INFORMATION SECURITY CHECKLIST

Securing Computing and Mobile Storage Devices/Media

Introduction

1. This document is intended to assist Users in checking their compliance with the Securing Computing and Mobile Storage Devices/Media standard.
2. This checklist has been issued by the Chief Information Officer to supplement the Securing Computing and Data Storage Devices/Media standard. Questions about this checklist may be referred to information.security@ubc.ca.

Checklist

Electronic Security	
☐	All accounts on the devices have strong passwords as per the Password and Passphrase Protection standard
☐	Screensavers activate in 5 – 30 minutes and require a password to unlock
☐	Where possible, remote locate services have been enabled
☐	Where possible, automatic data erasure has been set for 10 consecutive incorrect password attempts
☐	Where possible, the ability to remotely erase the data has been activated
☐	Anti-virus software is installed and regularly updated as per the Anti-virus Protection Guideline
☐	The firewall has been activated in accordance with the Firewalls Guideline
☐	A current version of the operating system is installed and configured to allow regular updates
☐	Data stored on the device is backed up on a regular basis
☐	Backups are checked periodically to ensure the integrity such that it can be restored.
☐	If High or Very High Risk Information is stored on the device/media, it is in compliance with the Encryption Requirements standard
Physical Security	
☐	Unattended devices are located in a locked cabinet or enclosed area with some form of access control
☐	Servers containing significant quantities of High or Very High Risk Information are located in a UBC Datacentre
☐	Keys or swipe cards giving access to devices are limited to authorized individuals
☐	Measures are taken to ensure devices cannot be viewed from outside the secure area
☐	Where possible, cable locks are used as a supplementary security measure
☐	Where possible, alarms are used as supplementary protection
Non-University-Owned Devices	
☐	Personally owned devices used for work purposes meet this standard
☐	Third-party-owned devices used for work purposes meet this standard
Special Requirements for Servers	
☐	Servers are not used to for general web browsing or e-mail
☐	If server applications are run on a desktop or laptop, this has been approved by the Administrative Head of Unit with compensating controls to limit exposure

Inventory of UBC-owned Laptops and Desktops	
☐	Central UBC IT Support Staff are maintaining an inventory of UBC-owned laptops and desktops that they have deployed
Return of Devices and Information Upon Termination	
☐	Upon termination of their employment, Users will return all of the UBC-owned Devices in their possession to an authorized employee of UBC, and return and delete any UBC Electronic Information stored on their personally-owned devices.
Loss Reporting Requirement	
☐	Users who lose a device, used for University Business (no matter who owns the device), or suspect that there could have been an unauthorized disclosure of UBC Electronic Information, will report any loss/disclosure

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Securing Computing and Mobile Storage Devices/Media standard