

<b>IM/IT Architecture &amp; Standards Manual ARCHITECTURE</b>  <b>Office of the Chief Information Officer Province of British Columbia</b>	<b>Effective Date:</b> 2012-06-14 <b>Scheduled Review:</b> Annual <b>Last Updated:</b> 2012-06-14 <b>Last Reviewed:</b> 2012-06-14
	<b>Type: Technical Standard</b>
<b>6.0 Information Technology Management (CPPM 12.3.5)</b>	
<b>6.12 Physical Security Technical Standards</b>	
<b>Keywords: Secure, Closet, Buildings, Utilities Services, Technical</b>	

### Description of Standard

The purpose of this standard is to ensure minimum standards are met in the new design, development and construction of locations for housing Ethernet switches, routers and other government owned telecommunications assets.

This standard replaces the “Ministry/Shared Rooms Secure Zone Standards v1.4” dated February 14, 2008 that had been in production for ten years. It has been revised in order to simplify the requirements set out in the previous standard for building a physically secure area for government’s telecommunications assets and to address cost savings.

The revised standards outline the security specification requirements for constructing a secure area for housing government’s information technology infrastructure devices like routers and switches.

### Where to Apply This Standard

The standard applies to core government and any organization that uses SSBC network services for the purposes of connecting to the SPAN-BC network. The standard can also be used by alternative service delivery partners in the design, development and construction of telecommunications closets.

The specifications documented here should be considered as minimum standards. If the implementer chooses a stronger option, it is permitted, but should be noted in the systems documentation.

The document applies to:

- All new construction and
- All renovations to existing telecommunications closets
- Telecommunications closets that are not compliant with the previous standard

The document does not apply to:

- The standard does not apply to Broader Public Sectors clients who do not connect to the SPAN-BC network.

## **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.

There are two exceptions to this standard. They are:

- Secure Enclosures for ministry telecommunications assets within a Special Purpose Building
- Secure Enclosures for Building Utilities Services telecommunication assets

## **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**

[Physical Security Technical Standards – Network Centre/Server Room Secure Zone](#)

[Physical Security Technical Standards – Building Utilities Service](#)

[Physical Security Technical Standards – Special Purpose Buildings](#)

[Physical Security Technical Standards – Telecommunication Closets](#)

## **Contact Information**

[Gordon.Higgins@gov.bc.ca](mailto:Gordon.Higgins@gov.bc.ca)

Manager, ICT Facilities