Request for technical approval

Please fill out this form to request technical approval to purchase a non-standard computing device. For Computer Acquisition Fund (CAF) approval or University Policy AD2515 deviation, please use the Standards Review Document. Contact the TSC (tsc@uvic.ca) if you require assistance completing this form, or have any questions regarding its use.

This completed form must be attached to your WebReq. WebReqs submitted to the TSC without a completed Request for Technical Approval form may be returned to the WebReq originator to have the form completed. A completed *Request for Technical Approval* form is the only way to indicate to Purchasing Services that Technical Approval has been granted.

Contact information

Date:

Name:

Dept.:

Tel.:

Email::

Make and model of requested device(s)

What is the intended use of requested device(s)?

Who will be supporting the requested device(s), and are they aware?

Have you included all necessary components for your intended use (such as adapters and cables)?

Technical information

1. Is the device a tablet or phone?	Y	N	Don't know
2. Will the device store confidential or highly confidential information?	Y	N	Don't know
3. Will the device be encrypted?	Y	N	Don't know
4. What operating system will be used on the device?			
5. What type of warranty does the device have?			
6. Does the device have a Keep Your Drive service plan?	Y	N	Don't know
7. Is the device CSA/CE/UL compliant?	Y	N	Don't know
8. Will the device be used to connect to speciality research equipment?	Y	N	Don't know
If yes, answer questions 9 and 10. If no, skip them.			
9. Is the device recommended or required by the specialty equipment vendor?	Y	N	Don't know
10. Does the device have a support contract provided by the equipment vendor?	Y	N	Don't know

To be completed by TSC staff:

Technical approval status Granted Denied

Justification

Approver

Technical review is explained in *Purchasing Services Policy FM5105* and is defined in *University Policy AD2515* as "review of technology acquisitions, performed by University Systems, in order to ensure the acquired technology is compatible with the university environment. This includes, but is not limited to, Canadian Standards Association (CSA) compliance, Internet Protocol (IP) network support, and operating system version suitability for enterprise use."

Technical approval indicates TSC has performed a technical review and determined the technology is suitable for use on campus. Any use of institutional funding for purchase of technology requires technical approval. Further information regarding technical approval and the related legislation and policies can be found at www.uvic.ca/systems/techapproval.

Question clarification

1. Mobile devices must adhere to the same information security standards as all computing devices. To gain approval a device must have a current operating system, be capable of connecting to secure wireless networks, and support encryption. More information on the requirements for technical approval can be found in the *Technical Approval Process* document.
2. If the device will access or store any Confidential or Highly Confidential data as described in *Information Security Policy IM7800*, encryption must be used. If the device will not store sensitive data it may be granted technical approval under the condition it will not be re-purposed for any purpose that requires encryption.
3. The recommended methods of whole disk encryption are FileVault2 for Apple devices and centrally-managed BitLocker for Windows devices, which requires a Trusted Platform Module (TPM). Encryption is required for any confidential or highly confidential data as described in *Policy IM7800*. It is the responsibility of the administrative authority responsible for the equipment to ensure that appropriate data protection is in place.
4. The device must be using a current enterprise operating system with necessary features to support encryption, the ability to access UVic enterprise applications, and secure networking. Windows devices with inappropriate licensing or out-of-support operating systems may require upgrade or a detailed description of the intended use in order to receive technical approval.
5. *Purchasing Services Policy FM5105* establishes the responsibilities and accountability associated with the efficient and economical acquisition of goods and services. Onsite warranties are recommended for all computer purchases to ensure assets can be used reliably for an appropriate length of time. Note that *Policy IM7700* requires that all storage media must be destroyed. This requirement may impact the usability of a manufacturer's warranty.
6. "Keep Your Drive" is a warranty service that ensures no hard drives with UVic data leave campus in the event of a warranty claim. All storage devices must be securely wiped and physically shredded when they have reached end of life as per *Policy IM7700*.
7. Electronic devices that have not been granted CSA compliance by Canadian or U.S. safety standards may be dangerous for use on campus. Any incidents caused by non-CSA compliant electronic equipment may result in legal liability to the administrative authority responsible for the equipment.
8. Specialized research computing devices can be exempted from technical approval under specific circumstances. Approval can only be authorized on a case by case basis after consultation with the Technology Solutions Centre.
9. If a device is required by a vendor for use with speciality equipment, TSC may request additional information to be gathered from the vendor if not provided in advance to technical approval.
10. Devices with vendor-specific maintenance contracts cannot be serviced on campus by University Systems staff in order to avoid jeopardising any warranty or software support from the equipment vendor.