emily carr
university of art + design

Policy Number	9.7
Approval Body	Executive Committee
Policy Officer	Director ITS
Approval Date Review	August 2009 2012

9.7 LAPTOP SECURITY

ENABLING LEGISLATION + LINKED POLICIES

Emily Carr University of Art + Design policies:

9.3 Appropriate Use of Information Technology, Facilities + Services
9.4 Software Use + Copyright Compliance
9.5 Data Backup + Recovery

OBJECTIVE

As laptops are portable and may be used off-site, they have the potential to enhance productivity, but are more susceptible to physical damage and theft. In some cases, they are used to store highly sensitive information, the value of which may exceed that of the actual hardware. As such, laptops are subject to unique security provisions.

The objective of this policy is to outline those provisions, minimize information security risks affecting laptops and define the security-related responsibilities that users have with laptops that are Emily Carr University of Art + Design (University) property.

SCOPE

This policy applies to all laptops that are the property of the University, whether they are owned, leased, rented or on loan to the University.

The policy applies to faculty, staff, students and third parties provided with, or using, laptops that are the property of the University. While this policy is not specific to student-owned laptops, much of the policy provides general guidance for students to protect their personal laptops and portable devices.

POLICY

1. Requests for laptops will be based on demonstrated need and job function. All requests will be approved by the appropriate Faculty Dean or Department Director. Requests are generally identified during the annual budgeting cycle, but may be accommodated at other times based on need and budget availability. All requests and orders for laptops will be processed by Information Technology Services (ITS). All approved requests will include purchase of a locking device.
2. Laptops provided by the University will be used to conduct University business and for the purpose of carrying out the user's job responsibilities.

3. Laptop users must assume a reasonable amount of responsibility for the safekeeping and care of the equipment and data stored on it. Damage to a laptop may result in user downtime while the equipment is repaired or replaced.
4. If a laptop is presumed stolen or misplaced, ITS must be immediately notified. A police report will be filed for stolen equipment and the report provided to ITS.
5. The University will evaluate the circumstances of laptop theft or loss and may hold the user financially responsible for the cost of the laptop.
6. While the University does maintain insurance coverage, the deductible for self-insured property (owned) and leased (must be listed on the optional policy) generally exceeds the value of most laptops in the University. In addition, both coverages exclude “mysterious disappearance of property” and there are some geographic limitations to coverage.
7. As per University policy 9.4 Software Use and Copyright Compliance, no unauthorized or illegal software will be installed on laptops.
8. Users are given administrative rights to a laptop based on need. Such rights are not granted on a default basis. Users that are granted administrative rights to a laptop will be held responsible for changes they make.
9. Users are responsible for connecting to the University network on a regular basis (eg. minimum every two weeks) to obtain updates to operating systems and anti-virus software. For urgent or significant security alerts, laptop users may be requested to bring in their laptops or promptly connect to the network to obtain such patches or updates. If a laptop is frequently off-site, the user must consult with ITS as to the process for applying manual updates and will be responsible for applying them in that manner.
10. Users are responsible for configuring their laptops for Internet access off-site and to work with their personal Internet Service Provider. ITS may provide general guidance, but laptop users are responsible for making remote connections work.
11. The University reserves the right to audit any laptop that is University property. Audits will be carried out in such a way as to minimize the impact on curriculum or academic functions.
12. Laptops that are provided to users for a specific period of time, such as a lease term or for a specific project, must be returned in a timely manner when the usage period expires. While we recognize normal wear and tear on laptops, equipment must be returned in good working condition along with all accessories provided (eg. power supply, carrying case, mouse, batteries, etc.). Users are responsible for ensuring all personal data is removed from the hard drive when equipment is returned.
13. Faculty and staff may have an option to buy-out leased laptops they have been using upon termination of their employment. Such decisions will be at the discretion of Faculty Deans and Department Directors. The University will incur no costs related to the buy-out.
14. A laptop should never be stored in a vehicle for any length of time due to temperature and theft considerations. Users will be held fully responsible for laptops stolen from vehicles.
15. Laptops should never be used while operating a motor vehicle.
16. A laptop should never be left unattended and unsecured. When laptops are used in an office or classroom setting, they will be physically secured with a locking device. If the office or classroom is left unattended, the room should be locked.

17. Laptop users will use secure passwords for all logins and services accessed from their laptop. Users should not select “remember me” options when logging into applications or websites. Passwords should be changed on a regular basis. Passwords should be “strong” (eg. complex, not easily guessable) and contain upper and lower case characters and numbers.
18. ITS oversees all laptop support and maintenance issues. Issues that cannot be addressed over the phone or via email will be done on campus at the University. After diagnosis, ITS may request that a user take their laptop to a certified repair centre. Repair status will be tracked by ITS. Modifications to the laptop, or any of its components, requires written authorization from ITS. Modification examples include adding ram, replacing hard drives, manually changing the BIOS, and marking the case.
19. Laptop data should be backed up regularly to prevent data loss. Depending on how a user uses their laptop, some data may need to be stored on the hard drive. Users are responsible for establishing a process of regular and frequent copying of data to a central storage location, such as our network, or to a secure peripheral device, such as an external drive that will be stored securely when not in use. Personal data should not be backed up to University central storage. ITS can advise on products and processes for laptop backup.
20. Sensitive data stored on a laptop, or stored on a removable storage device, should be encrypted. ITS will make recommendations to users on suitable encryption products and tools.
21. When maintenance is performed on a laptop, the user is responsible for backing up their equipment prior to the maintenance being performed.
22. ITS will maintain an inventory of all laptops that are University property. Any changes to the equipment, that are material to maintaining accurate inventory records, will be recorded in the inventory.
23. All University laptops will have an ID tag attached with identifying information and contact details.