a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U7
Securing Computing and Mobile Storage Devices/Media

1. Introduction

1.1 All Devices used for University Business—no matter whether they are owned by the University, by the User, or by a third party—need to be protected from theft and/or unauthorized access. This standard specifies the minimum security requirements that Users must comply with to protect these Devices. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users in implementing these requirements where necessary.

1.2 Two broad categories of Devices are covered by this standard:

1.2.1 Computing Devices, e.g. Servers, desktop and laptop computers, tablets and smartphones; and

1.2.2 Mobile Storage Devices/Media, e.g. external hard drives, DVDs, and USB sticks.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Electronic Security

2.1 Computing Devices used for University Business must comply with the following electronic security requirements. Users with IT-related responsibilities should also see the Vulnerability Management standard.

	Servers	**Workstations**	**Smartphones & Tablets**
Password Control	All Devices must be password-protected in accordance with the Passphrase and Password Protection standard. Always lock Devices or log out before leaving them unattended.		
Screensaver Locks/Idle Timeout	Console automatically locks after no more than 5 minutes of inactivity.	User interface automatically locks after no more than 30 minutes of inactivity (5 minutes is recommended for Devices storing Medium, High or Very High Risk Information).	
Device Location	n/a		Enable any features that will allow the Device to be remotely located in the event of loss or theft.
Data Destruction	n/a		Enable the feature that automatically erases data if 10 consecutive incorrect passwords are entered.
Remote Wiping	n/a		Enable any features that will allow data stored on the Device to be erased in the event of loss or theft.
Endpoint Detection and Response (EDR)	EDR software approved by the CISO must be installed on all UBC-owned Servers.	EDR software approved by the CISO must be installed on all UBC-owned Workstations, where technically possible.	n/a

Malware and Spyware Protection	On Computing Devices not required to have EDR, install up-to-date anti-malware and spyware cleaning software (except for smartphones and tablets that do not offer this feature) and configure it to update at least once per day. See the UBC IT Malware Protection page.		
Automatic Blocking of Malicious Websites	Servers on-premises and in the cloud (Infrastructure as a Service) must be protected by a DNS firewall. It is recommended that Servers on-premises use UBC Domain Name Servers, which make use of DNS firewall protection.	UBC-owned Devices that access, process or store Medium, High or Very High Risk Information must be protected by a DNS firewall. It is recommended that on-premises Devices use UBC Domain Name Servers, which make use of DNS firewall protection. For all other Devices, a DNS firewall is recommended.	
Firewalls	Install and configure firewalls (except for tablets and smartphones that do not offer this feature). See the Firewalls guideline.		
Operating System	The Device must run a version of its operating system for which security updates continue to be produced and are available. If this is not possible, see the Vulnerability Management standard for compensating controls. If the Device is University-owned, software updates must not be impeded, and no unauthorized changes may be made to the Device.		
		Workstations must be regularly restarted to facilitate patching of vulnerabilities. The recommended frequency for restarting is at least once per week.	
Data Availability	Any UBC Electronic Information stored on the Device must be regularly backed up to a secure location and checked periodically (preferably quarterly) to ensure the integrity and availability of the information such that it can be restored. See the Backup guideline.		
Encryption	Refer to the Encryption Requirements standard.		

2.2 Mobile Storage Devices/Media must be encrypted as explained in the Encryption Requirements standard.

3. Physical Security

3.1 For their protection, unattended Devices must be located in one or more of the following areas:

3.1.1 a room or other enclosed area that is locked or otherwise access-controlled; and/or

3.1.2 a locked cabinet or other fixed container such as a locked server cabinet/cage.

3.2 Servers containing significant quantities of High or Very High Risk Information must be hosted in UBC Datacentres that are compliant with the Physical Security of UBC Datacentres standard, or third party datacentres that have an equivalent level of security. To get access to server space in a UBC Datacentre, Users can rent space or use the EduCloud Server Service.

3.3 Keys or swipe cards giving access to Devices must be limited to authorized individuals.

3.4 Measures should be taken to ensure Devices cannot be viewed from outside the secure area, e.g. by drawing curtains or blinds.

3.5 Cable locks are recommended as a supplementary security measure for Computing Devices, but they do not provide sufficient protection by themselves. It is safer to lock portable Devices, such as laptops, in a cabinet out of sight rather than relying on a cable lock.

3.6 The use of alarms is highly recommended, especially to protect Devices used to store Medium, High or Very High Risk Information.

4. Use of Non-University-Owned Devices

4.1 UBC recognizes that it is often convenient for Users to use their personally-owned Devices for work purposes and such use is permitted provided that they manage their Devices in accordance with this standard.

4.2 Some Users may also use Devices supplied by third parties in connection with University Business. Users, in consultation with University IT Support Staff, are responsible for determining whether these Devices meet the minimum security requirements in this standard; for example, Health Authorities have good information security measures in place, and it is acceptable to use their computers for University Business.

5. Special Requirements for Servers

5.1 Servers (especially Web and FTP servers) are attacked on a continual basis. To avoid creating security weaknesses, servers must not be used for general web browsing or email.

5.2 Users must not run server applications on desktops or laptops (e.g. web or FTP servers) that are Internet-facing. Exceptions may be approved by the Administrative Head of Unit, in consultation with University IT Support Staff, provided that compensating controls are put in place to control security risks.

6. Inventory of UBC-owned Laptops and Desktops

6.1 Central UBC IT support staff must maintain an inventory of UBC-owned laptops and desktops that they have deployed, including which Users these Devices are assigned to. All other University IT Support staff are recommended to maintain such inventories.

7. Return of Devices and Information upon Termination

7.1 Upon termination of their employment, Users must return all of the UBC-owned Devices in their possession to an authorized employee of UBC, and must return and delete any UBC Electronic Information stored on their personally-owned Devices.

8. Loss Reporting Requirement

8.1 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 must report the loss/disclosure in accordance with the Reporting Information Security Incidents standard.

9. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Vulnerability Management standard

Passphrase and Password Protection standard

UBC IT Malware Protection

UBC Domain Name Servers

Firewalls guideline

Backup guideline

Encryption Requirements standard

Physical Security of UBC Datacentres standard

Data Centre Co-Location Service

EduCloud Server Service

Reporting Information Security Incidents standard