Teaching and Research Labs Management

Intent:

To provide policy and direction on how various lab space and resources can be effectively used and managed

Applies to:

Any course

Author:

Facilities Committee

Dates:

1 Dec 2003: last updated

30 May 2003: faculty unanimously approve this proposal

July 21st 2010: revised Ankur and Stephen

Sept 20th 2010: revised Ankur

21 Sep 2010: revised by Stephen, approved by Ankur

Context and Description:

The Cherry-Parkes building was occupied at the end of 2003, providing four new labs for the Institute of Technology. In addition, the then new CSS graduate program, increased emphasis on faculty research, and the possibility for other programs in the Institute have focused more attention on how coursework and research will co-exist, and where they will take place. The subsequent addition of the CES and the ITS programs have enhanced the need to revise this document and update the policy.

The current design of the existing labs is as follows:

1. **DOU110, SCI106** and **SCI108** are **general development labs with nearly identical software installed**. Using workstations and servers administered by Institute lab staff, students work on their course assignments and projects, communicate with others, browse for information, and learn new application skills. Occasionally, faculty members use these labs for demonstrations and instruction, especially when the software used is not typically installed in campus computer classrooms. In addition, some resources of these labs can be utilized remotely.
2. **SCI113** is now the de facto CES Senior Projects lab; its official status as such is pending faculty approval.
3. **SCI104** currently hosts some ITS TINFO 320 student labs, the second Virtual Computing Lab (VCL2), research projects, and several inactive "special teaching servers".
4. **PNK130** and **PNK131** were designated as the **graduate research labs**. PNK131 was subsequently utilized as a classroom and now finds itself in that role. Their

use was envisioned to be for **graduate thesis and project work**. Currently, we do not have a dedicated graduate research lab. ~~Like SCI113, removable hard disks containing preloaded software are available, and students can also install whatever else is desired. Unlike SCI113, the PNK130 labs have servers which were intended to be dedicated or shared by the students while they work on their thesis work or projects. Also, these labs were considered to be a place that the graduate students could call their own, to attract prospective graduates and retain existing ones.~~

Note that on 24 Oct 2003, the faculty re-purposed the use of PNK130 for student club use. Now only PNK131 is allocated for general graduate and directed research use. The rest of this document reflects this change.

PNK131 was loaned to the campus as a classroom since no one was using it. The loan period was supposed to be one year, but has lasted since. The campus administration does not view it as our classroom. When the Joy building becomes available for use in 2011, we hope to ask for the return of PNK131 as a lab for general research use.

In a late Spring 2010 meeting, Orlando, Sam, Yan, Don McLane and Stephen discussed the need for a Wireless Lab. PNK130 was proposed as the location, with the student lounge moving to CP206 Reception Area. Since then, Stephen determined that the cost for RF-shielding PNK130 for wireless exercises was very high and not useful for individualized exercises (no isolation of work). Its revised use is now as an ITS Senior Projects lab, much like SCI113's current de facto role as the CES senior projects lab.

Cherry-Parkes Labs:

The majority of the second floor space in Cherry-Parkes is devoted to the Institute of Technology. Most of that space is for labs; other uses of that central space are a conference room shared with the rest of the campus, and an Institute-only "manager's office", reception area/lobby, and repair room. On the east and west sides of the second floor are faculty offices.

There are four labs (206D, 206H, 206I, 206M) with storage closets, two server rooms (206F and 206N), and one communications room (206F). Three of the labs are about 650 sq. ft. apiece; one (206D) is about 1800 sq. ft. For more details, see the Cherry-Parkes section of the future plans of the labs.

Here is a rough diagram of the central part of the second floor. It is not to scale, but the positioning is correct and it gives a good feel for the layout.

<table>
<tr><td><table><tr><td>Comm.
206F</td><td>F/S Srv
206E</td><td>Stu. Srv
206N</td></tr></table></td><td rowspan="2">Conference</td><td rowspan="2">(Open Area)</td><td rowspan="2">Lab
206M</td></tr>
<tr><td>Lab 206D (1800 sq ft)</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td colspan="3">Reception/Lobby/Hall</td><td rowspan="2">Repair 206J</td><td></td></tr>
<tr><td rowspan="3">Lab 206H</td><td>Mgr Office</td><td rowspan="3">Lab 206I</td><td>Stor 206L</td></tr>
<tr><td>Stor 206O</td><td rowspan="2">Stor 206P</td><td rowspan="2">Stor 206K</td><td rowspan="2">(hall)</td></tr>
</table>

Here is a brief legend:

1. Comm. 206F -- locked communications room, controlled independently by faculty/staff and authorized students
2. F/S Srv 206E -- locked server room controlled by faculty/staff
3. Stu. Srv 206N -- locked server room controlled by authorized students
4. Mgr Office -- interior office space for someone related to the labs
5. Stor 20xx -- storage room tied to a nearby lab

Research Groups:

Draft Sep 21st 2010:

Lab Name	Room	Managers	Group Members (min 2)	Comments
Embedded Computing Systems (ECS)	CP206D	Larry Wear	Larry Wear, Jenny Sheng, George Mobus, Donald Hauesin, Robert Gutmann	
Information Assurance & Networking (IAN)	CP206H	Yan Bai	Yan Bai, Barbara Endicott-Popovsky	+Wireless using specialized rf testing boxes
Web and Data Science (WDS)	CP206M	Ankur Teredesai	Ankur Teredesai, Matthew Alden, Guy Johnson	
Applied Distributed Computing (ADC)	CP206I	Sam Chung	Sam Chung, Dan Zimmerman, George Mobus	
Virtual Computing Hardware (VCH)	SCI104	Stephen Rondeau	Stephen Rondeau, Ankur Teredesai, Yan Bai	Server Room for ITS if ever needed
ITS Projects (ITP)/ Graduate Research	PNK130	ITS projects coordinator or Grad coordinator	ITS/Grad committee	

Computer Engineering Projects (CEP)	SCI113	Jenny Sheng	Jenny Sheng, Larry Wear, Robert Gutmann	

Here are some observations:

1. **Applicability:** not all research areas require labs
2. **Teaching Scope:** labs may also be used for teaching, in accordance with the UWT mission
3. **External Research Scope:** research outside of these areas is likely, especially with directed study
4. **Need:** some research can be done by students using other, more general labs
5. **Sharing:** use of lab resources may be requested by people who are not group members
6. **Affinity:** setting up a research lab can be a time-consuming process
7. **Infrastructure Support:** nearly all labs require a core set of services and infrastructure
8. **Criteria:** the space should be managed to be as fair, effective, and practical as possible

Proposed Lab Types:

1. General Development Labs (DOU110, SCI106, SCI108)
2. Designated Teaching and Research Labs (SCI104, SCI113, PNK130, CP206D, CP206H, CP206I, CP206M)

Lab Management Issues:

For many reasons, including property protection, fairness, and use of external shared resources, the lab space and associated resources (collectively called "the labs" hereafter) need to be managed. The issues that need to be addressed are:

1. What does a lab constitute?
2. Who is responsible for the labs?
3. Who has the authority to change a lab or authorize its use?
4. Who pays for the labs?
5. How can the use of the labs be made equitable?
6. What infrastructure supports the labs, who does it and how is it paid for?
7. How can compliance to policies be ensured?

1. Lab constitution and contents:

Each lab provides the basics:

1. floor space
2. desks or tables and chairs
3. lighting and electricity
4. heating, cooling and ventilation

5. network connections to a centralized communications closet
6. physical access control via key cards
7. wall-mounted whiteboards (except SCI104)

Some labs also include:

1. data projectors (DOU110, SCI106, SCI108, PNK131)
2. other A/V media equipment (DOU110, SCI106, PNK131)
3. lockers (all except DOU110, SCI104, SCI113, PNK131)
4. easily movable desks (PNK130 in part)
5. storage cabinets (DOU110, SCI113, SCI106)
6. soldering hoods (SCI113, Cherry-Parkes 206J)

The Cherry-Parkes labs also include:

1. easily movable desks, some with shelves
2. stackable chairs
3. moveable whiteboards
4. display areas for posters
5. bookcases
6. lockable storage rooms
7. overhead, flexible electrical and network connections
8. faculty/staff/student-managed copper Ethernet networking

The lab constitutes the group of faculty and staff that uses the lab along with the students that benefit from it and the physical contents of that lab.

2. Responsibility:

A research group is responsible for its assigned lab(s). This includes:

- acquiring equipment (includes hardware, software packages and licenses, as well as other materials)
- tracking equipment for inventory
- securely installing and maintaining equipment
- coordinating the sharing of infrastructure beyond the basics
- recording and reporting lab usage

Responsibility can be delegated, but ultimate responsibility rests with the research group.

Each research group must have a person who serves as the lab manager. The lab manager should be active and must make it their job to know what is going on in the lab and what each lab member is doing, both to manage the lab, and to handle external requests about the lab.

It is recommended that the manager position rotates amongst group members over time, and that there is a well-defined procedure for transferring the knowledge and responsibilities between the outgoing and incoming manager.

The Institute Facilities Committee consists of all lab managers plus other stakeholders. Lab managers will be responsible for presenting a quarterly update documenting the activities of their lab to the facilities committee. These reports will be made available as part of the institute facilities committee meeting minutes. Requests for collaboration and sharing of resources can also be made during the quarterly update.

3. Authority

Members of the research group in general have the authority to manage their labs, in accordance with UW, campus, Institute of Technology, program and any funding-source policies and restrictions.

Whenever anything is shared there must be some rules. If a group member's intended actions will:

1. affect other group members, consult those members or the lab manager beforehand
2. affect other labs, consult that lab's manager beforehand
3. affect Institute infrastructure, consult with Institute lab staff beforehand
4. affect the UWT campus infrastructure, consult with the UWT's Information Technology department beforehand

The group should decide how it wants to handle external requests for lab resources.

If a resolution concerning the intended actions between the group member and others cannot be made, the faculty may decide to charge the Facilities Committee with recommending a resolution to the issue.

4. Funding

Equipment for the labs or for the infrastructure may be funded by:

- equipment donations (must follow UWT guidelines)
- gifts
- grants
- program budget funds
- Institute of Technology budget funds

Please keep in mind there are many types of equipment costs:

1. fixed, one-time costs such as the outright purchase of hardware
2. maintenance costs, to keep existing equipment operational/usable
3. renewal costs, to replace existing equipment with better equipment
4. periodic costs, usually for services or subscriptions

The cost of labor may be the largest cost, but it won't be covered here.

5. Equitable Use:

If someone outside of a research group wants to use that group's lab, then the outsider should take these actions in the order given:

1. Contact the lab manager for that group, who will bring it back to the members for a decision.
2. If an unfavorable decision was made, appeal to the program's Facilities Committee to determine if there may be similar resources available elsewhere. The requester is encouraged to submit a written request ahead of the next facilities committee meeting to explain the request.
3. If no resources are available, appeal to the program's faculty to determine if the Facilities Committee should be charged to recommend developing or re-allocating some resources to satisfy the request.

6. General Infrastructure:

Complex entities don't stand by themselves; they rely upon other entities. What gets relied upon is the infrastructure, the stuff that is often hidden from view but is essential, like electrical power is to computing.

Nearly all labs will need access to the infrastructure. Basic infrastructure for labs such as its walls, ceiling and floor as well as lighting are often taken for granted. Other infrastructure, such as cooling and electricity are more well-known because we sense when something is too hot or a circuit trips if too much electrical load is placed on it.

Here are some references for infrastructure contacts:

1. **building functions** (structural, electricity, plumbing, heating/cooling, ventilation, lighting)

   These areas are handled by campus Facilities personnel.

2. **data and voice communications** (telephone network, data network)

   The first point of contact is campus Computer Services. Additional detailed help with the operation of the data network can come from Computing and Communications (C&C) Network Operations staff.

3. **safety and security** of people, rooms and buildings

   From any campus phone, dial **#333** to contact campus safety and security personnel.

4. **presentation and projection** (media)

This is supported by the campus Media Services department.

Institute of Technology Infrastructure:

Institute lab staff manage:

- the general development and graduate research labs
- the servers and server network backbone behind the general development labs
- the software installed on all of those computers and removable hard disks
- general development lab reservations
- general development and graduate research lab printers
- various lab resource allocations, as recommended by the Facilities Committee
- networking of computers within those labs

This translates to a variety of services that **Designated Teaching and Research Labs** could use, as noted below. The research groups would be delegating responsibility and funding any such services, to whatever level is desired:

1. Full: all services are provided by Institute lab staff
2. Partial: some services are provided by Institute lab staff
3. None: no obligation to support; low priority if request is not an emergency

Here are the possible services:

1. Centralized Authentication and Authorization

   Normally, the operating system provides the mechanism for defining and managing users; once defined, they can be allowed access to various resources. The problem is that unless some planning is done ahead of time, each computer will only be able to authenticate the users it knows about. A central authentication source is desirable to reduce the amount of user account management.

   Using authentication and authorization, users can be accountable for their actions and the path of entry for anyone trying to infiltrate lab computers may be more easily identifiable and therefore fixable. One can also perform accounting of resources, to construct reports on usage of the authorized resources.

2. Centralized File and Application Access

   Data are typically stored in files that reside on fixed or removable media. If the storage medium is not accessible, the data cannot be used. In addition, if something happens to that storage medium, the data may be lost.

   Centralized file systems allow data stored there to be accessed by anyone who is connected to the file systems. Modern file systems are networked and accessible from the Internet, making access to files possible from any computer able to connect to the file server. Authentication and authorization protect other users

from being able to use the data without permission. However, if something happens to the storage for a central file system, the data may still be unrecoverable.

Since most applications are simply a collection of files, given the correct licensing, some can be centralized as well and run over a network, to avoid installing the application on individual computers. An alternative method is to distribute just the interface from a central site to a user, so that it appears that the application is running locally. This is the "terminal server" or "display server" point of view.

Another aspect made easier by centralized file systems is volume management -- the ability to expand storage easily. Windowsand Linux both have this capability for individual workstations or servers.

3. Data Retention

   Data retention services provide backup and restore capabilities. By copying files on a periodic basis to another storage device, one can recover from the failure of the original storage device. Data retention systems are key to the reliability of a centralized file system. Note that a centralized file system permits centralization of backups for all computers connected to it.

   One might also consider disk arrays as a means of protecting data from the failure of a disk drive. RAID 5 (Redundant Array of Inexpensive Disks, Level 5) provides parity and striping of data across disks. If one disk in the array fails, the data is still accessible via the parity information, although at a slower rate, until a new disk is added to the array and the array is rebuilt.

4. Data Distribution and Replication

   There are many instances in which you want to distribute something, like an application or a data file, from one computer to one or more others. You can often do this over the network with the right software, or the storage medium can be duplicated, as in a CD duplication device.

   When managing a lab with many computers in it, it is often useful to make one image of the operating system and applications that all lab computers will share, then to re-image their individual disk drives with that master image. This saves a lot of time and reduces the chances of making a mistake when manually installing the same thing many times.

5. Remote Access

   Students and faculty want to conveniently access their information and applications on a computer in a lab from their home or office computers.

Providing this capability requires a secure means of remotely accessing the computer. However, one must always consider software licensing issues when distributing applications

An additional concern may be remote control of servers. It is possible to control the power (turn it on and off), send keystrokes, view the display, and create and use virtual floppy disks remotely, although it takes more non-standard hardware to do this.

6. Printing

   If a printer is not locally attached to a computer, it needs to be networked in some manner in order to print from another computer and to manage the print jobs. A central print server can do this, or it can be set up with a designated computer in the lab.

7. License Pooling

   Commercial software is not sold, it is licensed. Use is bound by the terms of the license. Unless otherwise stated, you can install commercial software only on one computer or removable hard drive. If you want it on several computers or removable hard drives, you will need to purchase enough licenses to cover the number you will install.

   Often, there are volume licenses that significantly reduce the cost of licensing. In general, the more licenses one buys, the cheaper the per license cost, so it is cost-effective to consult others about your intended purchase to pool your request with theirs, or perhaps extend an existing volume license to include your additions.

   The UW campus may already have some kind of volume license you can use.

8. License Management

   Once a license is purchased, it is useful to know where it is used and how often it is used as well as have a mechanism to ensure that the number of uses don't exceed the number of licenses. This is the function of a license management tool, which is a central license server.

   Additional license management software licenses would still need to be purchased, but they can be pooled just like any other software.

   There are several advantages to managing licenses:

   a. Knowing how often a license is used helps one estimate costs for renewing licenses.

For example, if you bought 10 licenses but found that a maximum of 3 were ever used, your next renewal of the license might be for 5 (to account for a little extra growth).

b. Since the number of licenses in simultaneous use is enforced, you may be able to use existing licenses for non-license management software.

   This depends on the wording of the license.

c. The licensed software may be able to be installed on all license-managed computers instead of specially designated ones.

   This depends on the wording of the license. If possible for all software on a disk image, it simplifies the task of managing a lab of similar computers because the same disk image could be placed on each computer.

9. Network Connectivity

   The advantages of connecting to the network using a centrally-managed scheme are as follows:

   a. Control of network bandwidth use

      Quality of service (prioritized traffic) as well as providing fair use of bandwidth are possible.

   b. Filtering of network traffic to reduce effects of outside attacks
   c. Remote management of the network ports
   d. Gathering statistics on network usage

10. Security

    This topic covers physical access, individual computer and network security.

    a. physical access security

       Securing physical access to lab resources involves some kind of physical access controls. Common ones are door locks and key cards, but combination door locks, locker locks and cabling something to an immovable object are also used. Security cameras can also be used to deter or record activity in the labs.

       Generally, people who have access to a lab can use whatever is available. However, it is often prudent to secure some things to make sure they remain in the place you designated for them or to impede a thief from taking expensive or desirable equipment.

b. individual computer security

Anyone who has physical access to a computer can break into it. You can impede this somewhat by locking the computer case, putting a password on the BIOS and disabling booting from anywhere other than the hard disk, but there are even ways around this. Most of the time, it isn't necessary to take such measures, but some research requires it for sensitive or classified data.

Beyond physical security and ensuring that rogue software isn't involved in booting up the computer, one needs to make sure that rogue software isn't installed on the computer. This is often accomplished by installing antivirus software. It doesn't protect against all attacks (only the ones it knows about, which excludes newer ones than in its database). It also must be set up properly and on the network to keep up to date with the latest attacks.

One critical element in protecting a computer from attack is keeping up to date with the latest patches and updates for the operating system and application software.

c. Network security

As soon as a computer is added to a network, it is capable of being attacked by any other computer on the network. Centralized network control (see network connectivity above) can help in preventing attacks from affecting others. Unused network "ports" can be blocked, unused services can be turned off or uninstalled, public keys can be used for trusted computers, and other techniques can be employed to reduce the likelihood that a computer is attacked from the network, or is surreptitiously used to attack other computers.

Also, the use of unencrypted network protocols (e.g., ftp and telnet) can expose passwords to whoever has access to the network infrastructure. This is more prevalent today with wireless networks and good network "sniffing" tools.

11. Inventory Management

The UW as an institution wants to know where valuable equipment is. Anything over $2000 needs to be tagged with a white UW asset tag and recorded. For computer equipment, campus Computer Services can supply tags and sheets to record the data about the equipment.

Purple asset tags are used for equipment under $2000.

Institute or program-specific barcoding of equipment may make it easier to determine what you still have in a lab, or to help separate equipment you have as a researcher vs. what belongs to the program or UW.

7. Ensuring Compliance

At least once per year, the Designated Teaching and Research Labs will be reviewed for compliance with stated policies. The intent is to prevent damage to data, networks and equipment as well as to prevent or detect loss of equipment due to theft.