# Interim Standards For Information Systems Security and Network Connectivity

## Office of the Chief Information Officer
## Province of British Columbia

**August 12, 2004**

## TABLE OF CONTENTS

# INTERIM CORPORATE GOVERNMENT STANDARDS FOR INFORMATION SYSTEMS SECURITY AND NETWORK CONNECTIVITY

***These interim corporate government standards are effective immediately and will remain in effect until revised or rescinded by the Office of the Chief Information Officer.***

These interim corporate government standards are issued to guide ministries and their solution providers in regards to how the security and related network connectivity of information systems solutions must be structured.

Ministries are responsible for ensuring that the information systems solutions they build or buy comply with these security and network connectivity standards.

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

## Chapter 1 Interim Corporate Government Standards

### Government Authentication Standards

The government requires the ministries to ensure that information systems solutions utilize the government's Enterprise Security Gateway services 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

Information systems security is the protection of data, systems, documentation, computer-generated information and facilities from accidental or deliberate threats to confidentiality, integrity or availability.

References to the required security and privacy requirements can be found at the following web sites:

- Freedom of Information and Protection of Privacy Act -
  www.mser.gov.bc.ca/foi_pop/index_toc.htm#Legislation

- Core Policy Manual - Chapter 12 - Information Management and Information Technology Management
  *Freedom of Information and Protection of Privacy 12.3.2 II*
  http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1232iia
  *Security 12.3.3 III*
  http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1233iii

- Information about Privacy Impact Assessments (PIA) –
  www.mser.gov.bc.ca/foi_pop

- Information about the Privacy Protection Schedule (PPS) (contract language)- http://www.mser.gov.bc.ca/FOI_POP/PPS/default.htm

A proposed solution must meet the privacy requirements of the *Freedom of Information and Protection of Privacy Act* and Proponents must address any privacy concerns or impacts that are identified in the Privacy Impact Assessment

As part of the policy compliance, the province requires the solution provider to agree to meet the Province's security requirements as set out in Attachment: 2). Security Clauses.

## Application Security Standards

Role-based security controls and administration should provide access to government data for user roles consistent with the purpose for use and need for data. The software should provide role-based access control that includes:

- Access to multiple government services for a single user;
- Distributed access control administration; and
- Record-level or field-level security.

Applications must be designed in such a way that users can only access the data that they are entitled (authorized) to access.

Within the application, access control may be implemented by use of the Common Logon Service within the Enterprise Security Gateway to control access to application screens, and/or application specific functions or features.

## Network Connectivity

The province wishes to avoid creating new connections between the government secure network and the corporate networks of other organizations, until such time as a network segmentation project is complete. The aim of the network segmentation project is to architect a manageable, scalable, auditable, method of connecting users to systems, and systems to systems when either the users or systems are hosted on different organization's private networks.

A policy clarification was provided on July 9, 2004, respecting connections to the provincial SPAN/BC network. A copy of this policy clarification titled "Enhancing the Security and Functionality of the Provincial Network (SPAN/BC)" and further background materials in "Backgrounder to Policy Clarification on Connecting to the Provincial Network (July 12, 2004)" which provides background information to place the clarification of policy and rules respecting connectivity to the Provincial Network within the broader security enhancement context are available at http://www.cio.gov.bc.ca/prgs/memo.htm.

Specific guidance is provided in Attachment: 3) Network Connectivity Guidelines.

## Information Management Standards

Ministries to must ensure all government information is managed in line with Government Core Policy Manual Chapter 12 Information Management and Information Technology Management 12.3.2 Information Management,

http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1232
This includes Recorded Information Management, Information Utilization, Data Management and Forms Management.

# Chapter 2 Application of Interim Corporate Government Standards

If there are compelling reasons why an information systems solution should NOT make use of these standards, in the manner described, the ministry may seek an exemption through the information systems director of the program area's ministry by the Office of the Chief Information Officer.

If there are questions regarding these standards, contact Mr. Bruce Cuthbert, Manager, Technology Planning and Standards, Office of the Chief Information Officer, at 387-2194 or Bruce.Cuthbert@gems9.gov.bc.ca

**Attachment 1**

# Enterprise Security Gateway

---

## A. Authentication Policy

The Authentication Framework for e-Government Services policy is documented in CORE POLICY MANUAL 12 Information Management and Information Technology Management, http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1234

The Authentication Framework provides the process and tools for ministries to define identity and eligibility requirements, and to determine consistent approaches in meeting those requirements.

## B. Authentication Framework

The establishment of an authentication framework is a current initiative from the CIO's office. Several components supporting government-wide authentication are currently in development.

There are four levels of trust in the Authentication Framework (See Table 1).

Table 1. Trust Levels for e-Government Services

| Trust Level | Description |
|---|---|
| 0 | Anonymous Transaction |
| 1 | Pseudonymous Transaction |
| 2 | Identified Transaction |
| 3 | Verified Transaction |

**Definitions**

*Level 0: Anonymous transaction* – access provided for transactions that do not require or allow a person to be identified, or transactions which require protection of a person's identity. For example, access to online information about government programs or services or protecting a person's identity. Combining the transaction data with other data must not allow identification of a particular individual.

*Level 1: Pseudonymous transaction* – access provided for transactions that do not require a person to be identified but do require a means for further contact to deliver a product or service. For example, a note from someperson@internet.ca can not be readily translated into an individual's name, but it may be sufficient to request information, to provide some services, or on-going follow up.

*Level 2: Identified transaction* – access provided for transactions that require that a person be specifically identified. The nature of the transaction may require confirmation of a person's

identity (e.g., name, address, birth date, etc.) and/or data linking the person to a transaction (e.g., invoice number, personal health number, etc.).

*Level 3: Verified transaction* - access provided for transactions that require: the person to be specifically identified; verification of the integrity of the data exchanged and the exchange itself; and, the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction. For example, a note signed with a digital certificate, audit trails and security logs may provide sufficient evidence that a specific person intended to conduct a transaction.

**Overview**

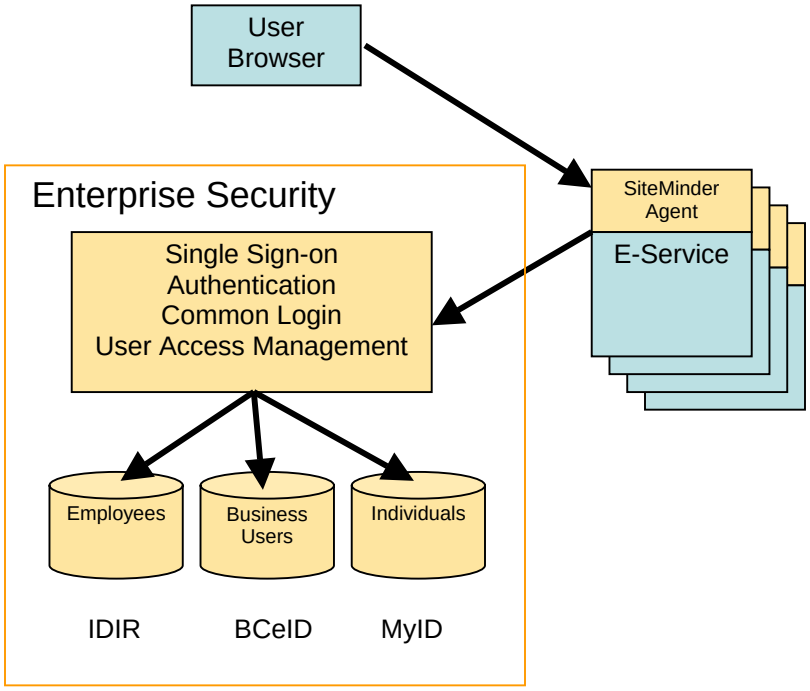
The Authentication Framework provides the process and tools for ministries to define identity and eligibility requirements, and to determine consistent approaches in meeting those requirements.

1. An Authentication trust level, as defined in the table above, must be defined for electronic service delivery initiatives:
2. An Authentication Profile, as part of the Privacy Impact Assessment, must be completed to determine the authentication requirements for an electronic service. The profile is used to determine the trust level for the minimum technology requirements for authentication.
3. The Authentication Profile must be reviewed and updated when a system or application is modified or updated. An update to the Privacy Impact Assessment is also required.

## C. Enterprise Security Gateway Overview

The Province of British Columbia ensures that only authenticated and authorized users access the protected e-services using the Enterprise Security Gateway infrastructure. This infrastructure consists of the following components:

- common logon user identity
- single sign-on,
- authentication
- user access management




### 1. Corporate Authentication LDAP directory service

The government of BC has chosen to provide a single logon credential for each of its customers. A business user or employee will have a single credential to access all of the protected web-based services. For individuals (residents and non-residents), Government allows individuals the choice of one or more credentials. A set of common directory services stores the logon credentials for each user domain: MyID directory service for individuals; BCeID directory service for business users; and IDIR directory service for employees.

### 2. Netegrity SiteMinder for web-based access management and single-sign-on

The SiteMinder infrastructure intercepts all web requests to e-services and ensures that only authorized users pass. SiteMinder utilizes the common logon pages (see below) for the logon

process and the corporate authentication services for credential validation and directory service. E-services must be enabled either with a SiteMinder agent directly installed or via a web proxy service. Developers must ensure the compatibility of their platforms with SiteMinder agents. The SiteMinder agents must communicate with the Provinces core SiteMinder servers via a secure data network connection.

SiteMinder forces the user to logon via the common logon pages by having the web agents send http redirect commands to the user browser. After logon, the user browser is redirected back to the target e-service. The single-sign-on feature of SiteMinder ensures that this redirect for logon only occurs once per session.

**3. Common Logon web pages hosted on the enterprise portal**

The Common logon web pages are hosted on the Enterprise portal and provide the logon function. Use of the common logon pages provide and ensure:

- A consistent user experience common presentation (look and feel)
- A consistent function (behaviour) and implementation of logon for each user domain
- A reduced-sign-on to all participating web-based services
- A reduction of duplicate development effort for logon services
- A reduction of infrastructure for logon services
- A consistent presentation of help information and other common services
- And, no need for each web-service to purchase an SSL server certificate for encryption of the logon dialogue

## D. Detailed Description

### 1. Architecture of the Enterprise Security Gateway

The Common Logon Page is a component of the governments Enterprise Security Gateway infrastructure, implemented using the Netegrity SiteMinder product. All participating E-services will have the SiteMinder http agent installed on the hosting (or proxy) web-server. The agent communicates with a SiteMinder Policy Server to evaluate access rules and to authenticate users. The SiteMinder policy server communicates with government user domain directories to authenticate user credentials. The Common Logon page is a special case of E-service that is specifically designed to perform user logon. The rules in the SiteMinder policy server instruct all agents to redirect the user to the Common Logon Page and then back to the E-Service upon successful logon.

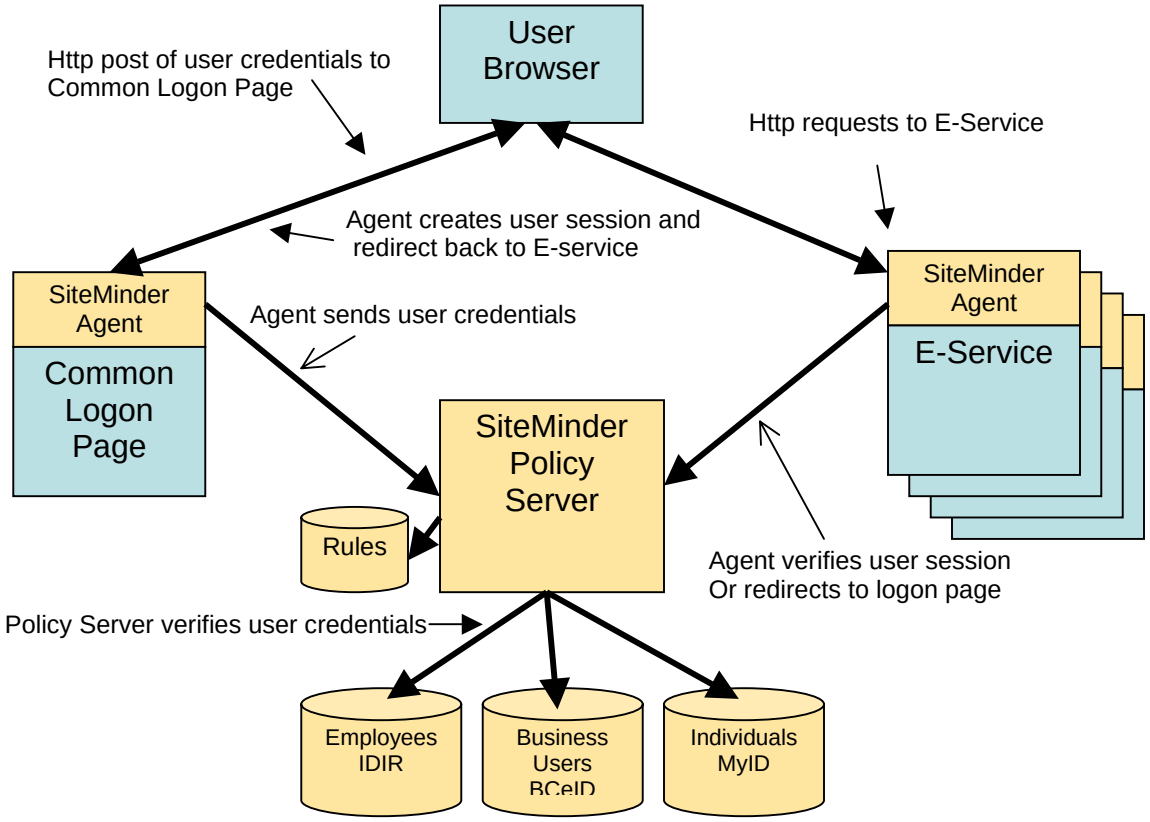



**Figure 1 Common Logon Page Architecture**

### 2. Web Application development considerations

This section describes the way in which web application developers will design and build their web server software programs to work with the Enterprise Security Gateway.

**Integration point for the Enterprise Security Gateway**

The point of integration between the Enterprise Security Gateway and the web application software is the SiteMinder web agent and the associated HTTP header variables. The web software will receive all identity information associated with a user (successful logon) in the HTTP header variables. The SiteMinder policy for the web server must be configured to create the HTTP header variables for the web application. The set of HTTP header variables is called the Application User Logon Profile.

The Application User Logon Profile will contain:

- the user domain for the user account (IDIR, BCEID, or MyID)
- the username for the user account

and may optionally contain attributes specific to the authenticating namespace eg.

- the email address of the user (this is an optional attribute for MyID)
- the name of the user (this is an optional attribute for MyID domain)
- the legal name of the business (BCEID only)
- the groups the user account belongs to
- the text representation of the GUID of the user account
- any other directory attributes available for e-services use (BCeID and employee only)

| User Profile Attribute | Employees | BCeID Users | MyID Users |
|---|---|---|---|
| Domain name | Yes | Yes | Yes |
| Username | Yes | Yes | Yes |
| Email address | Yes | Yes | Yes |
| Name | Yes | Yes | Yes |
| Legal business name | No | Yes | No |
| Groups | Yes | Yes | No |
| Text GUID | Yes | Yes | Yes |
| Other attributes | Yes | Yes | No |

**Figure 1 - User Profile Attributes available to E-Services**

**URL Design for Logon and Access Control via the Enterprise Security Gateway**

The SiteMinder policy server is the master controller for all Enterprise Security Gateway functions and is configured on a URL by URL basis. If a particular or unique function or behaviour is required of the common logon pages and associated access control (authorization) for a web application then it (web application) must be structured to have URL paths that will drive the unique function or behaviour.

A good example of this is where a web application has IDIR users that access some administrative function and BCEID users that use the remainder of the application. The designers/developers can place all of the administrative functionality under a separate URL path and have a SiteMinder policy configured for that URL path. The SiteMinder policy can force an IDIR logon and only allow access to IDIR users or members of an IDIR group.

If the web application cannot be structured in this way then the web application can guide its behaviour from the user profile information passed to it.

**Single-Sign-On for IDIR Users**

The Enterprise Security Gateway service includes a SiteMinder enabled Microsoft IIS server that can use NTLM authentication to logon an IDIR user. E-services that intended only for employees and are only accessed via the Intranet can make use of this service. The SiteMinder policy is configured to redirect the user to the IIS server for logon and then back to the e-service. Note that the user browser must be configured to permit NTLM authentication.

Applications that have BCeID or MyID and IDIR authentication can make use of this service if they structure their web application with distinct URL's for each user domain.

**Welcome Page and User Logon Switching**

Web applications should as a best practice display the user context (individual, business, etc) and username on the first page the user goes to. This is especially important for those applications that support logon from more than one user domain (two or more of IDIR, BCEID, and MyID) since the user may have used the wrong user account. Applications like this are also encouraged to provide a link to the common logon page so that the user can switch to a different account or user domain.

**Non Supported Web Servers**

Netegrity does not provide SiteMinder web agents for all platforms and web servers. Web applications with non supported platform/web server combinations can make use of a web agent on a reverse proxy host. The portal Apache servers can be configured with virtual hosts that can act as the integration point with the common logon page. The HTTP header information will still be received by the web application in the normal manner. The web-application server should be configured to only allow HTTP connections from the reverse proxy virtual host(s).

**Scope of Authorization and Access Control**

The authorization and access control function is limited to the HTTP traffic going through the SiteMinder agent on the web application server. No downstream application authorization mechanisms are provided. Web applications are responsible for managing any downstream access control using the User Profile information passed in the HTTP headers.

**Enterprise Authentication by User Domain**

The government of BC has a set of common directory services for the logon credentials for each user domain: MyID directory service for individuals; BCeID directory service for business users; and IDIR directory service for employees. The directory services IDIR and BCeID directory services have been developed by the government of BC. New functionality is added to these directory services based on the prioritized, funded business requirements of the ministries.

The following table summarizes the current status of the implementation of the Authentication trust levels in each of the user domains.

| User Domain | Authentication Trust Levels | | | |
|---|---|---|---|---|
| | 0 | 1 | 2 | 3 |
| Employee | Access without userid | Not applicable | **IDIR** | **IDIR** with security check |
| Businesses | Access without userid | **MyID** | **BCeID** | Future **BCeID** enhancement |
| Individuals | Access without userid | **MyID** | Future **MyID** enhancement | Future **MyID** enhancement |

### *Employee - IDIR*

The IDIR repository represents the directory of BC government employees and other individuals who require a business reason for accessing government applications. It is an instance of Active Directory and provides authentication services for government employees.

### *Business - BCeID*

BCeID has been developed to support the identity and authentication of businesses within the province that interact with government program and information. Authentication is based on the registered business within the province and is not based on individual identities except in the case of a sole proprietorship. The directory supporting the BCeID is organized by business identity (registered business number) and represents a relatively small percentage of the BC population. BCeID represents a repository of business partners that require authentication to access electronic government programs. The BCeID directory is an instance of Active Directory.

The customer of the BCeID Authentication Service, typically a government program area offering an e-service, is responsible for cost of the BCeID service as well as any authorization processes deemed appropriate to allow access to their e-service.

The BCeID Authentication Service authenticates businesses and other organizations external to government, which enables individuals in these entities to identify themselves to applications providing government e-services.

A strictly controlled, due diligence process confirms the identity of the organization. After the corporate identity has been verified, individuals from that business or organization can each obtain a single identifier that enables them to access one or more secured e-services. Once a BCeID is obtained, it can be used to authenticate with other secured government e-services.

Currently BCeID provides for trust level 2 access. As government identifies, prioritizes and funds development a trust level 3 access can be provided if required.

### *Individual Authentication - MyID*

MyID has been developed to support a non-verified identity credential. E-services that have a requirement for a persistent user state or transaction over multiple visits and do not have a requirement for verified identity can have users logon with their self-registered MyID. MyID is a level 1assurance credential. A level 2 MyID has been proposed and is under evaluation.

## 3. Products

### *Netegrity SiteMinder 5.5*

www.netegrity.com
http://www.netegrity.com/products/products.cfm?page=SMoverview
SiteMinder provides enterprises with a centralized security infrastructure for managing user authentication and access to Web sites. Specifically, SiteMinder provides:

- Centralized, policy-based control of user authentication and authorization management
- Enterprise wide SSO to all web applications
- Enterprise-class manageability
- Secure federation with partner sites
- Enterprise-class scalability and high-availability
- Extensive support for heterogeneous IT environments
- Comprehensive audit and reporting services
- Role-based access control (RBAC)

**Resource Center**

http://www.netegrity.com/products/products.cfm?page=resourcecenter

**FAQ**

http://www.netegrity.com/products/products.cfm?page=SMfaqs

**Technical white paper**

http://members.netegrity.com/access/files/SiteMinder55.pdf

### *Microsoft Windows 2000 Active Directory*

***www.microsoft.com***

***Windows 2000 Active Directory is the enterprise directory product used for BCeID, MyID, and IDIR credentials. Active Directory provides***

- LDAP directory
- Kerberos authentication
- Windows 2000 integrated security for Windows servers and desktops
- DNS services

Resource Centre

http://support.microsoft.com/default.aspx?pr=win2000

http://www.microsoft.com/windows2000/technologies/directory/AD/default.asp

**4. Industry Standards and Protocols**

| | |
|---|---|
| HTTP | Hypertext Transfer Protocol - the client/server protocol that defines how messages are formatted and transmitted on the World Wide Web |
| HTTPS | Secured HTTP - HTTPS is the Hyper-Text Transfer Protocol with SSL Encryption. It is the most popular network protocol for establishiing secure connections for exchanging documents on the World-Wide Web |
| SSL | SSL is the Secure Socket Layer. It is a protocol that encrypts a single TCP session. Using this Asymmetric Encryption, all data exchanged over a TCP socket can be cryptographically protected. SSL is the base of HTTPS - the secure World-Wide Web protocol. |
| LDAP | LDAP stands for Light-weight Directory Access Protocol. It is a network protocol, based on TCP that is used to access a hierarchical directory of information on a directory server. LDAP is considered to be lightweight because it is based on a simplified version of X.500 directories |
| Active Directory | A directory service from Microsoft that is a part of Microsoft Windows environment |
| Kerberos | An authentication system designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message. |
| Netegrity SiteMinder | Info on www.netegrity.com |

**5. Links to More Information**

**Authentication**

CORE POLICY MANUAL 12 Information Management and Information Technology Management,
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm#1234

Determining Authentication Levels within the BC Government
http://www.mser.gov.bc.ca/foi_pop/main/authv1.doc

**Portal Implementation**

http://gww.cio.gov.bc.ca/portal/

Sample Application
url to follow

**Attachment 2**

# Security Clauses

## 2.1 Security of Information

The Contractor and sub-contractors (referred to as Contractor) agree to meet the Province's security requirements as set out in this section and, as amended from time to time.

## 2.2 Adherence to Provincial Security Standards

The Contractor agrees to conform to security policies, standards, guidelines and practices of the Province of British Columbia as outlined in the Province's Core Policy Manual (http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm particularly sections 12 and 15) and the Information Technology Security Policy (ITSP;http://www.cio.gov.bc.ca/prgs/ITSP.pdf).

## 2.3 Communicating Security Requirements

The Contractor will understand and communicate to all employees all of the security requirements issued by the Province as detailed in this section.

## 2.4 Contractor Compliance Monitoring

The Contractor will monitor employees for security compliance requirements as outlined in government policy.

## 2.5 Security Clearances

The Contractor will have all personnel that require access to government facilities pass a background security clearance as determined by the Province.

## 2.6 Access Control Procedures

The Contractor will have procedures in place during the life of the Agreement to issue access to government assets, to properly Authorized individuals and promptly revoke access in the event of a personnel termination or security concern.

## 2.7 System Access

The Contractor agrees that access to any government systems or facilities used under this Agreement will be limited to Authorized personnel only. Any processing platforms or telecommunications facilities used to provide a Service that are shared with other Clients or any sub-contractor will be partitioned in such a way to allow only Authorized personnel to access Provincial data and Service configurations.

## 2.8 Data Access

The Contractor will ensure that access to the Province's data transiting the Contractor's data networks or resident on Contractor owned or maintained hardware systems is limited to Authorized personnel.

Province's data that is being used for testing or contract work will be removed from contractor systems upon the expiry of the agreement unless there is written provisions made between the

contractor and government to maintain the data for testing and maintenance. Such provisions will include a timeframe for removal of the Province's data.

### 2.9 Physical Access

The Contractor will ensure that equipment and telecommunications facilities used to provide a Service to the Province are secured by an electronic card access system, combination lock, lock and key, or equivalents. The Contractor will maintain logs of all accesses to any Site including the Province's Regional Network Centres used to provide the Service, and provide access to security and audit reports to the Province.

### 2.10 Monitoring of Data and Telephone Calls

The Contractor agrees to use its best efforts to ensure the security of all data and telephone calls within the Service . The Contractor will restrict data and telephone call monitoring to Authorized, security cleared, personnel performing network maintenance activities only, ensure that any information obtained is not stored at, used by or disclosed to third parties, and have policies in place that prohibit the use or disclosure of any sensitive monitored information by its staff or subcontractors.

### 2.11 Security Records and Reporting

The Contractor agrees that:

(a) The Province will be given immediate notification of any actual or suspected security breaches or violations;
(b) Security and other similar records relating to the agreement will be kept for two years after expiry of agreement. The Province will have complete and open access to all records relating to the agreement for that period.; and
(c) Security records are subject to privacy regulations and will be protected from disclosure or access by unauthorized personnel.

### 2.12 Security Investigations

The Contractor will ensure that court ordered monitoring of telecommunications facilities used to serve the Province is only initiated via a representation to the Province by an Authorized law enforcement agency. The Province will be granted access to monitored information for the purposes of either court ordered or internal security investigations.

### 2.13 Network Acceptable Use

Telecommunications facilities that are purchased and used by the Province are to be used only to conduct the business of the Province. Routing of traffic not associated with the Service supplied to the Province by the Contractor's personnel on the Province's networks and the use of unauthorized attachments of cables, modems, wireless or other communication equipment on any portion of the Province's networks is prohibited. The Contractor agrees to have policies and procedures that will prohibit such use and attachments.

### 2.14 Fraud and Inappropriate Use

Contractors will not misuse or misrepresent resources within the Province's network. The Contractors will support the Province's investigation of suspicious events.

**2.15 Consequences for Misuse, Inappropriate Use or Security Violations**

Failure to comply with any of the above conditions or misuse of any Government of BC resources may result in the removal of all access and other privileges, termination of this Agreement and possible criminal charges. In addition, the Government of BC may seek restitution for any damages due to negligence, wilful disclosure, or criminal actions. The Government of BC may also seek to recover costs of the associated investigation.

**2.16 Audit**

The Province may require the Contractor to provide a third party audit of the Support Services in accordance with Section 5900 of the Canadian Institute of Chartered Accountants Handbook. The Contractor will provide such an audit, if requested, or agree to terminate the Agreement. The audit will be at no cost to the Province.

If material deficiencies are noted, the Contractor will correct any deficiencies within three months of the auditors' report or agree to terminate the Agreement.

**Definitions:**

"Authorized" means having the permission of the Contractor and / or the Province to work on the Equipment or Service;

"Regional Network Centre" or "RNC" means one of the Province's Regional Network Centres used for the aggregation of telecommunications traffic;

"Service" or "Services" means the services described in the Schedules to this Agreement;

"Service Location" means any community in British Columbia or geographic area where equipment and/or information is owned by the Province;

"Site" means a civic address or other geographical location within a Service Location designated by the Province from time to time as an end point or a transit point for the location of Equipment or delivery of the Service;

**Attachment 3**

## Network Connectivity Guidelines

The guidelines listed in this section assume that readers are familiar with the policy memorandum issued July 9 and available at http://www.cio.gov.bc.ca/prgs/memo.htm.

Further to the above mentioned policy memorandum, in cases where information systems solutions cannot comply with the policy memorandum, the steps required to implement an alternative are as follows:

1). Technical design, review, and alternatives analysis of connectivity options

Key considerations will be:

- Ability to operate and manage the information systems in question
- Ability to protect the government network at large (it's users, assets, and information) from the compromise of any non-government network or computer systems
- Ability to protect any non-government network or computer systems from compromise of government network or systems
- Ability for government to manage and audit any network connections, the security, and the related systems
- The financial and other resource costs associated with the alternative

It is generally understood that alternatives will involve technologies such as private network links, point to point network links; firewalls, access control lists on routers, network encryption and so on.

It is strongly encouraged that ministries find ways to provide the business solution without requiring modification to the existing configuration of the SPAN/BC network.

2). Any proposed alternatives must be approved by the Office of the Chief Information Officer before they are implemented

Any ministry proposing an alternative to the policy must factor the time and cost of the above process, as well as the costs required to implement and operate any alternative, into their plans and budgets.