Office of the Chief Information Officer

PHYSICAL SECURITY TECHNICAL STANDARDS FOR TELECOMMUNICATION CLOSETS

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● Collaboration ● Innovation

Version 2.0

November 25, 2011

Physical Security Technical Standards for Telecommunication Closets

Introduction

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 standard outlines the security specification requirements for constructing a secure area, referred to as a "Telecommunications Closet", for housing government's information technology infrastructure devices like routers and switches.

The new standard has been in pilot since May 2011 and has been through a successful peer-review.

Purpose

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

Scope

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 does not apply to:

Legacy or already constructed telecommunication closets. However, any augmentation to existing telecommunication closets to meet these standards is acceptable.

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

Normative References

Standards Manual

- Information Security Standards and Guidelines. Physical Security Standards. https://gww.cio.gov.bc.ca/services/security/standards_guidelines/default.htm

Exceptions to this Standard

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

Terms and Definitions

For the purposes of this document, the following terms, definitions and acronyms apply:

ACROYNYM	TERM	DEFINITION
T-Bar (ceiling)		Also known as a drop **ceiling** requires interlocking sections of metal bars in the shape of a "T" and foam or fiberglass acoustic panels.
	Elephant Foot	A device attached to the bottom of the door to hold the door open.
ULC	Underwriters Laboratory of Canada	An independent entity that regulates safety standards and certification in security. ULC provides testing and certification in security alarm installation and monitoring, protective signaling systems (fire panels & sprinklers), alarm response service and fire alarm testing and inspection
Schlage - Falcon		Two companies whom manufacture lock sets, deadbolts and lever locks in a variety of finishes and levels of security
WSI	Workplace Solutions Initiative	A partner with the Integrated Workplace Solutions division of SSBC

Annex A. Physical Security Technical Standards for Telecommunication Closets

Information Security Standards and Guidelines Office of the Chief Information Officer Province of British Columbia	Effective date: November 25, 2011 Scheduled Review: March 2012 Type: Technical Standard
Physical Security Technical Standard	

1. Ministry Telecommunication Closet Classification

1.1 Secure Office.

2. Location

2.1 Within client's secure space.

3. Walls/floor

3.1 Demountable partition walls with no openings reaching T-Bar height.

4. Doors

4.1 All doors are to be of solid core (heavy duty 1.6mm (16ga.)) steel with steel cladding and steel frames.
4.2 All doors are to be equipped with NRP (non-removable pin) hinges
4.3 All perimeter doors are to be equipped with door closer.
4.4 No elephant foot installed

5. Signage

5.1 Room numbers only. No signage to identify the room as "Telecommunications Closet".

6. Lockset and Keyways

6.1 Locksets shall be heavy duty security hardware with steel dead-bolts into steel inserts, with ULC approval at the highest level. Locksets to be "Storeroom lock" type (outside knob fixed, entrance by key only). Inside knob always unlocked.
6.2 Keyways shall be restricted to approved types such as Schlage D, G, or T series or Falcon G series.
6.3 All keys to be marked "DO NOT COPY".
6.4 WSI to maintain a list of all keys distributed.

7. Intrusion Alarm System

7.1 The Telecommunication Closet shall be protected by the customer's base building intrusion alarm system.

7.2 Each Telecommunication Closet is to have the following equipment:
- 7.2.1 Doors to be equipped with door contact(s).
- 7.2.2 One motion detector installed in each space.

8. Secure Cabinets (applicable to SSBC Servers Only)

8.1 SSBC servers must be housed in an approved SSBC/OCIO secure cabinet. The server cabinet must be physically and seismically anchored – bolted to either floor or wall – within the former Ministry/Shared server room.

8.2 Keys to the secure server cabinets will be approved and controlled as per SSBC Key Control Procedure:

- *8.2.1 When necessary, SSBC Enterprise Hosting will delegate key authority to a local Ministry Office Manager if operationally needed. In the case of smaller communities where there may only be one site, the Government Agent may also be considered.*
- *8.2.2 Conditions for having a key: The key must not be signed out to anyone. The key must not be left lying around in view or in a drawer. The key must be secured either on your personal key ring or in a locked cabinet. The owner of the key must know at all times when they used it and who requested them to use it.*