a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #18
Physical Security of UBC Datacentres

Introduction

1. Effective security measures require physical security controls. While electronic controls alone are important, they may become useless if the device is physically accessed or removed by an unauthorized party.
2. This document defines standards for the physical security of UBC Datacentres. These Datacentres are intended to provide a secure location for operations, controlled access to equipment and data, protection against environmental threats, and support for the availability requirements of UBC Electronic Information and Systems. University IT Support Staff are responsible for ensuring that the requirements of this document are complied with.
3. The University has a responsibility to protect Confidential Information from unauthorized viewing and use. In particular, the *Freedom of Information and Protection of Privacy Act* (FIPPA))[1] and Records Management Policy[2] require public bodies to implement reasonable and appropriate security arrangements for the protection of Personal Information (in both electronic and paper format). Therefore, servers containing significant quantities of Confidential Information must be hosted in UBC Datacentres, which provide the highest level of security. Sensitive and Public Information may also be hosted in UBC Datacentres where appropriate.
4. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Physical Security Controls

5. The table below outlines the minimum set of physical security controls required for UBC Datacentres, based upon the Security Classification of UBC Electronic Information standard.

Control Area	Information Security Classification		
	Confidential	Sensitive	Public
Rooms	Datacentre must be located in a fully enclosed room. Walls must meet the following criteria: • Must extend from floor to ceiling slab. • Should preferably be constructed from a solid, resistant material such as concrete or brick. If they are not solid (e.g. drywall), then they must be reinforced with wire mesh.		Equipment can be located in open areas if other protective measures are in place, e.g. locked cages.
Doors and Locks	• Datacentre doors must be locked when room is not in use. • Good practice is to install automatic closing mechanisms. • Security grade door fastening hardware must be used in conjunction with a metal door and frame. • Acceptable locking mechanisms include electronic proximity access cards/fobs, keypad type entry locks, and biometric locks.		Datacentre doors must be locked when room is not in use. Either electronic or mechanical locks are acceptable.

[1] FIPPA, section 30
[2] Policy 117, section 2.4

Control Area	Information Security Classification		
	Confidential	**Sensitive**	**Public**
Glazing	All exterior glass in doors and accessible windows must be reinforced. Consider installing high grade security film (minimum standard should be Profilon AXA1-15Mil or equivalent) to resist forced entry.		Windows must be able to securely lock from the inside.
Visibility of Equipment	Window coverings (blinds/shades) or reflective/tinted film should be installed on glazed windows or doors in order to reduce direct sightlines to valuables inside the facility.		
Cabling	Power and network cabling carrying data or supporting information services should be protected from interception or damage outside of the Datacentre.		
Managing Access	• The public must not have direct access to the Datacentre perimeter. An outer security perimeter should be established with access controls sufficient to prevent direct public access. • Use signage to clearly delineate publicly accessible space from Authorized Personnel-Only areas. Signage should not indicate the presence of UBC Electronic Systems. • Individual(s) must be assigned the authority to grant access to the Datacentre and someone must be appointed to formally manage the physical access process including revocation of access (fob/card, keypad access). • Individuals who are not authorized to access the Datacentre must be escorted at all times by an authorized individual. • Access must be logged electronically or in a logbook in the case of keypad entry doors that do not uniquely identify an individual.		
Alarms and Remote Monitoring	Alarms (monitored 24/7) must be installed that trigger on unauthorized access.	Good practice is to install and monitor an alarm system to detect intruders.	
	CCTV has been debated as an effective deterrent to crime, but if employed with adequate resolution and proper camera placement, its forensic effectiveness is undisputed. All CCTV installations must be approved by the Access and Privacy Manager.		
Power Supply	• Redundant power should be supplied to the Datacentre where possible. • Servers should all be connected through a UPS in order to remain running in the event of short power outages.		N/A
Environmental Controls	• Sufficient Heating, Ventilation and Air Conditioning (HVAC) systems must be in place to effectively maintain all UBC Electronic systems within the manufacturers' required temperature and humidity operating ranges. • Measures must be in place to monitor and detect variation in temperature and humidity • Where possible, water and drainage plumbing should not run across the ceiling of a Datacentre. • The floor of the Datacentre should be raised above the subfloor to reduce the risk of flood damage.		Comply with Building Code requirements.
Fire Protection	Fire detection and suppression devices, such as fire		Comply with Building Code

Control Area	Information Security Classification		
	Confidential	Sensitive	Public
	extinguishers and pre-action or dry pipe sprinkler systems, must be in place.		requirements.
Data Backups	If information is backed up onto electronic media, the same physical security requirements are to be applied to that media unless the information is encrypted (see the Encryption Requirements standard).		

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Encryption Requirements standard

Security Classification of UBC Electronic Information standard