Information and Digital Technologies
February 9, 2009

IDT Security Guidelines

Physical Hardware/Media Access

All physical hardware/media is in locked rooms or cabinets within the IDT office suite on the 4th floor or the SCC office suite on the 2nd floor of Love Library

On the 4th floor:

- Equipment inventory is kept secure in LL-464 and LL-408.
- Surplus inventory awaiting pickup is kept secure in LL-459 and LL-461.
- Software media is kept secure in locked cabinets in LL-406 and LL-465.

On the 2nd floor:

- Equipment inventory is kept secure in LL-242 and LL-252.
- Surplus inventory awaiting pickup is kept secure in LL-459 and LL-461.
- Software media is kept secure in locked cabinets in LL-227 and LL-229.

A variety of cable management is stored on LL-464 shelving and includes 2 types of cable traps, 1 hub slot lock fastener, 1 hex adapter foot, and 1 washer. These can be used to create cable security for computing and non-computing items. Also available on this shelving are Master locks/keys.

Cable management for the SCC & 24/7 areas is stored in LL-242 and includes from BMS (Business Machine Security; see http://locdown.com) BMS-SDSU2 packages (containing 1 3-foot cable, 1 cable plate, 1 cable nut, 1 mouse trap, and 1 linker each) to setup security cabling for SCC equipment. Also available in this room are Master locks/keys.

Generally, cable management is super-glued to the item with a cable running through the opening, wrapped around furniture, and secured with a Master lock. Exception - the new Dell computers now come with their own locks.

SANS and SCC & 24/7 technicians are currently handling all lockdowns of their respective workstations and printers, while Operations Support handles lockdowns of miscellaneous other equipment.

The Server Room Coordinator handles securing the physical hardware in the Library Server Room (LL-405A).

The IDT Software Coordinator or designee handles the access to the software media.

Network Access

Open access (no authentication) is available on all computers in Library buildings for the public. Novell authentication is required for employee computers and public printer server computers to reach networked services (i.e. printing).

Wireless network access is available throughout the University. Wireless network access is intended for community use, similar to connections from home. Wireless network access should not be used for University business. All systems used for campus business are connected to the wired network and wireless networking is disabled. Laptops connected via the wired network must have the wireless connection disabled.

Utilizing the wireless network access requires a registration process for the first time of use, after which access is automatic. All University acceptable use policies apply to the wireless network, as well as the wired network.

Software Access

Faculty/Staff computers with Windows XP or MAC OSX are given USER access only by default. IDT maintains an ADMIN access to these computers. This applies to both Library and non-Library customers of IDT.

Exceptions with justification allow for a second ADMIN account that the Faculty/Staff can use, if needed. Some non-Library customers (those supported by Brock Allen) are given ADMIN access with a caveat --- IDT will wipe the computer and place a fresh image, if anything requires IDT intervention.

Proof of License must be available to IDT, before IDT staff can load software to a computer.

- If the software is part of the Standard Image set, proof of purchase is on file in the Software Cabinets in LL-406. For information on the current software, see IDT Customer Resources under Facilities and Software for Standard Images by platform.

- If the software is provided by the employee/unit, proof of purchase is handled by the employee/unit. The Division/Unit head must complete a Software Release prior to installation, if no proof of purchase is available. Then the Division/Unit head must provide the installation media and complete documentation on how to install the software. In the event the employee/unit supplied installation media is lost, the Division/Unit head must contact the vendor for replacement media.

- Faculty members must provide proof of purchase for their software to be installed on any SCC workstation. The faculty member must complete a Software Release prior to installation, if no proof of purchase is available. Then the faculty member must provide the installation media and complete documentation on how to install the software. In the event the

faculty member supplied installation media is lost, the faculty member must contact the vendor for replacement media.