The Computer and Information Science department has a robust computing infrastructure designed to support the academic, administrative, and research missions of the department. As a student in CIS, you have access to many of these resources and others available upon request.

**CS Account**

Within 24 hours of enrollment in your first CIS classes, a CS account will automatically be created for you. Your username and password are identical to those you would use access other IUPUI resources (e.g. Oncourse and Onestart). As such, if you wish to change your password, you will have to use the UITS password page, [https://passphrase.iu.edu/](https://passphrase.iu.edu/), and follow the guidelines there.

**Core Services**

CIS runs many of its own servers such as email and web. As soon as your CIS account becomes active, you are welcome to take advantage of these. Your home directory is automatically mounted on any UNIX/Linux system you access. Your quota limit is set to 250MB. If you need more space, your advisor can request an increase on your behalf.

**Pegasus.cs.iupui.edu:**

This server is the general purpose workhorse for the department. It includes compilers and applications to help with much of your coursework. As with all our UNIX and Linux systems, you will need to use SSH to login. Windows based SSH clients (putty and WinSCP) can be obtained via IUWare.

**Tempest.cs.iupui.edu:**

Tempest is our primary web. As a CIS student, you can create your own website. To do so, log into pegasus and create a directory called public_html and put your files in there. Those files and directories will need to be world readable. Your URL will be [http://www.cs.iupui.edu/~<username>/](http://www.cs.iupui.edu/~<username>/)

Note that we do support personal CGI and PHP but they will need to be run via cgiwrap. Details about that can be found on the CIS IT FAQs (currently being rewritten).

Tempest is also the department email server. When you receive your CIS account, you automatically get a CIS email address as well. Your address will be <username>@cs.iupui.edu. Included into the email system is extensive spam filtering with a web interface that you can use to see any messages that has been quarantined, add addresses to white/blacklists, and tweak other filtering settings. You will need to log into the web interface initially to activate the filtering. The URL to use is [https://tempest.cs.iupui.edu/mail/](https://tempest.cs.iupui.edu/mail/). You will need to use your email address as your username.

As for accessing your email, most people use GUI programs like Thunderbird or Outlook. Here are some settings you will need:
Incoming Server: imap.cs.iupui.edu / SSL / Port 993
Outgoing Server: smtp.cs.iupui.edu / SSL / Username login / Port 465

When you connect, you will receive a warning about the SSL certificates. We are using self signed ones. You can accept these permanently the first time and not be asked again. If you are using Outlook as your mail client, you will need to import these certificates in order not to be asked about them every time you log in. They can be downloaded from the following URLs:

http://www.cs.iupui.edu/facilities/certs/imap.cs.iupui.edu.crt
http://www.cs.iupui.edu/facilities/certs/smtp.cs.iupui.edu.crt

General Purpose Labs:

SL251 is our primary, general purpose lab. It includes Dual-Core 3.0GHz PCs running Windows 7. You can also access our Linux servers via those PCs via putty and Xming. Access is the room provided via your JagTag. To get your JagTag added, please contact Nicole Wittlief or send an email you soshelp@iupui.edu

Research Facilities:

Many of you may also work in one of the research labs supporting faculty research. Space and access to resources will be allocated as appropriate. When you are assigned a workstation, you will also receive a local administrative access to that system. Please see and sign the attached Privileged Access Policy and return to your advisor as soon as possible. A copy of this policy can also be found at :

http://anvil.cs.iupui.edu/mediawiki/index.php/Privileged_Access_Policy

If you do need this privileged access to other research systems, your advisor can request it on your behalf.

Our Faculty members periodically bring guests to the lab. Often this is unannounced so we would greatly appreciate it if you can keep your work area neat and presentable at all times.

Printing:

Printers are available in each of our teaching and research labs. Unlike many other facilities on campus, we have chosen not to deploy the pay-for-print model. To help us, please only print what you need and if you need to print very large documents, you should find the department copier as one of your printer options.

If you notice any problems with the printer, low toner, or no paper, please let us know as soon as possible.

Acceptable Use Policy:

System and network security is very important to us (and is a personal area of research for me). As such, you should not do anything which may weaken or compromise the integrity of CIS resources. A copy of the current CIS Acceptable Use Policy is attached.

Getting Help:
The Computer Science department uses an online request ticket for all problem reports and new software/hardware requests. Requests can be submitted directly by sending emails to soshelp@iupui.edu. You can track the status of your requests via the following URL:

http://rt.science.iupui.edu/

Note that this site can only be accessed from on campus or via a VPN connection.

If you have any questions, my personal email address is sorr@cs.iupui.edu. You can also call my office – 274-9734

Welcome to the department and please don't hesitate to come to use with questions or problems.
User Accounts Policy

IUPUI Computer Science Department Computing Conduct Policy

The IUPUI Computer Science Department provides various computer accounts to faculty, staff, students, alumni, and guests of the department. The use of these accounts is subject to the following policies.

As a member of the Indiana University computing environment, users of the Computer Science Department computing facilities are required to abide by the policies set forth in the Indiana University Computer User's Privileges and Responsibilities Document as well as any other policies governing conduct at Indiana University. Many of the policies outlined below are also included in the IU policies but are included here for emphasis.

- **No illegal activity** - Your account must not be used to engage in or assist any illegal activity including, but not limited to, harassment, abuse, fraud, theft, and vandalism.

- **No commercial activity** - We do not allow any commercial activity from CS computers without prior authorization. Some examples of things that are not permitted would include sending out email advertisements, hosting a business web page, or selling advertising space on your CS homepage. If you have any doubt about whether your activity would be considered commercial, please ask.

- **No SPAM** - In the context of email, spam can be defined as the sending of bulk quantities of unsolicited email and is prohibited. In the context of Usenet News, spamming means to send a message to a large number of newsgroups where most of the newsgroups have nothing to do with the subject of the message. Spam violates the spirit of the university community.

- **Account monitoring** - The CS department IT staff reserves the right to monitor all system activity in the event of any real or suspected security threat. This may include, but is not limited to, the monitoring of keyboard input, file contents, or network traffic as needed to assess, control, or stop any security-related attack on our computing systems.

- **No account and password sharing** - Your account is for your use only. You must never allow anyone to use your account for any purpose. You should protect your account password and never give it to anyone. No member of the CS IT support staff will ever need or ask for your password. You must also not configure your account (via .rhosts, .shosts, .ssh/authorized_keys, or other similar authentication method) in such a way as to permit others to gain access to your account.

- **No setuid/setgid programs** - On a unix/linux system, a setuid or setgid program allows other users to run programs under your user identity or group. Such programs are not allowed without prior approval.

- **No anonymous activity** - Nothing you do on the CS systems should be identifiable as having been done by anyone else. You should never attempt to
send email or newsgroup messages in such a way as to conceal or forge your identity.

- **Respect the privacy of others** - Just because another user has left files in his or her home directory world readable, this does not give you the right to use them. Some users do not understand the file protection mechanisms that are available and may inadvertently leave files readable.

- **Do not attempt to compromise system security** - The CS department is very concerned with the security of its systems and you should engage in no activity that might compromise security. For example, you should never try to exploit a potential security vulnerability to gain privileged access to any CS system even if your intent is just to experiment and not do anything malicious.

- **Your home directory must conform to certain security-related constraints** - There are certain file and directory permissions you can set that open your home directory up to attack or use by other users. For this reason, your home directory must not violate the following rules:
  - Your home directory must not be writable by any other user. This could include setting the group or world write permission bit or by using Access Control Lists (ACLs).
  - Your ~/bin directory must not be writable by any other user.
  - The following files in your home directory must not be writable by any other user: .forward, .emacs, .cshrc, .login, .profile, .bashrc, .tcshrc, .kshrc.
  - The following files in your home directory must not be readable by any other user: .rhosts, .shosts, .Xauthority.

The systems staff does scans to identify files and directories that violate these rules and the permissions may be changed without notice.

- **No unauthorized persistent server processes** - A persistent server process can be defined as any process that makes it possible to access system resources from a remote machine for an extended period of time (1 day or more). Some examples of servers are web, ftp, irc, and news servers. Users are not permitted to run any such server process on any CS machine, or non-CS machine using the CS network without faculty sponsorship and approval from the CS faculty or IT staff.

- **Don't overload system resources** - You should engage in no activity that overloads the computing systems or support staff. You should also never run cpu-intensive processes such as SETI@Home or any of the various crypto-challenges on any shared machine without prior approval.

- **Do not leave machines locked** - The machines in the student labs should not be left screen-locked for more than 15 minutes. These machines are for use by multiple people so you should logout if you are going to be away from the machine for any length of time. You may be logged out of any machine left locked for longer than 15 minutes. Screen-locking is permitted in the research labs but please make sure you save all important work before leaving. The IT staff may need to access your machine to make configuration changes in your absence.

All CS accounts are provided as a courtesy by the Computer Science Department and we
reserve the right to remove or disabled accounts at any time without prior notice.
Privileged Access Policy

The following policies govern privileged (root, superuser or administrator) access to Computer Science workstations and servers. They are designed to protect the integrity of these systems, while allowing appropriate access for research purposes. Failure to follow these policies could result in having access revoked. A signed copy of this policy must be on file with the Computer Science IT staff as part of the access granting process.

These policies serve to augment the User Accounts Policy.

Desktop Workstations

When a student is assigned a workstation in one of the Computer Science department research labs, he/she will also be provided with local privileged access to that workstation. Privileged access will be for a specific research purpose and will expire when no longer needed for that purpose.

Privileged Access Restrictions:

- Users do not have permission to modify any files except in designated user directories without specific authorization from the IT Staff. Specifically, no system configuration files may be modified unless specifically authorized.
- Users may not use their privileged access to examine or modify the files of any other users of the system.
- Users may not give other students access to the privileged access account.
- Users may not add or remove users from the workstation.
- Users may not add or remove software and operating system components other than what is required for their research project.
- Users may not in any way compromise the security of the system.

Privileged Access To Special Purpose Research Computers/Servers

Privileged access to computers designated for special-purpose research may be granted to users of those computers. Such special-purpose computers will not have any users' home accounts or contain confidential information. Mechanisms and policies governing privileged access will be agreed to by the faculty members responsible for the computer system and the IT staff. If necessary, the IT staff may impose other restrictions on such computers in order to protect the security of the computing facility.
If privileged access is granted:

- Users do not have permission to modify any files except in designated user directories without specific authorization from the IT staff. Specifically, no system configuration files may be modified unless specifically authorized.
- Users may not use their privileged access to examine or modify the files of any other users of the system.
- Users may not add or remove users from the workstation.
- Users may not give other students access to the privileged access account.
- Users may not add or remove software and operating system components other than what is required for their research project.
- Users may not in any way compromise the security of the system.

### Privileged Access To Other Facilities

Privileged access to the following CIS facilities is restricted to designated IT staff:

- Instructional facilities
- Servers and Infrastructure computers
- General-purpose multiuser computers

By signing below, you agree to abide by the Privileged Access Policy terms described above.

Student Name: ________________________________

Student Signature: ______________________________

Date: ________________________________

Workstation/Server Name: ________________________________

Advisor Name: ________________________________

Advisor Signature: ________________________________