource Management Glossary is currently under review.

Additional Information

Information Access Operations of the Ministry of Citizens' Services is the owner of this standard. Its website is: www.gov.bc.ca/citz/iao.

Contact

Information Access Operations, Ministry of Citizens' Services
www.gov.bc.ca/citz/iao/records_mgmt/edrms_trim

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2007-03-22 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
	Type: Technical Standard
3.0 Information Management (CPPM 12.3.3)	
3.9 Aboriginal Administrative Data	
Keywords:	

Description of Standard

This standard establishes data specifications that provide consistency to Aboriginal identification in provincial government administrative data.

Where to Apply This Standard

This standard should be applied by ministries and agencies responsible for the delivery of services and programs designed to improve the socio-economic outcomes for Aboriginal persons, and ministries and agencies that monitor and measure citizen outcomes.

At the time of the first release of this standard, the following ministries were identified as mandatory adopters:

- Ministry of Education
- Ministry of Advanced Education
- Ministry of Health
- Ministry of Forests and Range (Housing)
- Ministry of Employment and Income Assistance
- Ministry of Economic Development
- Ministry of Children and Family Development
- Ministry of Attorney General
- Ministry of Public Safety and Solicitor General

Authority and Exemptions

This standard has been formally authorized by:

- Executive Director & Chief Information Officer, Ministry of Attorney General.
- Assistant Deputy Minister, Ministry of Aboriginal Relations and Reconciliation.
- Government Chief Information Officer (CIO), Ministry of Labour and Citizen Services.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory for the designated list of ministries (see *Where Standard is Used* above). In addition, each of these ministries is expected to:

- Implement and monitor compliance to this standard through a ministry data administration function
- Influence their agencies to adopt this standard.

This standard is not intended to limit the collection of data that a ministry may require in order to fully support their regular business functions; develop a central data warehouse, a common personal identifier, or an identity management approach.

Terms and Definitions

There are a number of data administration terms and definitions in this document. These will be included in the *B.C. Government Information Resource Management (IRM) Glossary* listed below in *References*.

References

- The location of the document containing the *Aboriginal Administrative Data* is: www.cio.gov.bc.ca/local/cio/standards/documents/standards/aboriginal_administrative_data_standards.pdf.
- The *B.C. Government Information Resource Management Glossary* is currently under review.

Additional Information

The Ministry of Aboriginal Relations and Reconciliation (MARR) is the owner of this standard and as such is responsible, along with the ministry's Chief Information Office (MCIO), for managing the review and revision process, and for ensuring that the standard is used in the planning and development process of all applicable information systems.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2008-12 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01 Type: Technical Information Standard
3.0 Information Management (CPPM 12.3.3)	
3.10 Common Raster Cell Origin, Shape and Sizes Standard for the Government of BC	
Keywords:	

Description of Standards

This standard is designed to bring consistency to the creation and use of raster data by adopting common raster cell origin, shape and sizes across government. The standard is based upon the existing provincial, 25 metre gridded Digital Elevation Model (DEM). The gridded DEM uses even planar coordinates generated in the provincial standard BC Albers coordinate reference system to define its centre-points. Therefore the outer boundaries of each cell which represent this origin are situated at Albers planar coordinates ending in 2.5m or 7.5m.

Where to Apply This Standard

This standard is to be applied across the Government of BC wherever raster data is used and/or created.

Authority and Exemptions

This standard has been formally authorized by:

- Natural Resource Sector Information Council
- Architecture Standards Review Board
- Executive Director, Architecture and Standards, Ministry of Labour and Citizens Services

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

The intention of the OCIO is to advertise and promote this standard as being mandatory across government whenever raster data is used or created. However, the GeoBC Crown Registry and Geographic Base Branch is responsible for adopting and monitoring compliance to this standard.

Terms and Definitions

Raster: the rectangular formation of parallel scanning lines that guide the electron beam on a television screen or a computer monitor

References

The location of the submission document containing the Common Raster Cell Origin, Shape and Sizes Standard for the Government of BC standard is:
<http://ilmbwww.gov.bc.ca/risc/pubs/other>

Additional Information

GeoBC Crown Registry and Geographic Base Branch is the owner of this standard. Therefore, it is responsible for managing the review and revision process, and for ensuring that the standard is used in the planning and development process of all applicable information systems. The website for GeoBC is: www.geobc.gov.bc.ca/

Contact

Peter Friesen, Head
Corp Data Architecture and Warehouse Operations
GeoBC Information Services
Phone: 250-387-9347 Email: Peter.G.Friesen@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2010-03-01 Scheduled Review: Annual Last Updated: 2010-03-01 Last Reviewed: 2010-03-01
	Type: Technical Standard
3.0 Information Management (CPPM 12.3.3)	
3.11 Open Data Physical Dataset Format Standard	
Keywords: Open, data, formats, Open Government	

Description of Standard:

This standard describes physical formats that must be used when publishing Open Datasets. Open Datasets are files that contain machine processable information that is accessible by the public.

The scope of this document is file formats only. All other factors such as file contents, metadata, hosting, licensing, IP, and security are out of scope.

Format Types:

Open Datasets

These dataset types must be used for any Open Dataset. These "least at-risk" formats are non-proprietary, open formats. These tend to promote a wide range of uses, backward and forward compatibility, and an independence from short-term commercial interests.

Dataset	Description
<u>KML</u>	Keyhole Markup Language – an XML-based language schema for expressing geographic annotation and visualization.
<u>KMZ</u>	Zipped KML files.
<u>GML</u>	Geography Markup Language – the XML grammar defined by the Open Geospatial Consortium (OGC) to express geographical features.
<u>GeoJSON</u>	GeoJSON is a format for encoding a variety of geographic data structures.
<u>GeoTiff</u>	GeoTIFF is a public domain metadata standard that allows geo-referencing information to be embedded within a TIFF file.
<u>Jpeg2000</u>	JPEG 2000 is a wavelet-based image compression standard and coding system.
<u>XML</u>	Extensible Markup Language – a set of rules for encoding documents electronically.
<u>CSV</u>	Comma-separated values – a file that is used for the digital storage of data structured in a table of lists form.
<u>ODF</u>	Open Document Format – XML-bases document format.
<u>OOXML</u>	Office Open Extensive Markup Language – an ISO/IEC standardized file format.
<u>JSON</u>	JavaScript Object Notation is a lightweight data-interchange format.

Semi-Open Datasets

These are proprietary. They should only be used as a companion to a Format found in the Open Dataset Formats list above.

Dataset	Description
<u>Shapefile</u>	A popular geospatial vector data format. www.esri.com/library/whitepapers/pdfs/shapefile.pdf
<u>PDF</u>	Adobe document format.
Pre Office 2007 .DOC, .XLS, .PPT, MDB	Microsoft Office file formats. www.microsoft.com/interop/docs/OfficeBinaryFormats.msp Microsoft Access file format, a database file format http://office.microsoft.com/en-us/access/default.aspx

Where to Apply This Standard

This standard must be used when publishing any file that is an Open Dataset.

Authority and Exemptions

If there are compelling business reasons why an organization is unable to comply with the format types outlined in this standard or wish to extend the standard the organization's, CIO may authorize a submission for exemption through the Architecture and Standards Branch.

Metrics and Enforcement

Ministry designated contact.

References

Normative	Informative
KML/KMZ http://www.opengeospatial.org/standards/kml/	US Open Data Principles: http://wiki.opengovdata.org/index.php?title=OpenDataPrinciples The American Library Association: "Key Principles of Government Information" http://www.ala.org/ala/aboutala/offices/wo/woissues/governmentinfo/keyprins.cfm Open Knowledge Foundation's Open Knowledge Definition: http://www.okfn.org/
GML: http://www.opengeospatial.org/standards/gml/	
GeoJSON: http://geojson.org/geojson-spec.html	
GeoTiff: http://www.remotesensing.org/geotiff/spec/geotiffhome.html	
Jpeg2000: http://www.jpeg.org/jpeg2000/	
XML: http://www.w3.org/XML	
CSV: http://tools.ietf.org/html/rfc4180	Australia http://www.csiro.au/solutions/ps1u1.html New Zealand http://data.govt.nz
OOXML: http://www.ecma-international.org/publications/standards/Ecma-376.htm	
ODF: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office	
JSON: http://www.json.org	Open Access/Licensing framework (NZGOAL): http://epsiplatform.com/layout/set/print/content/download/28721/381845/version/1/file/New+Zealand+open+licensing+Draft_NZGOAL%5B1%5D.pdf

Additional Information

Please refer to the Open Data document (currently under development).
The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2010-04-01 Scheduled Review: Annual Last Updated: Last Reviewed:</p> <p>Type: Technical</p>
<p>3.0 Information Management (CPPM 12.3.3)</p>	
<p>3.12 Physical Address and Geocoding Standards – Conceptual Model</p>	
<p>Keywords: geocoding, physical address, address</p>	

Description of Standard

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.

The standard supports four key areas:

1. Geocoding – what is the location (coordinates) of an address? Does a given address exist?
2. Reverse geocoding – what are all the addresses within a given distance of a point location? What are all the addresses within a given area? What is the most current address of a given dwelling or facility?
3. Physical address standardization.
4. Synchronization of addresses in client applications with addresses in a geocoder.

This standard will be used by GeoCode BC and for hosting compliant address data within the BC Geographic Warehouse.

Where to Apply This Standard

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

Authority and Exemptions

This standard has been formally authorized by:

- Natural Resource Sector Information Council
- Architecture Standards Review Board
- Executive Director, Architecture and Standards, Ministry of Citizens Services

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

The intention of the OCIO is to advertise and promote this standard as being mandatory across government. However, the GeoBC Information Services Branch is responsible for adopting and monitoring compliance to this standard.

Terms and Definitions

See section 1.1 in [R.1]

References

The *Physical Address and Geocoding Standards Conceptual Model v1.0* can be found here:

http://www.data.gov.bc.ca/local/dbc/docs/geo/services/standards-procedures/geocoding_standards_conceptual_model_v1.0.pdf

Additional Information

GeoBC Information Services Branch is the owner of this standard and is responsible for managing the review and revision process and ensuring the standard is used in the planning and development process of all applicable information systems. The website for GeoBC is: www.geobc.gov.bc.ca/

Contact

Michael Ross, Geoweb Architect

GeoBC Information Services Branch, Integrated Land Management Bureau

Phone: 250-387-3995 email: michael.ra.ross@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2011-09-01 Scheduled Review: Annual Last Updated: 2011-09-01 Last Reviewed: 2011-09-01
	Type: Information
3.0 Enterprise Content Management	
3.13 ECM - Content Metadata Standard	
Keywords: ECM, Unstructured content, Metadata	

Description of Standard:

This standard provides the minimum content metadata requirements of the Province, providing a common baseline across all of the business areas.

Events and Definitions

Events during the lifecycle of the content determine key metadata elements. Identifying these events will help determine when metadata is required, and what it should be.

Event	Definition
Create/Capture	Creating or moving a paper form into an electronic form.
Stores	The act of moving content into a Content Management System.
Adding information to content	Inserting or updating new information to the content.
Removing information from content	Taking information out of the content.
Modifying personal information within the content	Inserting or removing personal information from the content.
New legislation	If there is a change in legislation.
Finalizing the content	The content becomes a Record of Government.
Publishing content	The content is published to the internet/intranet.

Principles:

Throughout this document the following principles apply:

- Consistency, through the use of the elements within the Content Metadata Model.
- Only authoritative sources will be used.

Metadata elements that must be present during the following events:

(NOTE: Refer to the Content Metadata Model for further information about the elements.)

- a. Event: Create/Capture – Creating or moving a paper form into an electronic form.
 - [Date Created](#)
 - [Creator](#)
 - [Title](#)
- b. Event: Stores – The act of moving content into a CMS.
 - [Security Label](#)
 - [Security Classification](#)
 - [Schedule Number](#)
 - [Primary Number](#)
 - [Secondary Number](#)
 - [Description](#)
 - [Keywords](#)
- c. Event: Adding information to content – Inserting or updating new information to the content.
 - [Security Label](#)
 - [Security Classification](#)
 - [Date Modified](#)
- d. Event: Removing information from content – Taking information out of the content.
 - [Security Label](#)
 - [Security Classification](#)
 - [Date Modified](#)
- e. Event: New Legislation – If there is a change in legislation.
 - [Security Label](#)
 - [Security Classification](#)
 - [Date Modified](#)
- f. Event: Finalizing content – The content becomes a Record of Government.
 - [Security Label](#)
 - [Security Classification](#)
- g. Event: Publishing content – The content is published to the internet/intranet.
 - [Security Label](#)
 - [Security Classification](#)

- [Publisher](#)
- [Date Published](#)
- [Audience](#)
- [Description](#)

Where to Apply This Standard

This standard applies to British Columbia government ministries and central agencies. Other organizations may choose to adopt these standards or may agree to adopt these Standards.

Authority and Exemptions

This standard has been issued by the OCIO.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

References

- US Department of Defense Discovery Metadata Specification (DDMS); Version 3.0
http://metadata.dod.mil/mdr/ns/DDMS/3.0/DDMS-v3_0-0.doc
- The Provincial *Document Disposal Act* (RSBC 1996, c.99)
- The OCIO [Information Security Policy](#);

ADDITIONAL INFORMATION

Contact

Architecture and Standards Branch

Office of the CIO

email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2000-09-27 Scheduled Review: SUPERSEDED/OBSOLETE Last Updated: Last Reviewed: 2009-01</p> <hr/> <p>Type: Process Standard</p>
<p>4.0 IDENTITY MANAGEMENT (CPPM 12.3.4)</p>	
<p>4.1 Secure Electronic Transactions – OBSOLETE/SUPERSEDED</p>	
<p>Keywords: Obsolete, superseded, cryptographic</p>	

IMPORTANT: This Standard is obsolete. It has been superseded by
6.10 Cryptographic Standards for Information Protection

Description of Standard

This interim standard defines government's general strategic direction and some decisions regarding public key infrastructure (PKI) until one or more standards for secure electronic transactions are available.

1. The Government will not compete with private sector certification authority services in the provision of digital certificates to parties external to government.
2. The Government will not license or regulate private sector certification authorities.
3. Ministries must not establish certification authority services to issue digital certificates.
4. If a business need is established for digital certificates for internal government transactions, the OCIO will act as a certification authority and issue digital certificates, including anonymous digital certificates.
5. Where a ministry identifies a business requirement to use digital certificates for transactions with parties external to government:
 - the external parties will be directed to private sector certification authorities for digital certificates; and
 - government will function as the relying party in relation to the certification authority and parties external to government.
 - Existing PKI pilots for parties external to government will continue until private sector certification authority services are arranged for the external parties.
6. A PKI standard for government will not be established until:
 - stable standards exist within the marketplace; and
 - there is interoperability between leading PKI products.

However, a standard has been established for *Data Encryption and Minimum Key Length* and can be found in Section 6.9.

Where to Apply This Standard

This standard is intended to serve as a reference to all internal (government) and external (contracted) resources involved in the design, development, implementation and operational management of all information systems.

Authority and Exemptions

This standard has been issued in *interim status* because the OCIO is working to establish a more comprehensive and collaborative framework involving broad stakeholder participation for defining, approving, and issuing standards for securing electronic transactions.

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

The intention of the OCIO is to advertise and promote these standards as being mandatory throughout government. However, in order to effectively manage information systems security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated September 27, 2000) defined the standard related to the use of PKI for secure electronic transactions. A copy of this memo can be found at:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/secure_electronic_transactions_memo_20000927.pdf.

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2001-11-16 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Technical Standard</p>
<p>4.0 Identity Management (CPPM 12.3.4)</p>	
<p>4.2 Single Identifier for Transacting with Government Electronically</p>	
<p>Keywords:</p>	

Description of Standard

This standard establishes a single identifier (BCeID) for organizations and individuals transacting electronically with government.

A single corporate identification will:

- ensure that any organization can interact with the B.C. Government's online services using a single userid and password; and
- eliminate the duplicate identifiers and enrolments currently in existence.

Where to Apply This Standard

This standard is targeted at electronic service delivery initiatives that are being rolled out by ministries and other government agencies. A key part of that process is a registration service to permit users conducting business-to-government interactions to be authenticated.

Authority and Exemptions

This standard has not yet been fully defined because the OCIO is working to establish a more comprehensive and collaborative process involving broad stakeholder participation for defining, approving, and issuing a common identifier (BCeID) standard and governance process.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information systems security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated November 16, 2001) outlined the intent to establish a single identifier for organizations and individuals transacting electronically with government. A copy of the memo can be found at: http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/bceid_memo_20011116.pdf.

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO

email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture and Standards Branch STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2009-06-01 Scheduled Review: Annual Last Updated: Last Reviewed:</p> <hr/> <p>Type: Technical Standard</p>
<p>4.0 Identity Management (CPPM 12.3.4)</p>	
<p>4.3 Standard for Multi-Function Identity Card: Physical Characteristics and Graphical Topography</p>	
<p>Keywords: Standard, Multi-Function Identity Card, Smart Card, Identity Card, Access Card</p>	

Summary

This standard describes the technology standard for multi-function identity cards for B.C. public service employees, contractors, and visitors.

The International Standard ISO/IEC 7810, 7816, 14443 and FIPS 140, 201 have been used extensively in the development of this technical specification document.

Where to Apply This Standard

This standard is meant for any ministry that is considering implementing a multi-function identity card.

Authority and Exceptions

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout Government. However, in order to effectively manage information security, ministries and broader public sector agencies are expected to adopt and monitor compliance to this standard. The OCIO ISB will also monitor for compliance.

Physical and Technology Card Requirements

1. The card body must conform to the ISO 7810 ID1 standard.
2. The ICC contact chip must conform to ISO 7816-1-4 standards and FIPS 140-2 Level 3 Security.
3. The contact-less chip interface must conform to ISO 14443 parts 1-4.
4. The magnetic stripe must conform to ISO 7811-6 standard and be located on the back side.

5. The card will have a hole punched for attachment of a lanyard. The hole will be 14 X 2 mm and centrally located near the top of the card.

Text Requirements

1. All security text (see below) is to be printed in Arial font (FIPS 201-1).
2. All security text (section 4 below) is to be printed in 5pt normal for tags or labels and **6 pt bold** for text data (FIPS 201-1).

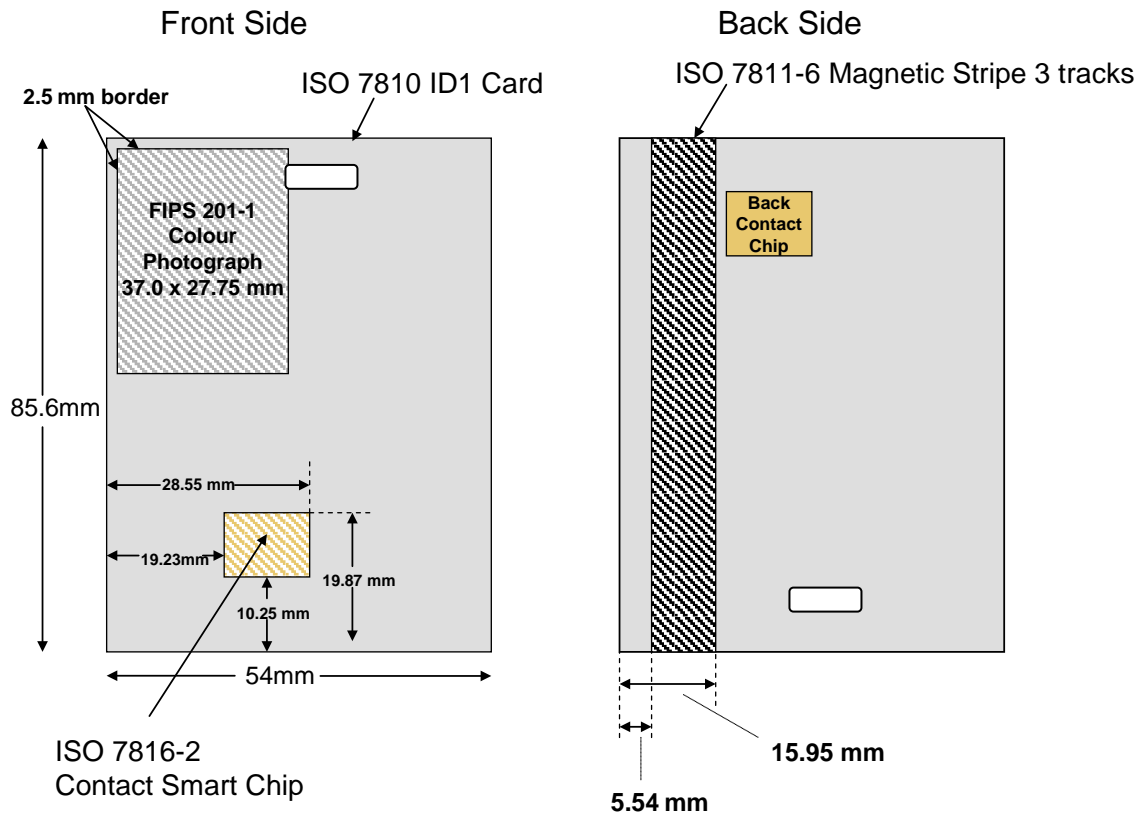
Security and Privacy Requirements

1. The card must have visual technology, such as holography, to prevent counterfeiting.
2. The card must have issue and expiry dates (**6 pt bold**) displayed on the front side, using Government standard date format (YYYYMMDD).
3. The card must have a portrait orientation to enable wearing with a lanyard.
4. The card must have a colour photograph of a full frontal pose, from top of head to shoulder and with a minimum 300 dots per inch resolution on the front side, as per FIPS 201-1 standard, excepting visitor and temporary cards which do not have photographs. The graphic designer is free to enlarge the photograph size from the size shown in the figure (37 x 27.75 mm), provided it does not conflict with the striped areas (chip contact and magnetic stripe).
5. The full first and last names of the legal name (see *BC Name Act*) (**6pt bold**) of the card holder must be displayed on the back side. A pseudonym may be used in approved situations with high security risk. Visitor cards have the name "Visitor" or "Temporary".
6. The Province of British Columbia (5 pt normal), as the card issuer, must be displayed on the front or back of the card.
7. A unique serial number (**6 pt bold**) for each card must be displayed on the front or back of the card.
8. Contact information (5 pt normal) for reporting lost cards must be displayed on the back side of the card.
9. A colour-coded rectangle for employee affiliation must be displayed on the front side of the card. The affiliation is one of Employee (all types), Contractor, Temporary, or Visitor. The graphic designer is free to choose the colour, shape and location on the front of the card, provided the affiliation is recognizable from a distance of up to 10 metres (corrected vision assumed where needed).
10. A blank space on the back side of the card must be included in the graphic design, so that a location-specific safety information sticker may be applied and replaced as necessary. The blank space must be a minimum of 30 X20 mm.

Card Topography

The figure below shows the physical layout of the common access card, as determined by the standards to be supported on the card. The front (left) and back (right) sides are presented below. The graphic design must provide for the location of the colour photograph, smart chip contacts, and magnetic stripe.

The graphic designer is free to choose the location of graphic elements and the location of the required security text, within the constraints of sections 3 and 4 above.



Striped areas are not available for printing.

References

The full Multi-Function ID Card standard, can be viewed at:

www.cio.gov.bc.ca/local/cio/standards/documents/standards/mfidcard_topography.pdf

Additional Information

The OCIO is the owner of this standard. Its website is www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

Email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2010-04-23 Scheduled Review: Annual Last Updated: 2010-04-23 Last Reviewed: 2010-04-23</p> <p>Type: Process Standard</p>
<p>4.0 Identity Management (CPPM 12.3.4)</p>	
<p>4.4 Identity Assurance Standard</p>	
<p>Keywords: Identity Information Management, Framework, Identity Assurance Level, Transaction Assurance Level, Identification, Registration, Identity Proofing, Evidence, Verification, Credential Strength, Biometric, Authentication, Risk Assessment</p>	

Description of Standard

This standard introduces the Identity Assurance Framework and sets the minimum information, process and technology requirements for achieving increasing levels of identity assurance over multiple service delivery channels.

It also provides guidance for conducting identity-related risk assessments and sets an overall framework for supporting standards and guidelines that are necessary for achieving identity assurance, including the *Evidence of Identity Standard*, the *Electronic Credential and Authentication Standard*, and the *Registration of Organizations and Affiliation Standard*.

Where to Apply This Standard

This standard applies to British Columbia government ministries and central agencies. Other organizations may choose to adopt these standards or may agree to adopt these standards for the purpose of fulfilling contractual, federation or other legal agreements.

This standard must be applied to all government services and resources that require identity assurance, regardless of the service delivery channel (online, in person, over the telephone, postal).

This standard also must be applied to the identification and authentication of individuals in an employment context (i.e. to the use of government services and resources by government employees).

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.4.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Terms and Definitions are defined within the standard.

References

1. The *Identity Assurance Standard* is available at www.cio.gov.bc.ca/local/cio/standards/documents/standards/identity_assurance_standard.pdf

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

Phone: 250-952-6913 email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2010-04-23 Scheduled Review: Annual Last Updated: 2010-04-23 Last Reviewed: 2010-04-23</p> <p>Type: Process Standard</p>
<p>4.0 Identity Management (CPPM 12.3.4)</p>	
<p>4.5 Evidence of Identity Standard</p>	
<p>Keywords: Identity Information Management, Identity Assurance Level, Identification, Registration, Identity Proofing, Evidence, Verification, Physical Credential, Credential Strength, Biometric, Authentication</p>	

Description of Standard

This standard re-introduces the Identification Levels set out in the *Identity Assurance Standard* and sets evidence of identity, registration and operational diligence standards for establishing an individual's identity to four increasing levels of identification strength.

It also sets standards for the subsequent confirmation or verification of an individual's identity over-the-counter (i.e. in person) and over the telephone.

Where to Apply This Standard

This standard applies to British Columbia government ministries and central agencies. Other organizations may choose to adopt these standards or may agree to adopt these standards for the purpose of fulfilling contractual, federation or other legal agreements.

This standard applies to organizations that perform their own registration and identity-proofing services and to organization that provide registration and identity-proofing services for other organizations.

This standard must be applied to all government services and resources that require identity assurance, regardless of the service delivery channel (online, in person, over the telephone, postal). This standard applies to both the initial establishment of identity and to the subsequent confirmation or verification of identity.

This standard also must be applied to the identification and authentication of individuals in an employment context (i.e. to the recruitment of, and the use of government services and resources by, government employees).

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.4.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of

government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Terms and Definitions are defined within the standard.

References

1. The *Evidence of Identity Standard* is available at www.cio.gov.bc.ca/local/cio/standards/documents/standards/evidence_of_identity_standard.pdf

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

Phone: 250-952-6913 email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2010-04-23 Scheduled Review: Annual Last Updated: 2010-04-23 Last Reviewed: 2010-04-23</p> <p>Type: Process, Technical Standard</p>
<p>4.0 Identity Management (CPPM 12.3.4)</p>	
<p>4.6 Electronic Credential and Authentication Standard</p>	
<p>Keywords: Identity Information Management, Identity Assurance Level, Electronic Credential, Electronic Authentication, Credential Strength, Password, Smart Card, Cryptographic Token</p>	

Description of Standard

This standard re-introduces the Credential Strength and Authentication Levels set out in the *Identity Assurance Standard* and sets technology, security, lifecycle management and operational diligence standards for authenticating an individual's identity to four increasing levels of credential and authentication strength. This includes requirements for:

- the types of electronic credentials that are acceptable,
- appropriate password values and how to store and manage password and related data,
- the authentication mechanisms and protocols that are acceptable,
- the assertion mechanisms that are acceptable to communicate the results of the authentication to an information system or application,
- how a credential is uniquely linked to an identity, and how credentials are created, delivered to the user and maintained over time, and,
- additional service management and information security policy requirements for organizations that provide electronic credential and authentication services.

Where to Apply This Standard

This standard applies to British Columbia government ministries and central agencies. Other organizations may choose to adopt these standards or may agree to adopt these standards for the purpose of fulfilling contractual, federation or other legal agreements.

This standard applies to organizations that issue and manage electronic credentials, authenticate electronic credentials or has an information system that relies on the use of electronic credentials and authentication. It applies to electronic credentials and authentication of citizens and businesses that use online government services and resources, as well as of individuals in an employment context (i.e. government employees).

Authority and Exemptions

This standard has been issued by the OCIO in accordance with

- CPPM Chapter 12.3.4 *Electronic Identity Management*,
- CPPM Chapter 12.3.1 *Appropriate Use of Government Resources*,

- CPPM Chapter 12.3.6 *Information Technology Security*, and
- *Information Security Policy* Chapter 7 *Access Control*.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Terms and Definitions are defined within the standard.

References

1. The *Electronic Credential and Authentication Standard* is available at www.cio.gov.bc.ca/local/cio/standards/documents/standards/electronic_credential_authentication_standard.pdf
2. The Information Security Policy is available at www.cio.gov.bc.ca/local/cio/informationsecurity/policy/chapters/chapter7.pdf

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

Phone: 250-952-6913 email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2010-04-23 Scheduled Review: Annual Last Updated: 2010-04-23 Last Reviewed: 2010-04-23</p> <p>Type: Information, Technical Standard</p>
<p>4.0 Identity Management (CPPM 12.3.4)</p>	
<p>4.8 Claims Information Standard</p>	
<p>Keywords: Identity Information Management, Claim, Authoritative Party, Relying Party, Security Token, Claim Type, Claim Definition, Identity Assurance Level, Name, Identifier, Organization, Business Role, OID, UUID, URI, URN</p>	

Description of Standard

This standard consists of a set of standards, guides and definitions of claims that, when implemented by government organizations, will support an interoperable system to securely exchange identity information or claims. It is related to the *Claims Technology Standard* that describes how to implement the claims-based architecture and federation technology.

This standard describes:

- the concept of a claim, how it relates to the claims-based architecture, how claims are intended to be used (such as for user access control or personalization), and how a claim is described,
- definitions for the core set of claims related to the *Identity Information Reference Model*, with focus on identity information about individuals representing themselves in different identity contexts (i.e. as an employee, a professional, a business representative), and,
- guidance on the rules and processes about how additional claims can be defined for use within information systems that implement the claims-based architecture.

Where to Apply This Standard

This standard applies to British Columbia government ministries and central agencies. Other organizations may choose to adopt these standards or may agree to adopt these standards for the purpose of fulfilling contractual, federation or other legal agreements.

This standard applies to organizations that use federation technology.

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.4.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Terms and Definitions are defined within the standard.

References

1. The *Claims Information Standard* is available at www.cio.gov.bc.ca/local/cio/standards/documents/standards/claims_information_standard.pdf

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

Phone: 250-952-6913 email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2010-04-23 Scheduled Review: Annual Last Updated: 2010-04-23 Last Reviewed: 2010-04-23 Type: Technical Standard
4.0 Identity Management (CPPM 12.3.4)	
4.9 Claims Technology Standard	
Keywords: Identity Information Management, Claim, Authoritative Party, Relying Party, Identity Provider, Federation, Protocol, Profile, Security Token, SAML, Web Services Federation, Information Card, Identity Metasystem, Interoperability	

Description of Standard

This standard consists of a set of standards of technology profiles that, when implemented by government organizations, will support an interoperable system that allows for the secure exchange identity information or claims. It is related to the *Claims Information Standard* that describes claims and defines a core set of claims that can be exchanged. This standard sets out:

- specific technology profiles to be used for various technical architectures that describe how to implement the secure communication protocols between Relying Parties and Authoritative Parties to request claims, initiate electronic authentication, and receive the resulting claims, and,
- the user interface features to guide the user to select their choice of Authoritative Party and digital identity, and submit their credentials.

Where to Apply This Standard

This standard applies to British Columbia government ministries and central agencies. Other organizations may choose to adopt these standards or may agree to adopt these standards for the purpose of fulfilling contractual, federation or other legal agreements.

This standard applies to organizations that use federation technology.

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.4.

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Terms and Definitions are defined within the standard.

References

1. The *Claims Technology Standard* is available at www.cio.gov.bc.ca/local/cio/standards/documents/standards/claims_technology_standard.pdf

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

Phone: 250-952-6913 email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2006-08 Scheduled Review: Annual Last Updated: 2008-08 Last Reviewed: 2009-01
	Type: Process Standard
Office of the Chief Information Officer Province of British Columbia	
5.0 INFORMATION TECHNOLOGY MANAGEMENT (CPPM 12.3.5)	
5.1 User Interface Standards and Guidelines for the Internet	
Keywords:	

Description of Standard

This document provides standards and guidelines for the design and development of B.C. government websites. In this case, "standards" refers to mandatory elements or processes; "guidelines" are non-mandatory, preferred methods to obtain intended results gleaned from research, feedback, and experience.

This document replaces all previous versions of the Internet Standards.

Branding and communications standards are governed by the Province's BC ID Program. For information, please contact the BC ID Program at:
PABBCIDTEAM@Victoria1.gov.bc.ca

Where to Apply This Standard

- The *B.C. Government Internet Standards and Guidelines* apply to all government websites and e-services that are accessible by the public over the Internet.
- All B.C. provincial ministries and organizations that have a direct reporting structure to a Deputy Minister must follow the standards and guidelines. If you are unsure of your organization's requirement to follow the standards, please contact the Public Affairs Bureau Online Communications Unit.

Authority and Exceptions

Exemptions to the B.C. Government Internet Standards may be considered if there is a valid business reason. The exemption application form is available through the Online Communications Office of the Public Affairs Bureau through:
Email: PABOC@victoria1.gov.bc.ca

Metrics and Enforcement

Both informational websites and e-services that are accessible to the public or identifiable business partners outside government must follow this standard. E-services must comply unless granted an exemption through the formal exemption process mentioned above. E-services that don't comply with the standard, and where an exception has not been granted, may be required to comply. In such cases, ministries will be expected to bear the cost of retrofitting e-service applications to comply with the standard.

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any additional web-based, IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. The location of the document, entitled Internet Standards and Guidelines that describes this standard can be found at

Public Internet:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/internet_standards_guidelines.pdf

It should be used as a companion to:

2. The Communication Standards for the B.C. Government Internet, which includes the B.C. government's Identity Program. This link, which requires government intranet access and an IDIR userid, is located at:

Public Internet:

Request this document from PABOC@victoria1.gov.bc.ca

3. The two primary means of becoming compliant with these standards are:
 - a) **The B.C. Government Content Management System (CMS)**
Based upon Interwoven TeamSite, this enterprise scale web platform allows non-technical staff to manage standards-compliant websites. Non-technical users can author, approve, and deploy pages autonomously.
 - b) **The 2008 Internet Templates** for Adobe Dreamweaver. In certain circumstances, smaller websites or updates to web pages may use these templates. This package includes HTML code, supporting javascripts, cascading stylesheets and images for use by developers with web development training.

Alternatively, for unique applications or if developers cannot use the CMS or Dreamweaver, these standards can be met through any other HTML development tool, though this may increase complexity and cost while reducing flexibility to make site-wide changes in the future.

Ministries should contact The Online Channel Office for guidance on which method is most appropriate for specific websites by emailing OCOServiceRequest@gov.bc.ca.

The form for applying for an exemption to this standard, which is intended for internal use within government, is available from

Public Internet:

Request this document from: PABOC@victoria1.gov.bc.ca

Additional Information

The Public Affairs Bureau is the business owner of this standard, and is responsible for the business needs relating to accessing government information and services. Several working groups have been organized by the Online Channel Office (OCO) of the Ministry of Citizens' Services in order to ensure partnership with the ministries in the management of online standards including:

- search
- web analytics and reporting
- standards and guidelines.

The recommendations of the working groups are approved by PAB and implemented by OCO. Where there is some potential conflict or issue in these recommendations, the OCO is responsible to escalate these to the Executive Director of OCO who will escalate to other levels of management and government as necessary. For further information, contact the OCO at the number below:

Contact

Online Channel Office

Telephone: 250 387-7573

eMail: OCOServiceRequest@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: August 2006 Scheduled Review:
	Type: Process Standard
Office of the Chief Information Officer Province of British Columbia	
5.0 Information Technology Management (CPPM 12.3.5)	
5.2 User Interface Standards and Guidelines for the Government Intranet	

Description of Standard

For websites or web-based applications that are intended to be accessible **only internally** within government, **there are currently no user interface standards and guidelines**. In particular and in accordance with information provided by the Public Affairs Bureau, the *User Interface Standards and Guidelines for the Government Internet* standard (Section 5.1) that defines mandatory practices and guidelines for the design and development of Province of British Columbia Internet and extranet websites **does not apply to government intranet websites** since these are intended only for government employees or designated contractors.

Where Standard is Used

If a standard existed for *User Interface Standards and Guidelines for the Government Intranet*, it would apply to all ministry and provincial agency websites and e-services that are **not accessible by either the public or identifiable business partners**. Otherwise, the standard entitled *User Interface Standards and Guidelines for the Internet* (Section 5.1) applies.

Authority and Exemptions

If you are unsure of your organization's website classification, i.e., whether or not it can be excluded from the *User Interface Standards and Guidelines for the Government Internet* standard, please contact the Public Affairs Bureau (PAB) at PABOC@Victoria1.gov.bc.ca.

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

Both informational and e-services websites that are strictly internal to the government may be exempt from the *User Interface Standards and Guidelines for the Government Internet* standard. If such websites are found not to be compliant with intranet usage, then the organization will be expected to bear the cost of retrofitting these websites to comply with the *User Interface Standards and Guidelines for the Government Internet* standard.

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT website, security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Public Affairs Bureau to the Ministry of Health clarified the types of websites that may be exempt from the *User Interface Standards and Guidelines for the Government Internet* standard. A copy of this memo is available from the OCIO.

Additional Information

The Public Affairs Bureau is the business owner of the *User Interface Standards and Guidelines for the Government Internet* standard (Section 5.1), and is responsible for the business needs relating to accessing government information and services. Several working groups have been organized by the Online Channel Office (OCO) of ServiceBC in order to ensure partnership with the ministries in the management of online standards including:

- search
- web analytics and reporting
- standards and guidelines.

The recommendations of the working groups are approved by PAB and implemented by OCO. Where there is some potential conflict or issue in these recommendations, the OCO is responsible to escalate these to the Executive Director of OCO who will escalate to other levels of management and government as necessary. For further information, contact the OCO at OCOServiceRequest@gov.bc.ca.

Contact

Online Channel Office

Telephone: 250 387-7573

eMail: OCOServiceRequest@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2005-04-18 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
	Type: Process Standard
5.0 Information Technology Management (CPPM 12.3.5)	
5.3 Wireless Internet Access and Wireless Hotspots	
Keywords:	

Description of Standard

This standard clarifies the precautions that employees must take when connecting to government information services via the Internet, in particular using wireless networks from wireless enabled laptops and other devices. One of the following security measures must be used when connecting from the Internet, including wireless hotspots:

- Shared Services B.C. (SSBC) -SPAN BC/Virtual Private Network (VPN);
- SSBC/Desktop Terminal Service (DTS); and
- application specific methods such as Secure Sockets Layer (SSL) enabled websites (e.g., spring.gov.bc.ca)

Where to Apply This Standard

The standard is meant for any government employee accessing wireless network hotspots from homes, hotels, and public spaces such as airport terminals and coffee shops. Wireless hotspots are considered to be the same as the Internet, i.e., not trusted and not secure because the transmission of information is in unencrypted form and via radio waves, and has the potential for the data to be intercepted and copied by another user by simply capturing the radio signal

Authority and Exemptions

These standards have been issued by the Office of the Chief Information Officer (OCIO) because hotspots are not controlled or managed by government and are therefore subject to security risks.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated April 18, 2005) defined the standard for Wireless Internet Access and Wireless Hotspots. A copy of this document can be found at:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/wireless_access_memo_20050418.pdf.

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2007-03-29 Scheduled Review: Annual Last Updated: 2009-01 Last Reviewed: 2009-01</p> <p>Type: Process and Product Standard</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.4 Connection of Multi-Function Devices (MFDs) to SPAN/BC Network</p>	
<p>Keywords:</p>	

Description of Standard

This standard defines the acquisition process and the security metrics that must be addressed with respect to the connection and operation of multi-function devices (i.e., devices combining photo-copier, printer, facsimile and scanner functionality) on the SPAN/BC network.

Where to Apply This Standard

The standard is meant for any ministry or other government agency that is

- considering purchasing an MFD, and
- intending on connecting the device to the SPAN/BC network.

Authority and Exemptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) because an MFD can create a security exposure that must be addressed before these machines can be connected to the SPAN/BC network.

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

Because MFDs are considered IT devices, SSBC offers a secure MFD Service. Details of this new Shared Services BC service offering can be found on the SSBC client website (see Reference #1 below).

This service will only support devices from the primary MFD supplier (currently, Ricoh Canada). These devices have been tested to verify compliance with OCIO security policy and standards, and processes have been established to provide operational support.

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. The SSBC Multifunction Device Service offering is located on an internal government website. For more information please contact:

SSBC.ClientServices@gov.bc.ca

250-387-8045

1-877-387-8045

2. The following SSBC Service Bulletins (#99, #109a and #109b) relating to the procurement of MFDs have been issued by SSBC:

- Announcement of completion of the RFP process for MFDs.
- MFD Service Offering Announcement - Core Government.
- MFD Service Offering Announcement - Broader Public Sector.

These documents are located on an internal government website. For more information please contact:

SSBC.ClientServices@gov.bc.ca

250-387-8045

1-877-387-8045

3. The Security Standards document for connection and use of MFDs is *located on the OCIO's intranet website on the Information Security Standards and Guidelines page. This document is not available to the general public.*

For more information please contact:

Security Strategies, OCIO

email: CITZCIOSecurity@gov.bc.ca

4. The following Government Chief Information Officer directives and memos have defined the policy and standards for connection of MFDs to the SPAN/BC network, and are included for background information only:

- May 31, 2005:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/mfd_security_standards_memo_20050531.pdf; and

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/mfd_security_standards.pdf;

- September 6, 2005:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/mdf_communique_20050906.pdf

Additional Information

The Information Security Branch, OCIO, is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Corporate Planning & Policy
Information Security Branch, OCIO
email: CITZCIOSecurity@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2002-04-09 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Product Standard</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.5 Use of webMethods® as Integration Broker Standard</p>	
<p>Keywords:</p>	

Description of Standard

This standard defines integration middleware functionality for the B.C. government. A memo from the Government Chief Information Officer (CIO) subsequently announced that webMethods® was selected as the preferred solution that met the Province's integration broker standard. SSBC offers an Integration Broker Service based on webMethods®.

Where to Apply This Standard

The webMethods® integration broker solution is intended for use by ministries and other government agencies that have a requirement for an application to application service that uncouples mainframe, server and desktop application dependencies, leverages common security, directory and portal services, and facilitates corporate data sharing.

Authority and Exemptions

On June 15, 2001 the B.C. government issued a Request for Proposal (RFP) for Integration Broker Software and Related Services. The RFP sought an integrated software solution based on the Province's integration broker standard. A memorandum was issued by the CIO which stated that webMethods® had been selected as the proponent to deliver this solution.

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

The intention of the OCIO is to advertise and promote this standard as being an integral part of Province's Enterprise Portal. However, in order to effectively manage the use of webMethods®, ministries and other provincial agencies are expected to monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. The Province's integration broker standard is contained within the *Request for Proposal (RFP) for Integration Broker Software and Related Services* and is available on request. To obtain a copy please contact the Executive Director of Architecture and Standards.
2. The CIO memo (dated November 12, 2001) announcing the selection of webMethods® integration broker is also available on request. To obtain a copy please contact the Executive Director of Architecture and Standards.

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca. Information on the Integration Broker Service can be obtained from a SSBC Client Relations Manager or Client Business Analyst.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2007-10-26 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Product Standard</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.6 SSBC Workstation Services Supported Hardware Products</p>	
<p>Keywords:</p>	

Description of Standard

This standard is a definitive listing of workstation hardware products that are available through iStore and supported by SSBC Workstation Services.

These workstation technologies are divided into five general areas:

1. Personal computers (PCs) including desktops, laptops and tablets
2. Monitors
3. Additional Hardware
4. Printers
5. Multi-function device (MFD) accessories. (Note: MFDs are covered by a separate IM/IT Standard in this Section.)

Where to Apply This Standard

The standard is intended for any ministry or other government agency that requires information about or is considering purchasing a workstation hardware product through SSBC Workstation Services.

Authority and Exemptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to facilitate the task of planning for and incorporating SSBC-approved workstation hardware products within the government's broad information systems environment.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security and government IT assets, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT workstation terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

The following documents are located on an internal government website. For more information please contact:

SSBC.ClientServices@gov.bc.ca

250-387-8045

1-877-387-8045

1. The SSBC Workstation Services list of supported workstations.
2. The SSBC Workstation Services list of additional hardware for workstations.
3. The SSBC Service Catalogue which includes frequently ordered workstation products, for both ministries and the broader public sector.
4. A detailed listing of *rates* for iStore ordering of workstation products, applicable to both ministries and the broader public sector.
5. A detailed listing of *lead times* for iStore ordering of workstation products, applicable to both ministries and the broader public sector.
6. A reference guide on standard workstation products and services entitled *Information Workstation Services – 06/07 Post Refresh Specifications*.
7. A graphical display of responsibilities for workstation costs.
8. A list of *Service Level Measurements* associated with the support of workstation products by SSBC Workstation Services.

Additional Information

Shared Services B.C. is the owner of this standard.

Contact

Shared Services B.C.

Phone: 250-387-8045 Toll Free: 1-877-387-8045

email: SSBC.ClientServices@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2007-11-06 Scheduled Review: Annual Last Updated: 2009-01 Last Reviewed: 2009-01</p> <p>Type: Product Standard</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.7 SSBC Workstation Services Supported Software Products</p>	
<p>Keywords:</p>	

Description of Standard

This standard is a definitive listing of workstation software products that are available through iStore and supported by SSBC Workstation Services.

These workstation software products are divided into three general areas:

1. Core – included as part of the standard software image on all workstations.
2. Supported – an additional product that can be ordered through iStore.
3. Line of Business – Ministry specific software, ordered through iStore.

In addition, the standard defines six support levels related to each of the above categories.

NOTE: unless approved by the Office of the CIO, software products acquired through iStore, including those originally installed on the workstation, cannot be used on employee owned computers. (See **References** below for this policy).

Where to Apply This Standard

The standard is intended for any ministry or other government agency that is requires information on or is considering purchasing workstation software through SSBC Workstation Services.

Authority and Exemptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to facilitate the task of planning for and incorporating SSBC-approved workstation software products within the government's broad information systems environment.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security and government IT assets, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT workstation terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

The following documents are located on an internal government website. For more information please contact:

SSBC.ClientServices@gov.bc.ca

250-387-8045

1-877-387-8045

1. The SSBC Workstation Services list of supported workstation software (*Productions of Primary Installation list*). This list is under review by the Software Standards Working Group (SSWG). When finalized, iStore will be updated to reflect any changes and additions.
2. The *Policy for Home Use of Government Software on Employee Owned Computers*.
3. The SSBC Service Catalogue which includes frequently ordered workstation products, for both ministries and the broader public sector.
4. A detailed listing of *rates* for iStore ordering of workstation products, applicable to both ministries and the broader public sector.
5. A detailed listing of *lead times* for iStore ordering of workstation products, applicable to both ministries and the broader public sector.
6. A reference guide on standard workstation products and services entitled *Information Workstation Services – 06/07 Post Refresh Specifications*.
7. A graphical display of responsibilities for workstation costs.
8. A list of *Service Level Measurements* associated with the support of workstation products by SSBC Workstation Services.

Additional Information

Shared Services B.C. is the owner of this standard.

Contact

Shared Services B.C.

Phone: 250-387-8045 Toll Free: 1-877-387-8045

email: SSBC.ClientServices@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2008-11-10 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Technical, Product and Reference</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.8 Network to Network Connectivity</p>	
<p>Keywords:</p>	

Description of Standard

This standard, which is composed of three sections, defines the connectivity requirements that must be addressed with respect to the connection between disparate networks. This includes connectivity to the SPAN/BC network and external service provider to external service provider networks.

1) Technical Standard:

a) Standard Components:

- **Connection Routers:** Each network to network connection must ensure appropriate logical, and if necessary physical, separation is achieved. A virtualized router may also be used, but logical separation needs to be guaranteed at all times (even in the event of device failure) through the use of appropriate controls.
- **Managed Router Access Control List (ACL):** The connection routers will be configured with a 'basic' ACL to deny/permit using the principle of least privilege, for access from the 3rd party network to the Provinces network or from 3-rd party network to another 3-rd party network. Separate ACL's, designed based on least privilege and using the "Deny All" as the default fall back rule, need to be configured and maintained on each interface in each direction (i.e. external vs. internal interfaces; inbound vs. outbound traffic directions) This access control list will be the first line of defense in a multi-layered protection strategy.
- **Firewall(s):** The firewall used must perform stateful packet inspection. Stateful Inspection Firewalls will be installed with the managed security rules permitting and denying access based on the principle of least access/privilege. **NOTE:** Devices that combine the Stateful Inspection Firewall and Routing functionality on one device are acceptable as long as the above requirements are met fully.
- **Intrusion Detection /Prevention System(s) (IDS/IPS):** IDS/IPS will be in place to monitor network traffic for security threats.
- **Content Filtering and Malware Protection:** Correction system(s) including content filters will be in place to screen for malicious code (viruses, etc.).

- **Data Leakage Protection:** Appropriate controls will be in place to ensure that data is prevented from being lost/leaked.
 - **Proxies: (optional)** HTTP Proxy server(s) can provide user authentication and DNS name translation for HTTP traffic if required.
- b) Security:** The principles of least privilege will apply.
- All ports will be closed by default and all IP addresses will be hidden by default. Opening of ports and IP addresses are requested by the Contract manager and must be approved by the data owner and the Ministry owning the contract.
 - Internal addresses will not be accessible by default. Requirements to connect to internal IP addresses will be addressed through the implementation of a Split DNS Service.
 - Minimum AES 128 encryption will be used for encryption. Encryption using keys of less than 128 bits are not acceptable. DES is not an acceptable encryption standard. If using 3DES encryption standard, the minimum key required is 168bit. Acceptable encryption standards include: 128bit AES, 168 bit 3DES.
- 2) **Product Standard:**
When one end of the connection is the SPAN network, then the Third Party Gateway (3PG) service must be used.
- 3) **Reference Standard:**
ISO/IEC 18028-3:2005 - Securing communications between networks using security gateways – will serve as the reference standard for network to network connectivity, specifically, the ISO Screened Subnet model.

Where to Apply This Standard

The standard is meant for SSBC, any ministry, other public agency or external service provider that is considering interconnecting networks that carries public sector information.

Authority and Exemptions

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.

Special note: For the time being a pre-existing policy directive issued in 2004 (see item 2 under References) still requires anyone connecting external networks to SPAN/BC to seek an exemption from the OCIO (whether this connectivity standard has been met or not). It is the intent that at the completion of the Network BC Project (JSRFP) this 2004 directive will be retired.

Metrics and Enforcement

SSBC offers secure network to network connectivity through the 3rd Party Gateway Service. Details of this Shared Services BC service offering can be found on the SSBC client website (see Reference #1 below).

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary which is currently under development by the OCIO.

References

1. A copy of the Submission for Network to Network Connectivity Technical and Product Standards can be found at www.cio.gov.bc.ca/local/cio/standards/documents/standards/n2n_connectivity.pdf
2. A memo from the Government Chief Information Officer (dated August 12, 2004) defined the Interim Standards for Information Systems Security and Network Connectivity. A copy of this document can be found at www.cio.gov.bc.ca/local/cio/standards/documents/standards/interim_n2n_standards.pdf
3. Security Schedule G: www.gov.bc.ca (TBD)

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, OCIO

email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2009-02-19 Scheduled Review: Annual Last Updated: 2009-02-19 Last Reviewed: 2009-02-19
	Type: Technical
5.0 Information Technology Management (CPPM 12.3.5)	
5.9 Technical Security Standard for Wireless Local Area Networks	
Keywords: Standard, Technical, Wireless, Conceptual, Mobility, WLAN	

Description of Standard

This standard describes the configuration parameters required for establishing a Secure Wireless Local Area Network, whether or not a device is directly connected to the SPAN/BC network.

The specifications documented here should be considered as Minimum Standards. If an implementer chooses a stronger option, it is permitted, but should be clearly noted in system documentation.

The National Institute of Standards and Technology Special Publication SP800-97, *Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i*, has been used extensively in development of this technical specification document.

Group	Topic	Current Standard	Comments / Rationale
Wireless Network Architecture	Robust Security Network (RSN)	IEEE 802.11 RSN consisting of only RSN Associations established using the 4-way handshake.	Only Robust Security Networks, which consist of only RSN Associations, are permitted. No Pre-RSN configurations are permitted. The 4-way handshake is used to validate possession of PMKs, establish temporal keys and select cipher suites.
	Protocol	WPA2-Enterprise	WPA is only permitted until hardware can be upgraded to support WPA2 with AES encryption.
	Protocol	WEP protocol must be disabled on APs and STAs.	WEP is not a secure wireless protocol.
	Network architecture	Access points configured as Extended Service Sets or Basic Service Sets. (i.e., infrastructure mode mandatory)	Independent Basic Service Sets (Ad-hoc mode) must be disabled on stations and access points.
	Network architecture	Must use an Authentication Server for keys.	Pre-shared keys must not be used for authentication due to significant management overhead in complex deployments.

Group	Topic	Current Standard	Comments / Rationale						
	Network architecture	Detection of Rogue APs mandatory	Implementation must be able to detect and disable unapproved APs.						
	Network architecture	Connection between AP and AS must be encrypted.	To prevent interception or manipulation of keys						
	Station configuration	STAs must be configured such that they authenticate to named servers only, and only accept certificates from the CA that signed the server certificates.	To prevent uncontrolled acceptance of invalid certificates						
Access Control	Authentication	Station authentication using an Extensible Authentication Protocol (EAP) method based on Transport Layer Security (TLS), one of: <table style="margin-left: 40px; border: none;"> <tr> <td style="text-align: center;">Preferred</td> <td style="text-align: center;">Minimal</td> </tr> <tr> <td>• EAP-TLS</td> <td>• LEAP*</td> </tr> <tr> <td>• EAP-TTLS</td> <td>• PEAP</td> </tr> </table>	Preferred	Minimal	• EAP-TLS	• LEAP*	• EAP-TTLS	• PEAP	EAP-TLS methods require the use of an enterprise PKI, with certificates deployed to each STA. STAs should be configured to only allow approved EAP methods.
	Preferred	Minimal							
	• EAP-TLS	• LEAP*							
• EAP-TTLS	• PEAP								
Access control	IEEE 802.1x port-based access control	The combination of EAP and 802.1x together support the establishment of RSNAs.							
Mutual Authentication	Mutual authentication between STA and AP	Mutual authentication is used to minimize the risk of masquerading access points.							
Cryptography & Key Management	Master Session Key / AAA key	MSK ≥ 256 bits							
	Pairwise Master Key	Maximum lifetime ≤8 hours PMK ≥ 256 bits							
	Group Master Key	Maximum lifetime ≤24 hours							
		GMK ≥ 128 bits (CCMP) GMK ≥ 256 bits (if using TKIP)							
	Transmission encryption	CCMP (with AES) Key ≥ 128 bits							

- There are known vulnerabilities related to LEAP.

Assumptions

- This standard applies to end-user devices, such as laptops, tablets and desktop workstations. This standard does not apply to ultra-mobile devices, such as PDAs and cell phones with wireless capability.
- This standard applies to wireless end-user devices that access information held within SPAN/BC.
- End-user and device-based authentication to the wireless network will be used (not user-based).
- The wireless network standard described here will only be used for known devices and users. Extensions may be developed and approved to accommodate guests, anonymous or public access.
- WPA using TKIP encryption is not permitted under the proposed standard. Organizations wishing to use WPA-Enterprise with TKIP must apply for an exception, using the process established by the GCIO.

Where to Apply This Standard

The standard is meant for SSBC, any ministry, other public agency or external service provider that is considering implementing a Secure Wireless Local Area Network that requires access to the SPAN/BC network.

Authority and Exemptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to minimize security exposures and maximize the privacy information traveling across the connected networks.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout Government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary, which is currently under development by the OCIO.

References

Information Security Policy

6.6 Communications and Operations Management – Network security management

6.6.1 A range of controls must be implemented to achieve and maintain security within the government network.

7.4 Access Control – Network access control

7.4.5 Groups of information services, users and information systems must be segregated on networks.

Additional Information

1. The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca
2. The full Architecture and Standard documentation can be found at:
www.cio.gov.bc.ca/local/cio/standards/documents/standards/wlan_connectivity.pdf.

Contact

Architecture and Standards, OCIO

email: ASB.CIO@gov.bc.ca

IM/IT Standards Manual Office of the Chief Information Officer Province of British Columbia	Effective Date: November 1, 2010 Scheduled Review: November 1, 2011
	Type: Technical Standard
5.0 Information Technology Management (CPPM 12.3.5)	
5.9.1 Technical Security Standard for Wireless Local Area Networks - Supplement	

Description of Standard

This standard describes the configuration parameters and security controls required for establishing a Secure Wireless Local Area Network whether or not a device is directly connected to the SPAN/BC network.

The specifications documented here should be considered as Minimum Standards. If an implementer chooses a stronger option, it is permitted, and should be clearly noted in system documentation.

The National Institute of Standards and Technology Special Publication SP800-97 *Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i* has been used extensively in development of this technical specification document.

Group	Topic	Current Standard	Comments/Rationale
Wireless hardware	Device certification	All wi-fi devices should be Wi-fi Alliance certified.	The Wi-fi Alliance published specifications for wireless device manufacturers. Devices that comply with these specifications are preferred.
Wireless network architecture	Robust Security Network (RSN)	IEEE 802.11 RSN consisting of only RSN Associations established using the 4-way handshake	Only Robust Security Networks, which consist of only RSN Associations are permitted. No Pre-RSN configurations are permitted. The 4-way handshake is used to validate possession of PMK's, establish temporal keys and select cipher suites.
	Protocol	WPA2-Personal	WPA2-Personal may only be used when the infrastructure required for WPA2-Enterprise or WPA-Enterprise is not available.
	Protocol	WPA-Personal MUST be disabled	WPA-Personal has published security weaknesses. WPA-Personal MUST be disabled.
	Protocol	WEP MUST be disabled	WEP is not a secure protocol and must be disabled.
	Protocol	Wi-fi Protected Setup (WPS)	WPS may be used, but the AP MUST reside in a secure location where an attacker would not be able to physically access the Push Button Configuration (PBC).
	Network architecture	Access points configured as Basic Service Sets (stand alone infrastructure mode).	Independent Basic Service Sets (Ad-hoc mode) must be disabled on station (STA) and access point (AP). Extended Service Set should only be used in WPA2-Enterprise or WPA-Enterprise deployments.

	Network architecture	Organizations must perform regular site surveys to detect rouge access points.	For the detection of rouge access points.
Access control	Pre-Shared Keys (PSK)	Maximum lifetime \leq 30 days PSK \geq 13 ASCII characters or PSK = 64 hexadecimal characters	ASCII PSK must be at least 13 characters in length to a maximum 63 characters. ASCII PSK must contain at least 3 of 4 of the following; one capital letter, one lowercase letter, one number, one special character. Hexadecimal PSK must be 256 bits consisting of 64 random or pseudo-random characters. The PSK must be changed immediately when any AP or STA on the WLAN is stolen or the confidentiality of the PSK is compromised (eg. The PSK is posted within an office or otherwise made accessible to unauthorized users). The PSK must be changed every 30 days.
	SSID	Maximum lifetime \leq 90 days SSID \geq 8 alpha-numeric characters	The SSID MUST contain numbers and alphabetic characters. Default SSID settings will compromise the strength of the PMK.
Cryptography & Key management	Pairwise Master Key	PMK \geq 256 bits	WPA-PSK derives the PMK from combining the PSK and SSID with other variables.
	Group Master Key	Maximum lifetime \leq 24 hours	
		GMK \geq 128 bits (CCMP)	
	Transmission encryption	CCMP (with AES) Key \geq 128 bits	

Assumptions

- This standard applies to end user devices such as laptops, tablets and desktop workstations. This standard does not apply to ultra-mobile devices such as PDAs and cell phones with wireless capability. Ultra-mobile devices are not permitted for use under this standard.
- This standard applies to wireless end user devices that access information held within SPAN/BC.
- The wireless network standard described here will be only used for known devices and users. Guest, public or anonymous wi-fi accesses are not covered by this standard.
- The standard defined in this update is not the preferred method for Secure Wireless Local Area Network connectivity and will be used only by organizations that are not able to implement WPA2-Enterprise.
- Organizations implementing this standard will abide by the sections of the BC Government Information Security Policy as listed in the references section below.

Where Standard is Used

The standard is meant for non-core government organizations that do not have the infrastructure required to implement WPA2-Enterprise, but have a business requirement for wireless local area network connectivity to government network resources.

Authority and Exceptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to minimize security exposures and maximize the privacy of information traveling across the connected networks. If there is a compelling business reason wireless networks should not or could not make use of this standard, the information systems director must address his or her concerns to the OCIO through a Request for Exception.

Metrics and Enforcement

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary which is currently under development by the OCIO.

References

IM/IT Architecture and Standards Manual section 5.9

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf

Information Security Policy

6.10 Communications and Operations Management – Monitoring

7.3 Access Control – User Responsibilities

9.1 Information Security Incident Management

9.1.2 Reporting Security Weaknesses

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, OCIO
ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual ARCHITECTURE</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2009-02-19 Scheduled Review: Annual Last Updated: 2009-02-19 Last Reviewed: 2009-02-19</p> <p>Type: Technical</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.10 High Level Architecture for Wireless Local Area Networks</p>	
<p>Keywords: Architecture, Technical, Wireless, Conceptual, Mobility, WLAN</p>	

Summary

The architecture presented in this document is classified as technical. It is conceptual in nature and vendor agnostic. Being vendor agnostic, this model can be implemented under a variety of vendor solutions. It is meant to provide guidance in the downstream development of detailed architectures and the selection of vendor solutions.

Authority and Exemptions

This architecture was developed by the OCIO (owner) in consultation with SSBC. The OCIO is responsible for its content.

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.

Business Context

The purpose of this architecture is to provide a conceptual view of core government wireless services and to support further development of detailed architecture. It supports IM/IT strategies for information sharing, improved secured access for a variety of client types, and supports an increasing mobile workforce. Similar design has been implemented in other jurisdictions and proven to be effective. The risks associated with this design are minimal.

ASDLC Requirements

This architecture should be reviewed upon completion of detailed architectural design and solution selection, and every 3 years thereafter. The OCIO or SSBC may both request update to this architecture.

Viewpoint

The viewpoint is "strategic planner". It is long-term and conceptual. Related projects include the SSBC Wi-Building project. The design aligns with existing security policy.

State

There is no preceding conceptual architecture. This model will be used in the SSBC Wi-Building Service, which should be available in the 2009/10 fiscal year.

Description of the Architecture

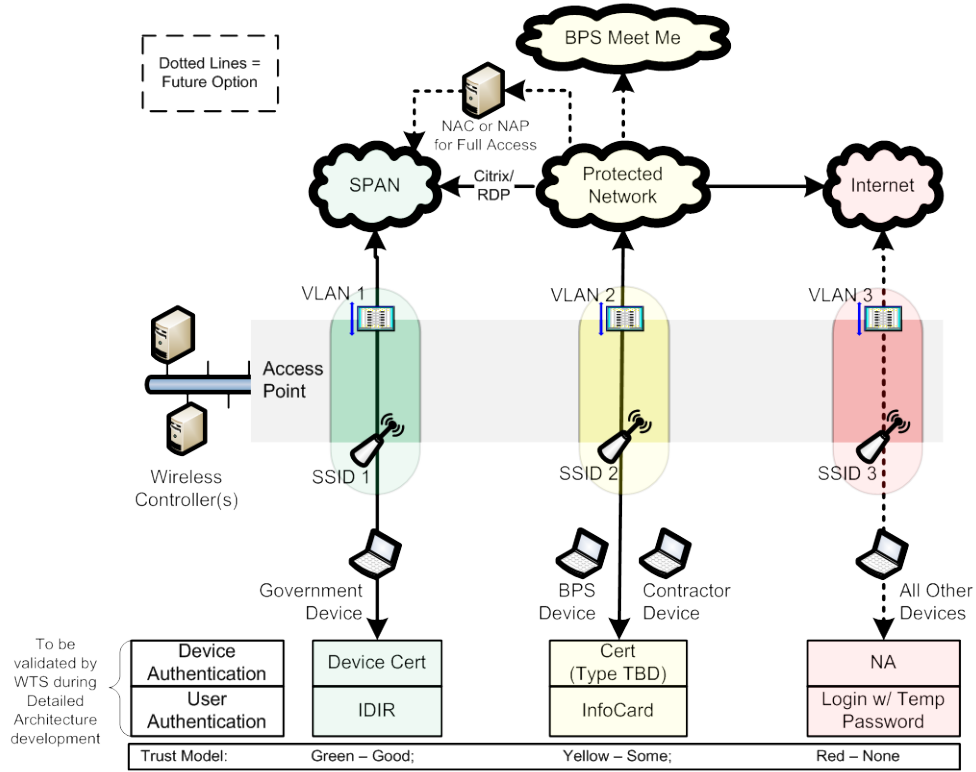
This architecture describes a design for establishing a Secure Wireless Local Area Network. The model allows for 3 classes of devices to gain access to SPAN wireless services:

1. **Trusted devices:** Core government-managed devices have direct secure access onto the SPAN network (see green below).
2. **Semi-Trusted Devices:** As an example, broader public sector devices are given access to a protected area from which they can securely access their own or other private network spaces (see yellow below). This may include contractors and consultants under contract to the government.
3. **Un-trusted Devices:** Devices over which the government cannot exert control (physically or by policy or contract) or those devices that pose an indeterminate risk are given access to the Internet (see red below). An example is vendors that require access in order to provide on-site presentations.

Under all scenarios, access is controlled. This may be through either device certificates and/or user passwords. Smart cards may also be a future option for authentication.

Access from the protected network back into SPAN will be through Citrix or RDP. Upon the availability of a Network Access Protection/Network Access Control capability, direct access may be allowed.

The lower section of the diagram will be finalized once detailed architectural design and vendor select is complete, as some capabilities may vary with the final vendor solution.



Additional Information

The full Architecture and Standard documentation can be found at:

www.cio.gov.bc.ca/local/cio/standards/documents/standards/wlan_connectivity.pdf

Contact

Architecture and Standards Branch, OCIO

email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2008-11 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <hr/> <p>Type: Process Standard</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.11 Security Threat and Risk Analysis Standard for Implementing Wireless Local Area Networks</p>	
<p>Keywords:</p>	

Description of Standard

This standard defines the security controls required for establishing a Secure Wireless Local Area Network that is part of the SPAN/BC network. There is an associated Technical Standard that describes the configuration parameters required for a Secure Wireless Local Area Network.

The specifications documented here should be considered as Minimum Standards. If an implementer chooses a stronger option, it is permitted, but should be clearly noted in system documentation.

The National Institute of Standards and Technology Special Publication SP800-97 *Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i* has been used extensively in development of this technical specification document.

Security Control Objectives and Process Standard

A set of security control objectives and security controls for Secure WLAN have been developed and comprise the Secure WLAN Process standard.

In order to simplify and streamline the threat and vulnerability analysis process, the Process standard has been constructed in the format of the Information Security Forum Healthcheck. The standard takes the form of “answers” to each of the relevant Healthcheck questions.

This approach eliminates the need for implementers and security analysts to translate between different formats when conducting threat and vulnerability analysis using the ISF Information Risk Analysis Method (ISF IRAM) tool. The approach will lead to greater certainty and consistency in risk analysis.

The format of this standard has been carefully constructed to streamline and simplify compliance verification and security threat and vulnerability analysis.

The standards writers selected the subset of ISF Healthcheck questions that are relevant directly to WLAN. For each question, the control standard is stated in the form of the answer that is expected of the in-scope organization. When using this standard for compliance checking, documented evidence is required as indicated within the answer text.

Security control objectives for Secure WLAN

The security control objectives that must be met by Secure WLAN security controls are:

#	Secure WLAN Control Objective
1	An "information security architecture" should be established, which provides a framework for the application of standard security controls throughout the enterprise.
2	Only software and hardware which has been generally proven to be reliable and robust should be used. All hardware and software must be recorded in an inventory.
3	All buildings within the enterprise that house critical IT facilities (e.g. data centres, network facilities and key user areas) should be physically protected against accident or attack.
4	Critical computer equipment and facilities should be protected against power outages.
5	Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.
6	Critical applications should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.
7	The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.
8	Systems should be configured to provide authorized functionality, and to prevent unauthorized or incorrect updates or elevated access to unauthorized users.
9	Workstations connected to systems within the computer installation should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.
10	Network devices should be configured to provide authorized functionality, and to prevent unauthorized or incorrect updates.
11	Networks should be supported by accurate, up-to-date documentation.
12	Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation.
13	All users of the computer installation should be authorized using documented procedures before they are granted access privileges.
14	All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (e.g. smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.
15	Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorized change.
16	Key network activities should be monitored.
17	Virus protection arrangements should be established, and maintained enterprise-wide.
18	Intrusion detection mechanisms should be applied to critical systems and networks.
19	Network traffic should be routed through a firewall, prior to being allowed access to the network.
20	Wireless access should be authorized, authenticated, encrypted and permitted only from approved locations/devices.
21	Cryptographic keys should be managed tightly, in accordance with documented standards/ procedures, and protected against unauthorized access or destruction.

22	Any public key infrastructure (PKI) used by the application should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.
23	Sensitive information held on data storage media (including magnetic tapes, disks, printed results and stationery) must be protected against corruption, loss or disclosure.
24	Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.

Secure Wireless Local Area Network controls

ISF HealthCheck question	Control standard for a large, complex organization
Local security co-ordination	
12 Are local security coordinators competent to carry out their security responsibilities?	Security coordinator/manager has been trained and as a result is aware of current wireless security issues. The job description of the security coordinator/manager includes responsibility for IT security, which includes network and wireless security.
Roles and responsibilities	
23 Are responsibilities for key security tasks assigned to individuals who are capable of performing them?	Individuals responsible for key security tasks have been trained, regularly update their knowledge and awareness. Note: certifications for security or wireless security may indicate training and knowledge
26 Has reliance on key individuals been minimized (e.g. by automating tasks, ensuring complete and accurate documentation, and arranging alternative cover	Reliance on key individuals has been minimized by cross-training, using established processes to maintain complete/current documentation and job task coverage.
Confidentiality requirements	
32 Does the organization assess the impact of business information being disclosed to unauthorized individuals?	The standard Business Impact Assessment for Wireless HAP has been reviewed, analyzed for applicability to the organization. Or, a new business impact assessment has been conducted which includes analysis of unauthorized disclosure, integrity failure and unavailability impacts, and is regularly reviewed. Privacy Impact Assessments have been completed as required.
Integrity requirements	
33 Does the organization assess the impact of business information being accidentally corrupted or deliberately manipulated?	Same answer as Q32.
Availability requirements	
34 Does the organization assess the impact of business information being unavailable?	Same answer as Q32.
Security architecture	
35 Is an 'information security architecture' established to implement consistent, simple-to-use security functionality across multiple computer systems?	Security models, controls and configurations are documented and conformance is checked. Security processes are documented and compliance to them is assessed.
36 Does the 'information security architecture' enable standard security controls to be applied throughout the enterprise?	For the wireless network and supporting infrastructure, the information security architecture is consistently applied.
Asset management	

ISF HealthCheck question	Control standard for a large, complex organization
37 Are proven, reliable and approved computer systems used?	Equipment has been evaluated to be proven, reliable and secure prior to purchase. Vendors have been selected that meet equipment quality, reliability, availability, security, support and technical requirements and are approved by the organization to supply equipment.
38 Do computer systems meet security requirements?	Same answer as Q37
39 Is essential information about hardware and software (e.g. unique identifiers, version numbers and physical locations) recorded in inventories?	An inventory of hardware and software is maintained, including identifiers, quantities, physical locations, and may include version numbers. The inventory is updated regularly and is verified periodically
Physical protection	
41 Are buildings that house critical IT facilities physically protected against accident or attack?	(Question re-directed to wireless focus) The critical wireless access components, including configuration servers, authentication servers, management computers and servers are physically protected using combinations of: Secure locked rooms/cabinets; no accessible windows; monitored alarm systems; no unattended devices in open areas.
42 Is physical access to buildings that house critical IT facilities restricted to authorized individuals?	(Question redirected to wireless focus) Physical access to the wireless networking components is restricted to authorized individuals by only issuing keys to authorized individuals.
43 Is critical computer equipment and documentation protected against theft?	(Question redirected to wireless focus) Portable devices are physically secured to deter theft by use of cables or chains, labeling of equipment, and training of staff to detect theft. Access to documentation is controlled. Access points and other wireless networking components are physically secured against theft by various means, equipment is labeled for ownership.
Power supplies	
44 Are critical computer equipment and facilities protected against power outages?	{If the wireless network is critical to doing business, then} the wireless network components are supported by backup power.
Hazard protection	
45 Are computer equipment and facilities protected against fire, flood, environmental and other natural hazards?	{If the wireless network is critical to doing business, then} the components are protected from fire, flood and natural hazards by location in areas free from intrinsic fire hazards; fitted with fire detection and suppression systems; and protected against the spread of fire.
Resilience	
46 Are systems supported by alternative or duplicate facilities?	The wireless network is implemented to ensure that single points of failure are minimized.
Installation and network design	
50 Are systems designed with sufficient capacity to cope with predicted information processing requirements?	The wireless network is planned, designed and monitored for utilization and capacity to ensure sufficient capacity exists.
51 Are systems protected by using a range of in-built security controls?	The wireless network uses only built-in security features of the manufacturer, and no custom security add-ons.
Host system configuration	

ISF HealthCheck question	Control standard for a large, complex organization
52 Are host systems configured to function as required?	The servers providing and controlling access to the wireless network are hardened, managed and operated according to documented organizational standards.
53 Are host systems configured to prevent unauthorized or incorrect updates?	Servers are configured to only allow system and software modifications by authorized system administrators.
Workstation configuration	
54 Are workstations purchased from a list of approved suppliers?	Workstations are purchased from a list of approved suppliers and obsolete computers are removed from service in a timely manner.
55 Are workstations tested prior to use?	Workstations are tested prior to deployment using standard procedures.
56 Are workstations supported by maintenance arrangements?	Workstation support is provided by: A process is in place to replace/refresh workstations regularly to ensure that current, supported, maintainable equipment is used.
57 Are workstations protected by physical controls?	Workstations are protected using physical controls to prevent or deter theft, such as: physical attachment to large or immobile furniture and/or encasing the device; clear, conspicuous ownership labels; regular inventory and training staff to notice equipment out of place. Physical protection for protection of displayed information is achieved through use of privacy screens or situating the device to prevent unauthorized viewing. Measures are implemented to minimize risks when devices are left unattended during emergency situations.
58 Do workstations 'time-out' after a period of inactivity?	((This answer must be addressed by risk assessment and is situational - compensating controls must be in place for non-detaching devices)) Workstations are configured to timeout after a period of inactivity as required by security and compliance standards to ensure that personal information is not visible and prevent unauthorized access using one or more of: password-protected screen saver; auto-logout; auto-disconnect. To reconnect, users are required to re-authenticate.
Configuring network devices	
59 Are network devices configured to function as required?	Wireless access points and controllers use a standard, enforced configuration. Refer to the technical standard for details.
60 Are network devices configured to prevent unauthorized or incorrect updates?	Wireless networking equipment is protected from unauthorized configuration changes through use of individual administration accounts, access controls and change logs.
Network documentation	
61 Are networks supported by accurate and up-to-date documentation?	Network and configuration documentation exists, is accurate and is verified regularly.
Access control	

ISF HealthCheck question	Control standard for a large, complex organization
62 Is access to information and systems restricted to authorized individuals?	(Question interpreted as access to the network by devices) Access to the wireless network is protected using strong device identification such as EAP. See technical standard for details. Note: it is assumed that the wireless network is private and considered to be part of the internal network - there should be no unauthorized devices connected.
63 Do access control arrangements restrict access to only approved system capabilities?	(As applied to the mobile wireless device) Access controls are implemented to restrict access to approved system capabilities on the end device to authorized individuals.
User authorization	
64 Are users authorized before access privileges are granted?	Note: this control standard applies to wireless networks that do not rely on user authentication for connection, but on device authentication. It is assumed that users are required to be authorized and authenticated by the workstation and applications, but not the network. As the question applies to device authorization: Only authorized devices are permitted to attach to the wireless network
65 Is there a process to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts?	(Question interpreted as related to device management) Processes are established to manage device authorization to attach and use the wireless network, including processes to remove access in a timely manner.
User authentication	
66 Are users authenticated before access is granted to target systems?	Note: this control standard applies to wireless networks that do not rely on user authentication for connection, but on device authentication. It is assumed that users are required to be authorized and authenticated by the workstation and applications, but not the network. As the question applies to device authentication: See Q62
Sign-on process	
68 Are users subject to a rigorous 'sign-on' process before they gain access to target systems?	Note: this control standard applies to wireless networks that do not rely on user authentication for connection, but on device authentication. It is assumed that users are required to be authorized and authenticated by the workstation and applications, but not the network. As the question applies to device authentication: See Q62
Event logging	
69 Are logs of key events maintained?	Logs of key events are kept for items such as: device attachment; certificate issued; certificate revoked; invalid connection attempt.
70 Are logs of key events reviewed periodically?	Logs of key events are reviewed at least weekly for patterns or automated alerts generated that may indicate attacks or break-ins.
71 Are logs of key events protected against unauthorized change?	Logs are protected from tampering or deletion by access control mechanisms, backups, and read-only permissions as appropriate.
System / Network monitoring	
72 Are computer systems monitored to identify potential security breaches?	Wireless networks are monitored to identify potential security breaches through use of tools and reports.

ISF HealthCheck question	Control standard for a large, complex organization
73 Does system monitoring include scanning host systems for known vulnerabilities?	Processes are implemented to detect unauthorized or mis-configured wireless network devices. (for example, processes may include active scanning, monitoring, vulnerability detection and management, configuration management and rogue access point detection)
74 Does system monitoring include checking whether powerful utilities/commands have been disabled on attached host systems?	Controls and processes are in place to ensure that powerful utilities are not available to end-users connected to the network.
75 Does system monitoring include checking for the existence and configuration of unauthorized wireless networks?	The organization's environment is configured or monitored to detect unauthorized access point hardware, and frequently scanned to detect broadcasts from unauthorized wireless networks in the organization's airspace. Policy and processes are implemented to actively disable or remove unauthorized hardware.
Virus protection	
90 Do virus protection arrangements cover workstations (including laptops?)	Virus protection policy, tools and processes are implemented, and cover workstations.
91 Is virus protection software kept up-to-date?	Virus protection software is kept up-to-date
Intrusion detection	
93 Are intrusion detection mechanisms applied to critical systems (e.g. using HIDS)?	Host-based intrusion detection is implemented for critical systems that support the wireless environment (e.g. the PKI servers, and configuration servers). Note: this may be achieved using features of some antivirus product suites.
94 Are intrusion detection mechanisms applied to networks (e.g. using NIDS)?	Networks are configured and technology implemented to prevent, detect and/or eliminate unauthorized/unwanted malicious traffic on the organizations' internal wireless network. Note: It is recommended that the organization implement automated NIDPS systems on the wired networks that are accessed via the wireless networks. For organizations that choose to not implement NIDPS, compensating controls must exist and address the issue in the organization's network security operations.
Firewalls	
106 Is network traffic routed through a firewall, prior to being allowed access to target systems?	Network traffic to the target systems is controlled using firewalls, access control lists or network filters.
Wireless access	
111 Is wireless access authorized only from approved locations?	Wireless access is available from approved devices (i.e. locations). EAP is used to restrict access to only authorized devices (i.e. Locations). Refer to the technical standard for details on authorization methods.
112 Is wireless access encrypted?	Wireless access is encrypted using. Refer to the technical standard for details regarding key lengths, algorithms and other parameters.
113 Is wireless access protected using a VPN (Virtual Private Network)?	Note: it is assumed that the wireless network is an internal, private network and is not managed as a public-access network. {If the wireless network is publicly available,} internal network access is protected using VPN technology from the mobile device to the corporate network.
Information privacy	

ISF HealthCheck question	Control standard for a large, complex organization
125 Are security controls for handling personally identifiable information applied?	Mobile devices attached to the wireless network have security controls implemented to protect personally identifiable information, as specified in the Privacy Impact Assessment (see Q126).
126 Does the organization comply with legal and regulatory requirements for information privacy?	A Privacy Impact Assessment has been conducted, reviewed and approved for the wireless network implementation.
Cryptography	
127 Are cryptographic solutions used to protect the confidentiality of sensitive information?	Cryptographic solutions are used to protect data in transit by encryption of wireless network traffic; and at rest by encrypting workstation hard drives. See technical standard related to Q112 for details.
128 Are cryptographic solutions used to preserve the integrity of critical information?	Cryptographic solutions are used to protect data in transit by encrypting wireless network traffic using protocols that have integrity protection features. See technical standard related to Q112 for details.
130 Are cryptographic solutions approved and documented?	Cryptographic solutions are documented, including technology and processes related to key provisioning, key management, cryptographic algorithms. See technical standard related to Q112 for details.
131 Are cryptographic keys managed tightly (e.g. to protect them against unauthorized access or destruction)?	Key management processes are documented, verified at least annually, and includes processes for creating/issuing keys, monitoring for loss/compromise, and rapid revocation of expired or stolen keys.
Public key infrastructure	
132 Where a Public Key Infrastructure (PKI) is used, is it protected by 'hardening' the underlying operating system(s)?	The PKI implemented to support EAP device authentication is protected through use of dedicated servers with access restrictions and measures to protect the root certificates.
133 Where a public key infrastructure (PKI) is used, is it protected by restricting access to Certification Authorities?	The PKI implemented to support EAP device authentication is protected through use of offline root certificate servers and other protective measures
Business continuity	
147 Are business continuity plans developed?	The wireless network is considered in the formal, documented business continuity and disaster recovery plans.
148 Are business continuity plans supported by contingency arrangements?	{If the wireless network is critical to your business, then} the BCP has contingency arrangements for it.
149 Are business continuity plans tested periodically?	{If the wireless network is critical to your business, then} the continuity plans for the wireless network are tested periodically.
Security audit/review	
150 Do security audits/reviews provide the system 'owner', and top management, with an independent assessment of the security status of the system?	The wireless network is included in regularly scheduled security audit/review plans to provide information about the security status of the network
151 Are security audits/reviews performed on a regular basis?	The wireless network is assessed at least semi-annually
152 Are security audits/reviews independent?	Independent reviews of the wireless network are conducted at least bi-annually.
Handling information	

ISF HealthCheck question	Control standard for a large, complex organization
165 Is sensitive information held on data storage media (including magnetic tapes, disks, printed results, and stationery) protected against corruption, loss or disclosure?	Mobile devices attached to the wireless network have security controls implemented to protect sensitive information, as specified in the Privacy Impact Assessment (see Q126). Asset disposal policy and processes are in place to ensure that sensitive information is disposed securely.
Acquisition	
170 Are security requirements considered when acquiring computer systems?	(Question refocused on wireless networking.) Security requirements have been considered in the wireless network design and specifications.
171 Are security deficiencies in computer systems identified?	Same answer as Q170
172 Are robust and reliable computer systems acquired?	Equipment has been evaluated to be proven, reliable and secure prior to purchase. Vendors have been selected that meet equipment quality, reliability, availability, security, support and technical requirements and are approved by the organization to supply equipment. (See Q37)
173 Are adequate software licenses acquired for planned use?	An inventory of software licenses is maintained, and regularly verified to ensure license compliance.

Assumptions

- Device-based authentication to the wireless network will be used (not user-based)
- The wireless network standard described here will be only used for known devices and users (no guests, anonymous or public access permitted)
- WPA using TKIP encryption is not permitted under the proposed standard. Organizations wishing to use WPA-Enterprise with TKIP must apply for an exception using the process established by the GCIO.

Where to Apply This Standard

The standard is meant for SSBC, any ministry, other public agency or external service provider that is considering implementing a Secure Wireless Local Area Network as part of the SPAN/BC network.

Authority and Exemptions

This standard has been issued by the Office of the Chief Information Officer (OCIO) to minimize security exposures and maximize the privacy information traveling across the connected networks

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary which is currently under development by the OCIO.

References

1. 6.6 Communications and Operations Management – Network security management
 - 6.6.1 A range of controls must be implemented to achieve and maintain security within the government network.
- 7.4 Access Control – Network access control
 - 7.4.5 Groups of information services, users and information systems must be segregated on networks.
2. A copy of the Submission for Security Threat and Risk Analysis Standard for Implementing Wireless Local Area Networks can be found at:

www.cio.gov.bc.ca/local/cio/standards/documents/standards/wlan_implementation.pdf

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2010-08-16 Scheduled Review: Annual Last Updated: Last Reviewed:
	Type: Technical and Product Standard
5.0 Information Technology Management (CPPM 12.3.5)	
5.12 Unified Communication Federation Standard	
Keywords: OCS, Advanced Communications, messaging	

Description of Standard

The Province currently uses Microsoft Office Communication Server (OCS) as the strategic platform for delivering Unified Communications to core government. OCS is capable of federating with a variety of other unified communication solutions.

This standard defines essential functional restrictions and the minimum requirements for the federation of Unified Communications between core government, broader public sector, and third parties.

There will be three categories of standards that apply; Technical, Product and Configuration.

1) Technical Standards:

- IETF RFC 3428 SIP: Session Initiation Protocol (SIMPLE extension)
- IETF RFC 5246 The TLS Protocol v1.2
- IETF RFC 3711 SRTP: Secure Real-time Transport Protocol
- Cryptographic Standards for Information Protection
http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf

2) Product Standard:

The current strategic product for unified communications is Microsoft OCS with Microsoft Communicator on the desktop. The current architecture only supports federated connections to other Microsoft OCS implementations.

3) Configuration Standards:

- Auto-federation options will be disabled. Federated partners will be managed with an explicit permit list.
- Phishing protection - Hyperlinks will be converted to plain text, and pre-pended with an underscore.
- Protection of privacy – Discovery of federated contacts will only be permitted through the use of a known, complete SIP address.
- Malware protection – File transfer of executable file types will not be permitted. (see section 7.1 “Characteristics and Standard” for complete list of blocked file extensions).
- Encryption – End to end communication will be encrypted with TLS v1.2 or above.
- A public trusted certificate authority must be used.

- Polite blocking will be used for users who reject subscription requests. Polite blocking does not indicate to the blocked watcher that they have been blocked from viewing a user's presence state.

Future Requirement

- Call Detail Records (CDR) records will be retained for investigation and enforcement of data leakage violations. SSBC should deploy CDR logging on or before the next unified communications upgrade, within two years of the adoption of this standard, or when a material change to the delivery of this service should occur.

Future Recommendations

- As end users are required to comply with FOIPPA, a hyperlink to FIOPPA compliance information should be displayed either when the UC client launches or at the start of an IM session.
- Federation with private non-OCS based unified communication systems is not permitted until such time that CDR logging is implemented and a separate STRA and PIA have been completed to assess security risks that may be introduced as a result of changes to this service.

Where to Apply This Standard

The Unified Communication Federation Standard is intended for use by government to extend the reach of Instant Messaging, Presence information, and other ACCS features to broader public sector entities and external business partners.

Authority and Exemptions

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, SSBC is expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary which is currently under development by the OCIO.

References

Core Policy and Procedures Manual – chapter 12
Information Security Policy version 1.2 sections 6.8, 6.10.1 and 8.5.4
<http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf>

Contact

Phone: 250-952-6913 Email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual ARCHITECTURE Office of the Chief Information Officer Province of British Columbia	Effective Date: 2010-08-16 Scheduled Review: Annual Last Updated: Last Reviewed:
	Type: Technical Architecture
5.0 Information Technology Management (CPPM 12.3.5)	
5.13 Technical Architecture for Unified Communication Federation	
Keywords: OCS, Advanced Communications, messaging	

Summary

The architecture presented in this document is classified as high level technical.

Authority and Exemptions

This architecture was abstracted from the detailed technical architecture developed by SSBC in consultation with the ASB. The ASB and SSBC are jointly responsible for this architecture.

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.

Business Context

The purpose of this architecture is to provide a conceptual view of core government Unified Communications services and provide an extension to the detailed architecture. It supports IM/IT strategies for information sharing improved secured access for a variety of client types and support for an increasing mobile workforce. Similar design has been implemented in other jurisdictions and proven to be effective. The risks associated with this design are minimal.

ASDLC Requirements

This architecture should be reviewed May 30 and every 1 year thereafter. SSBC may request update to this architecture.

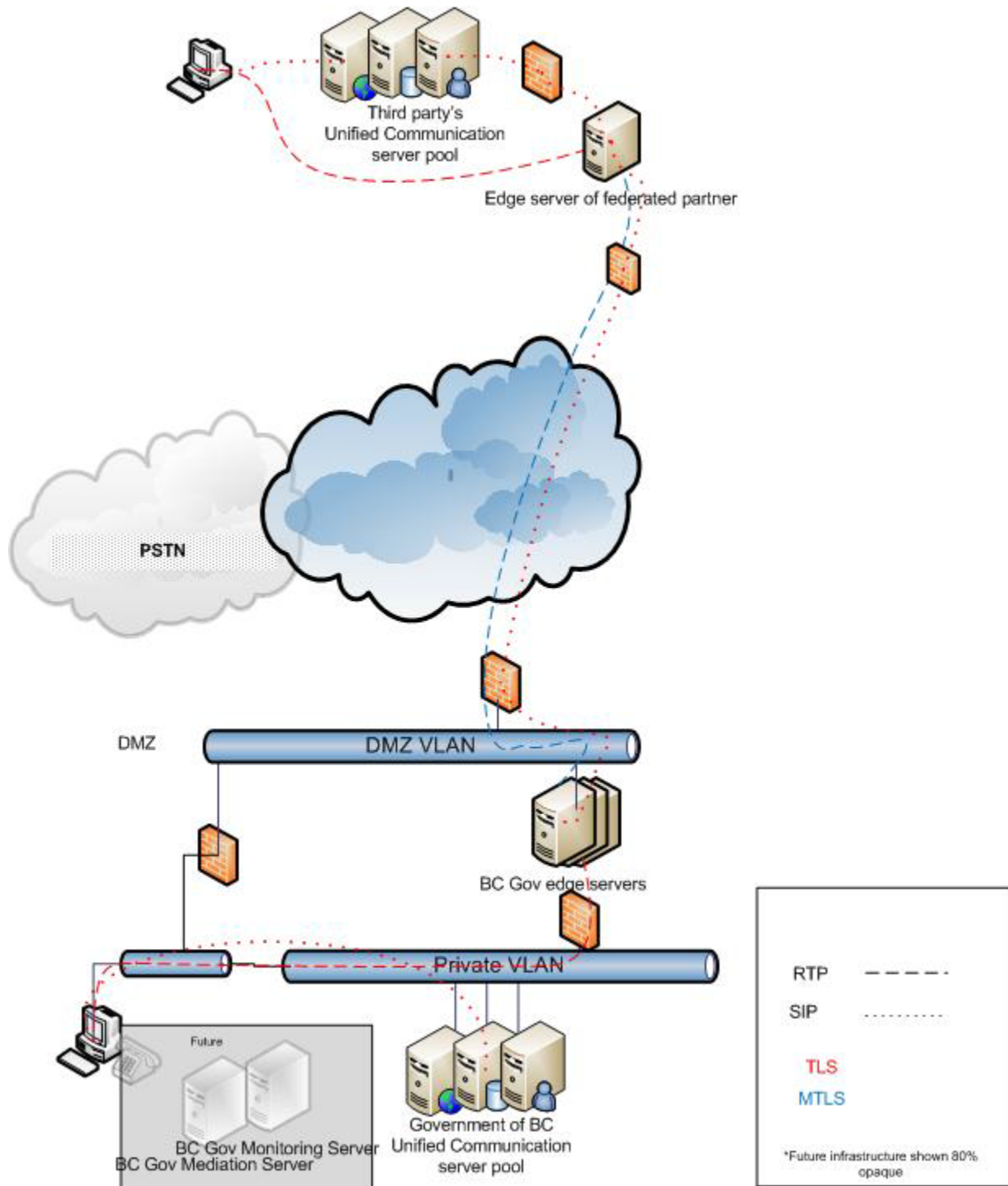
Viewpoint

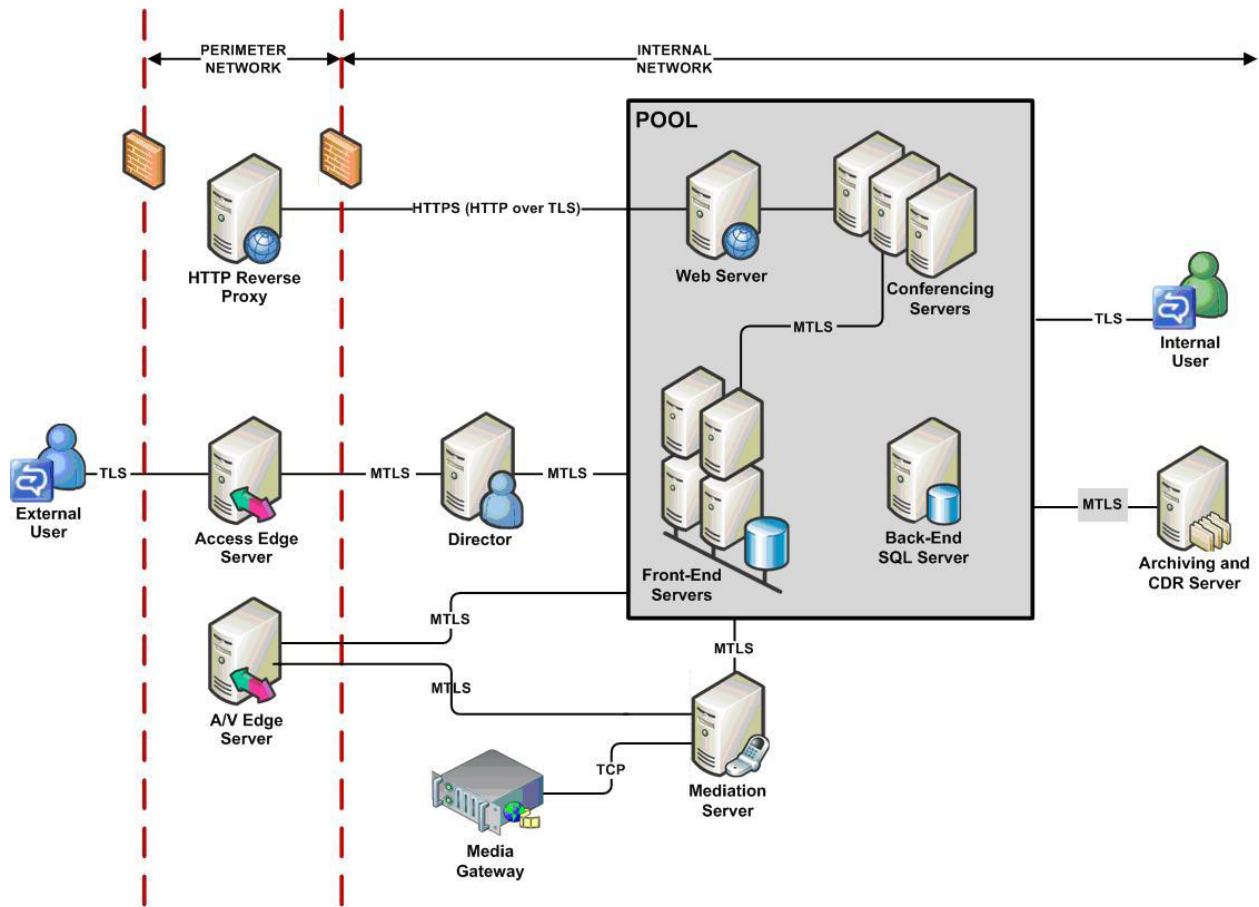
The viewpoint is strategic technical. It is long term and high level detail in nature. Related projects include ACCS. The design aligns with existing security policy.

State

There is no preceding conceptual architecture. This model will be used in existing services.

Description of the Architecture





Additional Information

Authority and Exemptions

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.

Contact

Architecture and Standards Branch

Phone: 250-952-6913 email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2011-11-09 Scheduled Review: Annual Last Updated: 2011-11-09 Last Reviewed: 2011-11-09</p>
	<p>Type: Product</p>
<p>5.0 Information Technology Management (CPPM 12.3.5)</p>	
<p>5.14 Tools for Collaboration with External Business Entities</p>	
<p>Keywords: Skype, WebEx, Collaboration</p>	

Description of Standard

Skype and Cisco WebEx may be used for collaboration with external entities that do not use the government standard products (OCS and Livemeeting). Users must use the government (POPI) prepackaged version of Skype and WebEX to ensure security configurations meet government security requirements. However,

- Internal (government device to government device) collaboration must continue to use OCS and Livemeeting.
- Internal to external collaboration, where the external entity uses OCS and LiveMeeting, must utilize federation (5.13 Unified Communication Federation Standard).

Where to Apply This Standard

This standard is to be applied to Government owned workstations.

Authority and Exemptions

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

A *Products of Popular Installation* image of Skype or WebEx must be used for installation on Government owned workstations.

All Government users of Skype must use anti-virus protection and must ensure that virus definitions are kept updated in accordance with Information Security Policy section 6.4.1 – Prevention and Detection Controls.

All Government users of Skype must use strong password, and should change them regularly as per Government [IM/IT Standards Manual 6.7 Password Standard, and Information Security Policy – Access Control – User Responsibilities 7.3.1](#)

All Government users of Skype must ensure that they do not check “remember my password” when using Skype on a shared or public computer.

Terms and Definitions

Strong password – A combination of upper-case, lower-case numbers and/or symbols with a minimum length of 8 characters and should not be derived from dictionary words, or proper nouns such as an individual's name. See Information Security Policy section 7.3.1.

References

Key references used in the development of this standard:

Skype IT Administrator's Guide version 2.0

<http://download.skype.com/share/business/guides/skype-it-administrators-guide.pdf>

IT Administrator Guide for Mass Deployment of WebEx

http://support.webex.com/US/PT/wx_pt_ag.pdf

IM/IT Standards Manual – 6.7 Password Standard

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf

Information Security Policy – 7.3.1 – Access Control – User Responsibilities

<http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf>

Unified Communication Federation Standard (Section 5.12)

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf

Guidelines for Conducting Citizen Engagement, Specific to Social Media

http://www.gov.bc.ca/citz/citizens_engagement/some_guidelines_master.pdf

Policy Summary No. 33 – *Use of Social Media in the B.C. Public Service*

http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/summaries/33_social_media.pdf

Contact

Chris Lyons,

Architecture and Standards Branch, OCIO

Phone: 250-356-1892

email: christopher.lyons@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2002-04-29 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
Office of the Chief Information Officer Province of British Columbia	Type: Technical Standard
6.0 INFORMATION TECHNOLOGY SECURITY (CPPM 12.3.6)	
6.1 Use of Employee Desktop Computers as Servers	
Keywords:	

Description of Standard

This standard affirms that employee computers cannot be used as servers except for circumstances that must be reviewed and approved by Shared Services B.C. security personnel.

Where to Apply This Standard

The standard is meant for any government employee or contractor that has been assigned a personal computer.

Authority and Exemptions

This standard has been issued by the OCIO because personal computers configured as servers do not conform to the government's server standards (i.e., using proper security, firewall, Domain Name System [DNS], backup, maintenance and anti-virus measures). These improperly configured servers also pose a threat to the government's network, as they provide opportunities for individuals to bypass government's infrastructure protection measures.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage the security of the government network, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated April 29, 2002) defined the standard for the use of employee computer as servers. A copy of this document can be found at:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/computers_as_servers_memo_20020429.pdf.

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2004-10-07 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
	Type: Technical Standard
Office of the Chief Information Officer Province of British Columbia	
6.0 Information Technology Security (CPPM 12.3.6)	
6.2 Web Traffic Filtering	
Keywords: Proxy Avoidance	

IMPORTANT: Name Changed from **Proxy Avoidance**

Description of Standard

This standard states that users within the government network cannot bypass website blocking mechanisms except for circumstances that must be reviewed and approved by Shared Services B.C. security personnel.

Where to Apply This Standard

The standard is meant for anyone who uses the government network.

Authority and Exemptions

This standard has been issued by the OCIO because some users are bypassing website blocking mechanisms and accessing inappropriate websites using a method called proxy avoidance. This technique uses a non-government proxy web server to bypass the site filtering provided by Websense® as mandated by the OCIO.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage the security of the government network, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

The OCIO has activated a Proxy Avoidance blocking category on Websense® to reduce the ability to bypass the existing blocks and gain access to inappropriate web sites. In addition, information systems directors are being notified in advance to determine if there are instances where staff are using proxy avoidance as a legitimate requirement.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated October 7, 2004) defined the standard for proxy avoidance. A copy of this document can be found at:
http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/proxy_avoidance_memo_20041007.pdf

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
Phone: 250-952-6970 email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2000-08-02 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
Office of the Chief Information Officer Province of British Columbia	Type: Technical Standard
6.0 Information Technology Security (CPPM 12.3.6)	
6.3 Internet Filtering of Well Known Ports	
Keywords:	

Description of Standard

This standard states that well-known ports will be filtered on government servers that control IP traffic between the Internet and the SPAN/BC network.

Where to Apply This Standard

This standard is targeted at web-based electronic service delivery initiatives that are being designed and implemented by ministries and other government agencies.

Authority and Exemptions

This standard has been issued by the OCIO because the filtering of access to certain ports from the Internet prevents a security vulnerability known as port scans. These port scans are the equivalent of trying all the doors and windows on a house to see which ones are vulnerable. Port scanning can identify not only which ports are vulnerable but also which ones in a given range have an intelligent device connected to it. These scans are often the precursor to attacks on the government server infrastructure.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage the security of the government network, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. A White Paper (dated August 2, 2000) presented by the Information Security Branch (formerly ISTA/ITSD Security Services) to the Technology Architecture Forum defined the rationale and standard for Internet filtering of well-known ports. A copy of this document can be requested from the contact below.
2. A form for requesting an exemption to this standard, which is intended for internal use within government, can be obtained through the Information Security Branch at the contact below.

Additional Information

The Information Security Branch, OCIO, is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Corporate Planning & Policy
Information Security Branch, OCIO
email: CITZCIOSecurity@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2004-08-12 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01 Type: Technical Standard
6.0 Information Technology Security (CPPM 12.3.6)	
<p style="text-align: center;">6.4 Interim Standards for Information Systems Security and Network Connectivity</p>	
Keywords: SiteMinder, IDIR, BCeID, Common Logon Pages, CLP, Enterprise Security Gateway, Authentication, User	

Description of Standard

The intent of these interim standards is to guide ministries and their solution providers in structuring the security and related network connectivity of information systems solutions. These standards define:

- *Government Authentication Standards* - ministries must ensure that information systems solutions utilize the government's Enterprise Security Gateway services (which includes SiteMinder, IDIR, BCeID) and technology for user identity, authentication, common logon, and user management support. These are detailed in Attachment 1: Enterprise Security Gateway.
- *Security and Privacy Standards* – any proposed solution must: (a) comply with the privacy requirements of the *Freedom of Information and Protection of Privacy Act* and (b) address any privacy concerns or impacts that are identified in the Privacy Impact Assessment. As part of the compliance process, the solution provider must to agree to meet the Province's security requirements as set out in the document's Attachment 2: Security Clauses.
- *Application Security Standards* - role-based security controls and administration should provide access to government information for user roles consistent with the purpose for use and need for information. Within the application, access control may be implemented by use of the Common Logon Service within the Enterprise Security Gateway (see above) to control access to application screens, and/or application specific functions or features.
- *Network Connectivity* – This section has been superseded by section 5.8: Network to Network Connectivity Standard. (See pgs 49 - 51)
- *Information Management Standards* - ministries must ensure all government information is managed in line with the Core Policy and Procedures Manual Chapter 12 Information Management and Information Technology Management. This compliance also includes recorded information management, information utilization, data management and forms management.

Where to Apply This Standard

These standards are intended to serve as a reference to all internal (government) and external (contracted) resources involved in the design, development, implementation and operational management of all information systems.

Authority and Exemptions

These standards have been issued in *interim status* because the OCIO is working to establish a more comprehensive and collaborative process involving broad stakeholder participation for defining, approving, and issuing standards.

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

The intention of the OCIO is to advertise and promote these standards as being mandatory throughout government. However, in order to effectively manage information systems security and network connectivity, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

The location of the *Interim Standards for Information Systems Security and Network Connectivity* document is:

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/interim_n2n_standard_s.pdf.

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2006-06-02 Scheduled Review: OBSOLETE/SUPERSEDED Last Updated: Last Reviewed: 2009-01</p> <p>Type: Technical Standard</p>
<p>6.0 Information Technology Security (CPPM 12.3.6)</p>	
<p>6.5 Use of Portable Storage Devices on Government-managed Personal Computers – OBSOLETE/SUPERSEDED</p>	
<p>Keywords: Obsolete, Superseded, Cryptographic</p>	

IMPORTANT: This Standard is obsolete. It has been superseded by
6.10 Cryptographic Standards for Information Protection

Description of Standard

This standard outlines the need to store sensitive or personal information on the government network and not on local hard drives or "non-encrypted" portable storage devices such as diskettes, memory sticks, MP3 players, CDs and DVDs:

- 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. Government information must be stored on the government network whenever possible to ensure the protection and long term availability of the information
- Sensitive or personal information (see item 2 in additional information) must be encrypted when stored on portable storage devices to ensure protection from loss, compromise or unauthorized disclosure.
- Since government policy requires that all information technology hardware purchases, including memory must be handled by Shared Services B.C. (Core Policy and Procedures Manual 6.3.5(a) 6)), ministries are requested to contact Shared Services B.C. for to purchase and the OCIO for advice on the use of memory sticks and details on the exception process.

Where to Apply This Standard

The standard is meant for any government employee or contractor that has been assigned a government-managed personal computer.

Authority and Exemptions

This standard has been issued by the OCIO in order to insure that government information is protected commensurate with its value and sensitivity.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage the security of the government network, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated June 2, 2006) defined the standard for the use of personal storage devices. A copy of this document can be found at:

www.cio.gov.bc.ca/local/cio/standards/documents/standards/portable_storage_devices_memo_20060602.pdf.

Additional Information

1. The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca.
2. Sensitive or personal information is determined by its Information Classification (Information Security Policy 3.2.1)

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2007-12-03 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Process Standard</p>
<p>6.0 Information Technology Security (CPPM 12.3.6)</p>	
<p>6.6 IT Asset Disposal</p>	
<p>Keywords:</p>	

Description of Standard

This standard classifies IT assets by their risk level (high, medium, low) and defines the disposal process to be used for those assets.

Where to Apply This Standard

The standard is meant to be used:

- By any ministry or broader public sector employee or contractor that has been assigned a government IT device and needs to dispose of that IT device.
- In conjunction with Chapter 6 of the *Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia*.

Authority and Exemptions

This standard has been issued by the OCIO in order to insure that government IT assets are disposed of in a manner that is consistent with policy, applicable legislation, and contract law.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage the security of information contained on government IT assets, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT device, security and network terminology found in this standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. The current version of this standard is contained in the *IT Asset Disposal Standards*. This document is located on an internal BC Government website. For more information please contact:
Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca
2. The *Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia* is found at:
pss.gov.bc.ca/air/disposal-handbook.html
3. A memo from the Government Chief Information Officer (dated Jan 3, 2007) provides direction on the changes to policies, procedures and processes related to disposal of computer or information technology assets. This document is located on an internal BC Government website. For more information please contact:
Security Strategies, OCIO
email: CITZCIOSecurity@gov.bc.ca

The following documents are located on an internal BC Government website. For more information please contact:

- Security Strategies, OCIO
email: CITZCIOSecurity@gov.bc.ca
1. A list of IT asset disposal recommendations entitled the *IT Asset Disposal List*
 2. A list of *frequently asked questions* related to IT asset disposal
 3. A form for requesting a review on devices **not** contained in the *IT Asset Disposal Standards*.
 4. A list of questions to help ministries determine their compliance to asset management policies and what areas need to be improved.

Additional Information

1. The OCIO is the owner of this standard. Its website is www.cio.gov.bc.ca.
2. Sensitive or personal information is determined by its Information Classification. See Section 3.2.1, Information Security Policy
<http://www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page>.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2006-08 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
	Office of the Chief Information Officer Province of British Columbia
6.0 Information Technology Security (CPPM 12.3.6)	
6.7 Password Standard	
Keywords:	

Description of Standard

This standard consists of two components:

1. A Password Management System Standard which identifies a set of rules that must be enforced in order to support information access control policies.
2. A Complex Password Standard which defines how passwords can be selected and changed.

Where to Apply This Standard

The standard is intended for any ministry or provincial agency to ensure that access to government information systems is limited to authorized users and processes.

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.1, *Appropriate Use of Government Resources*. Users (of government information technology):

- must not divulge, share or compromise their own or another's government authentication credentials
- must use the rules for complex passwords to create password.

and with Information Security Policy, Chapter 7.3.3:

- A password management system must be in place to provide an effective, interactive facility that ensures quality passwords. This includes the enforcement of regular user password change, i.e., user passwords will expire after a predetermined number of days.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. Information on both the Password Management Systems Standard and the Complex Password Standard can be found in Sections 7.3.1 and 7.5.3 of the *Information Security Policy* at:
<http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/chapters/chapter7.pdf>.
2. A two-part document entitled *Non-expiring Passwords Parameters and Exposures*, containing a *Non-expiring Password Acceptance Form*, is located on an internal BC Government website. For more information please contact:
Security Strategies, OCIO
email: CITZCIOSecurity@gov.bc.ca

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2008-01 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01</p> <p>Type: Process Standard</p>
<p>6.0 Information Technology Security (CPPM 12.3.6)</p>	
<p>6.8 Use of Non-government Managed Laptops by Contractors</p>	
<p>Keywords:</p>	

Description of Standard

This standard defines the measures which must be taken to protect the privacy of personal information and the security of the government network from the use of non-government managed laptops used by contracted personnel:

- Contractors must encrypt personal information on their laptops and other portable storage devices
- Contract Managers must verify that contractors have implemented appropriate security measures to protect personal information stored on their laptops and other portable storage devices
- Contractors must complete a ministry-supplied external party access agreement in accordance with Section 2.2.3 a) of the *Information Security Policy* if they wish to connect their laptop to the government network. (See **References** for a SSBC version of this access agreement.)

Where to Apply This Standard

The standard is intended any ministry or provincial agency that:

- Engages contracted staff and
- Allows contracted staff to use their own laptops to complete their assigned tasks.

Authority and Exemptions

This standard has been issued by the OCIO:

- In accordance with the *Freedom of Information and Protection of Privacy Act* under which government has a duty to protect the personal information in its care using reasonable security measures.
- To ensure the security of the government network and resources.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

1. A memo from the Government Chief Information Officer (dated September 4, 2007) defined the requirement for the encryption of personal information on contractor laptops. A copy of this document is located at: [encryption contractor devices memo 20070904](#).
For more information please contact:
Security Strategies, OCIO
email: CITZCIOSecurity@gov.bc.ca
2. Instructions for completing a SSBC Network Access Agreement form, which is intended for all individuals connecting non-government managed devices to the network at 4000 Seymour Place, Victoria, plus the form itself are located on an **internal BC Government website**. For more information please contact the Customer Business Analyst. The contact information can be found at:
http://www.sharedservicesbc.gov.bc.ca/contact/Ministry_Client_Contact_List.pdf

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD Office of the Chief Information Officer Province of British Columbia	Effective Date: 2007-12-28 Scheduled Review: OBSOLETE Last Updated: Last Reviewed: 2009-01 Type: Technical Standard
6.0 Information Technology Security (CPPM 12.3.6)	
6.9 Data Encryption and Minimum Key Length Standards – OBSOLETE/SUPERSEDED	
Keywords: Obsolete, Superseded, Cryptographic	

IMPORTANT: This Standard is obsolete. It has been superseded by
6.10 Cryptographic Standards for Information Protection

Description of Standard

The purpose of this standard is to define the minimum requirements for data encryption and minimum key lengths:

1. *Public Key Encryption and Minimum Key Length Standards* – the encryption standard is the commercially available 1024 bit RSA standard, or equivalent or better.
2. *Symmetric Key Encryption and Minimum Key Length Standards* – the encryption standard is the commercially available Advanced Encryption Standard with minimum key length of 128 bits (AES-128), or equivalent or better.

Some other considerations include:

- Use of Public Key Encryption requires both parties to acquire Digital Certificates from recognized and trusted service providers.
- The strength of encryption is proportional to the key length. The selection of key length can be done through a risk assessment that considers the nature of the information being protected, the cost and availability of longer keys, and any performance impact.

Where to Apply This Standard

The standard is intended any ministry or provincial agency that has a business requirement for data encryption.

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM Chapter 12.3.6, *Information and Technology Security*.

- Documents, computer media, data and system documentation must be protected from unauthorized disclosure, modification, removal or destruction.
- Data and information exchanges within government, or with an external entity, must be secure and managed through a documented process.
- Access to information, systems, and business processes must be managed and controlled on the basis of business and security requirements.
- Information and technology assets will be protected commensurate with the identified risks and security requirements.

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

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage appropriate use and the security of government resources, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard.

Terms and Definitions

Any IM/IT security and network terms in this document will be included in a Consolidated Glossary which is under development by the OCIO.

References

A memo from the Government Chief Information Officer (dated December 28, 2007) defined the standards related to the use of encryption and minimum key lengths. A copy of this memo can be obtained from the Executive Director, Architecture and Standards, OCIO.

Additional Information

The OCIO is the owner of this standard and can provide assistance with implementation considerations such as:

- Acceptable equivalent standards
- Acceptable service providers
- Key management best practices and standards
- Priority situations where encryption should be implemented.

Its website is located at www.cio.gov.bc.ca.

Contact

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2009-01-14 Scheduled Review: Annual Last Updated: 2011-08-11 Last Reviewed: 2011-08-11
	Type: Technical Standard
Office of the Chief Information Officer Province of British Columbia	
6.0 Information Technology Security (CPPM 12.3.6)	
6.10 Cryptographic Standards for Information Protection	
Keywords: Cryptography, Authentication, Digital Certificates, HTTPS, USB Flash Drives, X.509	

Description of Standard

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.

This family of standards governs the protection of information through the use of cryptographic controls. Topics include: authentication using X.509 certificates, protecting information in transit and at rest, digital signatures and messaging.

Where to Apply This Standard

This standard applies where there is a need to apply cryptographic protection of information. The need for cryptographic protection is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Authority and Exemptions

This standard has been issued by the OCIO in accordance with CPPM 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

Appendix A and B of the standard contain detailed requirements regarding compliance. Please take note that compliance requirements for Web Service SOAP Security involve fixed dates.

Shared Services B.C. Compliance

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 across SSBC services will be a multi-year undertaking.

Terms and Definitions

Terms and definitions are defined within the standard.

References

3. Information Security Policy:
<http://www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page>
4. Full Cryptographic Standard can be viewed at:
www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf

Additional Information

The OCIO is the owner of this standard. Its website is at www.cio.gov.bc.ca.

Contact

Architecture and Standards Branch, OCIO

email: ASB.CIO@gov.bc.ca

<p>IM/IT Architecture & Standards Manual STANDARD</p> <p>Office of the Chief Information Officer Province of British Columbia</p>	<p>Effective Date: 2011-01-01 Scheduled Review: Annual Last Updated: 2010-08-27 Last Reviewed: 2010-08-27</p>
<p>Type: Process Standard</p>	
<p>6.0 Information and Technology Security (CPPM 12.3.6)</p>	
<p>6.11 Standard for Information Security Threat and Risk Assessment Methodology, Process and Assessment Tool</p>	
<p>Keywords: Risk, Assessment, Risk Assessment, Compliance, Criticality, STRA, iSMART, Security Review, Risk Management, Information Security</p>	

Description of Standard

This Standard supports the efficient, secure operation of information systems while maintaining privacy, and maximizes the effectiveness and efficiency for information technology planning, design, implementation and operations. The Standard focuses on the minimum requirements to complete information Security Threat and Risk Assessment (STRA) and provides an analytical approach to information security risk management.

This Standard defines the methodology, process and tools for performing an information Security Threat Risk Assessment. The methodology is aligned with the government's Enterprise Risk Management (ERM) Model and provides additional specific details on Information Management/Information Technology (IM/IT) security threats and risks.

As per the government information security policy chapter 2.1.3 b, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister. Information Owners have the responsibility and decision making authority for information throughout its life cycle, including:

- Be involved with security reviews and/or audits;
- Define security requirements during the planning stage of any new or significantly changed Information system; and
- Ensure information and information systems are protected commensurate with their information classification and value.

Information Owners and Information Custodians must conduct an information Security Threat Risk Assessment to ensure that projects involving information, system development or acquisition activities are completed in accordance with documented requirements, standards, and procedures. This Standard is intended to address these issues and to establish compliance practices that are in line with the IM/IT security governance and policy frameworks. It also includes assessments of legal and regulatory requirements applicable to government.

The Ministry Information Security Officer (MISO) is responsible for assisting business areas in conducting Security Threat and Risk Assessments.

The information Security Threat and Risk Assessment standard used by government is supported through the Information Security Management and Risk Tool (iSMART). The Fundamental Information Risk Management (FIRM) methodology is used herein for managing information risk through a practical and constructive approach of evaluating and driving risk

down to acceptable levels. iSMART is used to assist in assessing and measuring the effectiveness of information security management that enables information risk to be managed systematically across the B.C. government.

iSMART allows Ministry Information Security Officers (MISOs) and the Office of the Chief Information Officer (OCIO) to identify information security issues, monitor mitigation activities, ensure compliance to standards and policies and report on the governments information security posture.

iSMART enables information security risks to be identified and measured using the Risk Register referred to as the HARM Reference Table. The HARM table is used as an objective basis for assessing the worst-case business impact and the level of harm that has been – or could be – caused by a disruption to or loss of the confidentiality, integrity or availability of business information. It can also be used to provide a common basis for evaluating other risks. See Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary for further detail.

iSMART is also used to assist in mitigating and establishing an information security risk monitoring capability in government. The risk tool serves as a repository for information Security Threat and Risk Assessments and enables authorized personnel to view individual organization results, ministry results and cross-government results.

Minimum information Security Threat and Risk Assessment Standard Requirement:

- 1. All IM/IT projects¹ must select any one of the Basis of Evaluation (BoE) scorecards listed, and complete the top-level sections (A through I – 61 statements) within the risk tool located in iSMART. (Each response to a question should be substantiated by adding comments, and attaching or providing a reference to the supporting documentation.)**
- 2. Any identified issues, risks and recommendations are to be entered into the issues log and action plan and remediation action provided. (This requirement can be met by attaching or providing a reference to the supporting documentation within the issues log and action plan.)**

iSMART Basis of Evaluation (BoE) Scorecards:

ISO 27001 or
Information Risk Assessment (IRA) or
Standard of Good Practice (SoGP)

It is highly recommended that further analysis of risk and compliance be undertaken by completing the underlying questions associated with the BoE scorecard chosen.

An Information Owner or Custodian may choose to complete a more detailed assessment based on the initial risk review and risk tolerance/acceptance of the ministry. When the initial risk assessment reports a high or medium risk to a system, a more detailed review as described

¹ An Information Management / Information Technology (IM/IT) project is any project or initiative which involves information, information system development or acquisition activities.

in the Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary is required.

Where to Apply This Standard

This Standard is meant for any ministry, public agency or external service provider that is responsible for managing B.C. Government's information. For maximum effectiveness, information Security Threat and Risk Assessments must be completed on every project involving information, a new application, service, system, and/or environment or whenever a major change is proposed.

This Standard is intended to be used government-wide as a guide to understand and generate their project specific information Security Threat and Risk Assessment's using the iSMART tool. It is intended primarily for Information Owners and Information Custodians and those individuals who are responsible for measuring and controlling information risk.

Authority and Exemptions

If there are compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the OCIO.

Metrics and Enforcement

All required documents in the information Security Threat and Risk Assessment Process Checklist should be completed, reviewed and signed off. See Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary for further detail.

The intention of the OCIO is to advertise and promote this information Security Threat and Risk Assessment standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other government agencies are expected to adopt and monitor compliance to this Standard. The OCIO Information Security Branch will also monitor for compliance.

When requested, the Office of the Comptroller General's Internal Audit group and the Office of the Auditor General will be provided with high-level or detailed reports. These reports may assist them in determining how Information Security related risks are being addressed within government.

Supporting documentation and supplemental information relating to the information Security Threat and Risk Assessment standard is available on the Information Security Branch website – Compliance web page:

- Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary
 - Information Security Threat and Risk Assessment Process
 - Fundamental Information Risk Management (FIRM) methodology and
 - HARM Reference Table

Terms and Definitions

Any IM/IT device, security and network terminology found in this Standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary

Located on the OCIO's Intranet site, this information can be found on the Information Security Compliance page. These pages are not available to the general public.

Information Security Management and Risk Tool (iSMART)

Located on the OCIO's Intranet site, this information can be found on the Information Security Compliance page. These pages are not available to the general public.

Core Policy and Procedure Manual (CPPM) Chapter 12

http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

Information Security Policy

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

IM/IT Standards Manual

http://www.cio.gov.bc.ca/cio/standards/standards_manual.page

Enterprise Risk Management

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

All policy references that support this information security threat and risk assessment standard are located in Appendix II of the Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary.

Additional Information

Compliance Management, Information Security Branch, OCIO, is the owner of this standard.

Located on the OCIO's Intranet site, this information can be found on the Information Security Compliance page. These pages are not available to the general public.

Contact

Information Security Branch, OCIO

Email: CITZCIOSecurity@gov.bc.ca

APPENDIX A: GLOSSARY

NOTE: A Consolidated IM/IT Glossary is under development by the Office of the Chief Information Officer (OCIO) and will include the definitions in this Appendix. For further information contact:

Architecture and Standards, OCIO
email: ASB.CIO@gov.bc.ca

Architectural Framework – a common, cohesive vision that is used to provide both an understanding of and guidance towards the design, construction, purchase, deployment, and management of information systems and information technology across government.

Best Practices - non-mandatory suggestions gleaned from research, feedback, and experience.

Directive - issued by the Government Chief Information Officer (CIO) to further clarify existing operational policy or establish procedures needed to manage government's information and communications technology resources. Bulletins or backgrounders may also be issued to supplement the directive and provide further information about the topic area.

Guideline – a suggestion or set of suggestions that guides or directs action. The purpose of a guideline is to provide additional information that assists service providers to comply with policy, usually until a standard is developed.

iStore – an electronic ordering and billing tool for ministries and other government agencies. This application is located on an internal government website. For more information please contact:

SSBC.ClientServices@gov.bc.ca
250-387-8045
1-877-387-8045

Memo – issued by the CIO, essentially for communications purposes. A memo may establish strategic directions for government's information and communications technology resources.

Policy - a guiding principle or course of action adopted to achieve a desired objective. Policy statements describe what must and must not be done but, in general, do not describe how the work is done. They state expectations, assign responsibilities, set limits and serve as the basis for consistent decision-making.

Procedure – a set of specific steps that describe activities that should be carried, and by whom. Corporate level procedures are designed to provide a starting point for ministries to help interpret how to implement and set operational core government policies.

Standard - an established, measurable, achievable and understandable statement or set of criteria that describes a desired level of performance against which actual performance can be compared. While a policy tells us what to do, a standard is a tool that allows us to measure, monitor and compare actual performance against a benchmark.

APPENDIX B: IM/IT STANDARDS CHANGE MANAGEMENT PROCESS

Note

A project to establish a change management process for IM/IT Standards has been initiated by the OCIO. For further information refer to the Architecture and Standards Development Life Cycle Process at:

www.cio.gov.bc.ca/cio/standards/asdlc

Contact

Architecture and Standards, OCIO

email: ASB.CIO@gov.bc.ca

APPENDIX C: STANDARDS ABSTRACT TEMPLATE

IM/IT Architecture & Standards Manual	Effective Date: YYYY-MM-DD Scheduled Review: Annual Last Updated: YYYY-MM-DD Last Reviewed: YYYY-MM-DD
STANDARD	Type: (Select: Technical, Product, Process, Reference)
Office of the Chief Information Officer Province of British Columbia	
X.0 Standards Family Name (one of the six CPPM Chapter 12 Policy headings)	
X.Y Title of Standard	
Keywords:	

Summary

Where to Apply This Standard

Authority and Exemptions

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

Terms and Definitions

References

Additional Information

Contact

[Title of Branch], [Divison]
email: [contact email]

APPENDIX D: ARCHITECTURE ABSTRACT TEMPLATE

IM/IT Architecture & Standards Manual ARCHITECTURE	Effective Date: YYYY-MM-DD Scheduled Review: Annual Last Updated: YYYY-MM-DD Last Reviewed: YYYY-MM-DD
Office of the Chief Information Officer Province of British Columbia	Type:
X.0 Information Technology Management (CPPM 12.3.5)	
x.y [High Level, detailed] Architecture for [xxx]	
Keywords: Architecture, Technical, etc.	

Summary

Authority and Exemptions

This architecture was developed by [xxx] (owner) in consultation with [yyy].

The [zzz] is responsible for its content.

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.

Business Context

The purpose of this architecture is to [etc.].

ASDLC Requirements

This architecture should be reviewed [when] and every 3 years thereafter. The [organizations] may request update to this architecture.

Viewpoint

The viewpoint is [strategic, tactical, planning]. It is [long, short] term and [conceptual, detailed] in nature. Related projects include [???]. The design aligns with existing security policy.

State

There is [no] preceding conceptual architecture. This model will be used in [???].

Description of the Architecture

Additional Information

Contact

[Title of Branch], [Divison]

email: [contact email]