Standard for Securing computing and mobile storage devices

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Infrastructure		
Stakeholders:	Okanagan College Users		
Approved by:	College Information Officer		
Effective Date:	29-April-2024		
Last reviewed:	29-April-2024	Scheduled review date:	29-April-2025

1. Purpose

1.1 All devices used for college business—no matter whether they are owned by the College, 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. College IT Staff, including staff in the IT Service Desk, are available to assist users in implementing these requirements where necessary.

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

a) Computing devices, e.g. servers, desktop and laptop computers, tablets and smartphones; and

b) Mobile storage devices/media, e.g. external hard drives, DVDs, and USB sticks.

1.3 Questions about this standard may be sent to itsecurity@okanagan.bc.ca

2. Electronic Security

	Servers	Workstations	Smartphones & Tablets
Passwords	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	User interface automatically locks after no more than 30 minutes of inactivity (5	User interface automatically locks after no more than 30 minutes of inactivity (5 minutes is	

	minutes is recommended for devices storing medium, high or very high risk information).	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) This includes antivirus protection	EDR software approved by the IT Security must be installed on all College servers.	EDR software approved by the IT Security must be installed on all College workstations, where technically possible.	N/A

3. External Storage Devices

3.1 Where possible, any portable media must be set to use encryption. Data is encrypted at rest.

4. Physical Security

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

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

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

4.2 Servers containing significant quantities of high or very high risk information must be hosted in College datacentres or third party datacentres that have an equivalent level of security.

4.3 Keys or swipe cards giving access to devices must be limited to authorized individuals.

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

4.5 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.

4.6 The use of alarms is highly recommended, especially to protect devices used to store medium, high or very high risk information.

5. Use of non-college-owned devices

5.1 The College recognizes that it is often convenient for users to use their personal-owned devices for work purposes and such use is permitted provided that they manage their devices in accordance with this standard.

5.2 Some users may also use devices supplied by third parties in connection with College business. Users, in consultation with College IT Staff, are responsible for determining whether these services 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 College business.

5.3 The installation and use of College VPN to access protected College networks and enterprise systems is only permitted provided that the device is managed in accordance with this standard and approved by IT Security.

6. Special requirements for servers

6.1 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.

6.2 Users must not run server applications on desktops or laptops (e.g. web or FTP Servers) that are internet-facing.

7. Inventory of College owned laptops and desktops

7.1 College IT Staff must maintain an inventory of College owned laptops and desktops that they have deployed, including which users these devices are assigned to.

8. Return of devices and information upon termination

8.1 Upon termination of their employment, users must return all the College owned devices in their possession to an authorized College employee and must return and delete any College electronic information stored on their personally owned devices.

9. Loss Reporting requirement

9.1 Users who lose a device used for College business (no matter who owns the device) or suspect that there could have been an unauthorized disclosure of College electronic information must report the loss/disclosure.

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*
2026-1-27	*Minor Revision: Section 2. Passwords updated to correct content*