Technical Computing Staff

Duties

Dave McKinsey
4-8042
mckinsey@mail.sdsu.edu

UNIX System Administration
Server Administration All platforms
Network Administration
Security
ESRI Technical contact
Erdas Technical contact
Coordination of technical staff activates
Coordination of day to day lab operations
GIS/Image processing assistance
Hardware support
Project support
Assist as needed

Marcus Chiu
4-8618
mchiu@mail.sdsu.edu

Windows System Administration
Server Administration
Faculty, Staff, Student Helpdesk
Operating Systems Support
Software Support
Hardware Support
Network Administration
User Accounts
Campus ESRI Contact (installs, and troubleshooting)
Smart room Facilitator
Assist as needed

Harry Johnson
4-0405
harry.johnson@mail.sdsu.edu

ESRI ArcGIS Online Administrator
ESRI Training Administrator
Campus GIS
Department Web Master
Faculty/Staff/Student Web page support
Faculty/Student GIS/Cartography support
Macintosh System Administration
Faculty/Staff/Student Hardware/Software support
San Diego Regional GIS Council Representative and web master
Assist as needed

Pete Coulter
4-6973
lcoulter@mail.sdsu.edu

Campus GIS Manager
Remote sensing/image processing support
Image data requests
Terrain data support
LIDAR support
GPS technical support/training
Custom airborne multispectral image collection
Spectrometry support
Assist as needed
Resources

Labs
The department has six labs dedicated to teaching and research. The CESAR lab, the Visualization lab, the Qualitative lab, and the William Finch Remote Sensing Lab are primarily research labs, however, they are used for teaching on occasion. The Richard D. Wright Spatial Analysis Lab is the primary computer lab for teaching. The Physical Geography Laboratory is the primary lab used for the 101 Laboratory sections.

As of the composition of this document, the distribution of computers throughout the research labs was still undecided.

Hardware

Richard D. Wright Spatial Analysis Laboratory (SH-324)
Computers: 26 Dell Precision Workstations, Windows 10
Printers: 1 HP LaserJet 600 M602 (Little_Cesar), Letter/Legal, B/W
            1 HP Color LaserJet CP4025 (Inkpot), Letter/Legal, 4 color
Equipment: 1 HP Scanjet 3970 Flatbed scanner

Cesar Laboratory (SH-328)
Computers: 7 Dell Workstations, Windows 10
            1 Sun Ultra 27, Windows 10
Printers: 1 HP LaserJet 600 M602 (Cesar), Letter/Legal, B/W
            1 HP Color LaserJet Enterprise M750 (ColorPig), Letter/Legal, Color
            1 HP DesignJet 5500ps (Nib), 42” paper roll, 6 color
Equipment: 1 CalComp DrawingBoard III Digitizer, High Precision
            1 Colortrac SmartLF SG Wide Format (44”) Flatbed Scanner

William A. Finch Jr. Remote Sensing Laboratory (SH-331)
Computers: 10 Dell Workstations, Windows 10, 3D capable
Equipment: Manual stereoscopes and air photos (for exercises)

Physical Laboratory (SH-333)
Computers: None
Equipment: Field Equipment

Qualitative Laboratory (SH-337)
Computers: 1 Apple iMac Workstations, Windows 10
            1 Apple Mac Pro Workstation, Windows 10/Mac OS 10 Dual Boot
            1 Dell Precision Workstation, Windows 10

Visualization Laboratory (SH-339)
Computers: 8 Dell Workstations, Windows 10
Equipment: 1 HP Scanjet 3970 Flatbed scanner
Software
The following list is not comprehensive in terms of software. It lists the main titles for GIScience applications. Software is constantly being evaluated and added to the installed base.

GIS
Windows: ESRI ArcGIS ArcInfo level; Business Analyst, Feature Analyst and other various extensions
ESRI ArcGIS Pro
IDRISI Terrset
QGIS
Common GIS

Remote Sensing
Windows: ERDAS Imagine
ERDAS LPS
ENVI
Definiens eCognition Developer

GPS
Windows: Trimble Pathfinder Office

Statistics
Windows: SAS
SPSS
R

Various desktop (Microsoft Office Suite), graphics, web design (Adobe), and utility applications are also part of the installed base. Please check the platform installations to find the comprehensive listing of software.

Students are not allowed to install software on the lab computers. If there is a specific application that is necessary for dissertation/thesis/project completion, please inform the technical staff and that software will be placed into the installed software base. Please inform the staff prior to the start of the semester, prior to the software image update, otherwise the installation may be delayed.

Software Base Updates (Imaging)
Prior to each semester, the installed software base for each platform is updated. This update includes operating system updates, security patches, application updates and any new, approved, software requests.

To construct the update, one computer from each platform is removed from general use. The operating systems and application updates are placed on these machines and a snapshot or image is taken of the completed installation. This installation becomes the new software installed software base.

Just prior to the start of semester, all lab computers are taken out of service and the new installed base applied. This generally takes less than a day.
The technical staff will inform all faculty, staff and students when these events will occur via email to the department mail lists.

**Printing**
All the printers and plotters are departmental resources. 
Mailroom printer is for use by the department as a whole. The department purchases all supplies.

Spatial Analysis Lab printers are for use in classroom lab instruction. The department purchases all supplies.

CESAR printers are for use by projects. Supplies are purchased through CESAR funds contributed by the respective projects using the facilities.

**Quotas**
Quotas are set by month and vary by printer. Unless specifically listed below, students will have no printing quotas set on department printers.

**Print/Copy Room**
All funded students (Ph.D., GA/TA) – 400 pages per month
Unfunded graduate students – 100 pages per month
Class accounts – determined by instructor

**Richard D. Wright Spatial Analysis Lab**
Class accounts – determined by instructor

**CESAR Lab**
Project G.A.s – unlimited (Soft quotas set, will be adjusted by request to Dave McKinsey or Marcus Chiu)
Large format printing for research, conference, and presentation posters on request.

Printers located in Faculty or Staff offices are for the exclusive use by said Faculty or Staff member. No quotas are set for these printers.

**Office Computing**
Each graduate student office has at least one computer to be shared between the office students. These computers are connected to the department domain and off-campus internet. These computers are for word processing, on-line research and other activities related to graduate studies. Generally these are former lab machines that have been replaced by newer models.

Occasionally, research project computers will be placed in the student offices. The Principal Investigator will set proper use policies for these machines.

Student personal laptops are not to use Ethernet cables to plug into the wall sockets. The department has wireless capability. Using the wireless connection, however, will not allow access to the department
domain. Transfer of files from the domain must be accomplished by either SFTP or by copying to a removable disk or device.

**Education Licenses**

**ESRI**

The CSU Site License with ESRI includes an ArcGIS On-line (AGOL) Organization, access to free on-line training, and student software licenses.

An AGOL account allows students access to all the features of AGOL, including creating web maps, web apps, and story maps. Each student account will have a quota of 100 credits. Additional credits can be granted if necessary for assigned class or project work.

Association with the SDSU AGOL Organization is also required to access the free ESRI on-line training classes.

Finally, the site license grants students the opportunity to install and run ArcGIS Desktop and/or ArcGIS Pro on their personal computer. These student licenses are active for one year and can be renewed each year a student is associated with the university. License renewals occur during the Fall Semester.

Please see Harry Johnson to obtain AGOL accounts and software licenses.

**ERDAS Imagine**

The CSU Site License for ERDAS Imagine allows students to install and run the ERDAS Imagine Remote Sensing software on their personal computer. These student licenses are one-year licenses and can be renewed as long as the student is associated with the university. License renewals occur during the Spring Semester.

Please see Dave McKinsey to obtain an Imagine license.

**Data**

**Archive**

The department maintains archives of GIS (vector and raster), terrain, imagery, and ESRI distributed data. The majority of these data were created/obtained for funded research projects. These data are available to all students to use for class, dissertation/thesis, or other research purposes.

The archives are still being populated with legacy data. The department has other data available for use. Please ask the staff if we have data that are not in the archives.

The archive is located at:  \Globe\DataLib
Additional Instruction

GPS
Depending on demand, technical staff member Pete Coulter may hold a GPS seminar. This seminar will introduce GPS fundamentals, GPS applications/functionality, department equipment (hand-held, mapping, survey), and the policies for use.

If/when any particular student needs complete training, a hands-on training session will be setup and other students invited to attend.

The date of the seminar will be announced via the GRADSTU department email list.

Accounts

Department
All graduate students receive a department computer account. This account allows students to use the lab and office computers and access the department domain. This account will be active while the student is enrolled at SDSU.

In order to receive the account, students must read the Security and Acceptable Use Policy sections and fill out and sign the Account Request Form. These forms are available from Harry Johnson. A faculty member must also sign the form (sponsor, Principal Investigator, or committee chair). Forms should be turned in to Marcus Chiu. Accounts will be issued within 48 hours of receipt of the request.

Due to security requirements of the university, passwords need to be updated every six months. Currently, passwords need to be 12 characters long, include 1 uppercase, 1 lowercase, 1 number and 1 special character.

Graduate space
All graduate students receive space on the department servers to store personal files related to graduate work. This space is usually mapped to the “Z” drive letter on Windows machines. The owner is the only person who has read/write access to the files in their directories.

The server space for these directories is shared among all graduate students. New graduate students receive 1GB by default.

Research space
File space is also assigned for funded projects and dissertation/thesis work. Principal Investigators request project space. Students request dissertation or thesis space with the approval of their committee chair. Direct research space requests to Marcus Chiu.

Backups
Student directories (“Z” drive) are backed up every week. It is recommended that students back up important files (dissertation/thesis drafts) to removable devices frequently.
Research directories (project/dissertation/thesis processing) are every week. Exact day varies depending on drive location.

University
All new graduate students should have received an SDSUID account and activation instructions.

SDSUID provides access to Microsoft Office 365, student email via Office 365, secured wireless (eduroam) and video conferencing. Please see http://sdsuid.sdsu.edu for more information.

E-mail
The SDSUID account is your campus email address. Please provide Harry Johnson with your SDSUID.

The campus email address is the only one that will be placed on the department mailing lists. The department uses the email list gradstu@geography.sdsu.edu to communicate important information to all graduate students. This list is also an appropriate method to communicate with fellow students. Students may be placed on other lists as appropriate.

Please check email often to keep up to date on department announcements.

The Department has restricted the email lists so that only those addresses on the lists can post to the lists. This was done to limit spam or other junk mail.

Addresses that bounce for whatever reason (i.e. mailbox full) will be removed from the department lists.

If you need assistance with SDSUID, please visit http://sdsuid.sdsu.edu.

Web Page
SDSU does not provide web hosting services for students.
Security Policy

Lab Security

Hours
CESAR and Finch Laboratories
7:30am – 4:00pm Monday through Thursday
7:30am – 3:00pm Friday
Closed Saturday and Sunday

Richard D. Wright Spatial Analysis Laboratory
7:30am – 9:00pm Monday through Thursday
7:30am – 4:00pm Friday
9:00am – 5:00pm Saturday
Closed Sunday

Physical, Qualitative, and Visualization Laboratories
Closed except for class times

These hours are subject to change depending on Graduate Student availability.

The lab doors are locked outside these hours.

After Hours Access
Access after normal hours is only through RedID card access. Students without card access can utilize the labs after hours if a student with access is also in the lab. Students may also request card access to the labs, however, access will only be issued due to special circumstances.

Laptop Policy
At no time will personal laptops be allowed to physically connect to the Ethernet network in the labs or offices. If a student is caught connecting a laptop to the network, that student will have their department account suspended.

The university has installed wireless routers in the building. All properly equipped laptops can connect to the Internet through the wireless network. As the university administers the wireless network, access to the Geography Department computer domain is restricted. Therefore, printing wirelessly to the department printers is not possible. The only method to wirelessly access files on geography servers is via secure file transfer clients.
University Policy

To view the entire University Security document, see http://security.sdsu.edu/policy/security-policy.html.

Introduction

The mission of San Diego State University (SDSU) is to provide high-quality education for undergraduate and graduate students, and to contribute to the solution of problems through excellence and distinction in teaching, research, and service. Computers and network resources, including the World Wide Web, play an important and essential role in fulfilling the educational mission of the University. In keeping with this mission, the University endeavors to provide a safe and secure computing environment.

Computing resources—hardware, software, and the data—are vital University assets. All users of SDSU computing resources need to be aware of and respect the value of these resources. By using these resources all users are part of a community responsible for ensuring that data is kept confidential, reliable, and available, and that the integrity of SDSU computing resources is not jeopardized.

San Diego State University recognizes that local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media and intellectual property bind all members of the University. It also recognizes the responsibility of faculty, management, and system administrators to take a leadership role in implementing existing policies.

To ensure that all members of the SDSU community have a clear understanding of the University's policies regarding computing resources, this document, the SDSU Computing Security Policy, was written and its guidelines implemented. It provides a framework for the implementation and enforcement of computer and network security policies at SDSU. The document assists the faculty, staff, and students in understanding the need for and the means of protecting SDSU's computing resources.

Faculty who require or recommend the use of University technology resources in their courses are encouraged to notify students in their course syllabus of this policy and its possible effect on their academic activities.

Reasons for a Security Policy

The SDSU Computing Security Policy defines the minimum standards for a common level of security that is to be implemented across all computing and network resources at SDSU. This policy may be supplemented by additional policies and guidelines created by the individual campus units. The supplemental policies will address each unit's specialized security needs with the understanding that they are consistent with the standard defined in the SDSU Computing Security Policy. It is the responsibility of the individual campus units to inform their subset of users regarding any documents specific to their processing environment.

This policy makes an effort to explain the rationale and intent of the policies contained in this document, and where appropriate, provide common examples of forbidden or unauthorized activity. Where examples are provided, they are not intended to be a complete list of authorized or unauthorized
activities and are provided only to clarify the intent of the policy. This document also assumes as a condition of use the exercise of common sense, common courtesy, and a respect for the rights or property and privacy of the University and other users.

Issues concerning the "appropriate use" of computing resources, other than those dealing with security or legal issues, are not covered by the SDSU Computing Security Policy.

**Scope**
The SDSU Computing Security Policy applies to all SDSU computing and network resources including computers, software, data, and communication networks controlled, administered, or accessed directly or indirectly by users at SDSU. Privately owned computer systems, when attached to the campus network and/or resources, are subject to the same responsibilities and regulations as pertain to University-owned systems.

The SDSU Computing Security Policy only covers computer security and is not a substitute for other campus policies related to campus computing.

This document addresses five key principles of security and the responsibilities that each individual has:

- Privacy of Data
- Data Integrity
- Service Integrity
- Legal Issues
- Authorized Use

**Privacy Statement**
The University supports each individual's right to privacy when using SDSU computing resources, and will take reasonable steps to ensure security of these resources. However, the University cannot guarantee absolute privacy of electronic communication and computing resources. Each user must recognize that risks exist with regard to the confidentiality of personal email, data, files and activity logs due to system limitations, software bugs, unauthorized activity, and potential system failures.

Data contained on SDSU computer systems is accessible to authorized personnel. These individuals are responsible for conducting normal system administration activities including diagnosing or correcting problems. Additionally, should suspicious activity become evident and at the request of the appropriate administrative authority, files may be examined by system personnel to determine if a user is acting in violation of the policies defined in the SDSU Computing Security Policy, other University policies, and state or federal statutes. Access to University computer systems and accounts is generally monitored. In addition, systems and accounts may also be more closely inspected or monitored when:

- Activity from a specific account prevents access to computing or networking resources by others.
- Usage patterns indicate that an account is responsible for unauthorized or illegal activity.
- There are reports of violations of policy or law taking place.
- It appears necessary to do so to protect University resources or data or to protect the University from liability.
- It is required by and/or consistent with law.
As a public institution, data on SDSU computer systems may also be made available to the public through public record laws. All requests for such data should be immediately forwarded to campus legal counsel.

**Authorized Access and Use**

Access to University information resources may be granted based on the following: relevant laws and contractual obligations, the requester's need to know, the information's sensitivity, and the risk of damage to or loss by the University. Access may be temporarily or permanently revoked for violation of security policy, other campus policies and CSU policies.

The University reserves the rights to limit, restrict, or extend computing privileges and access to its information resources. Data owners, whether departments, auxiliary units, faculty, students, or staff, may allow individuals other than University faculty, staff, and students access to information for which they are responsible. Methods for such access should not violate any license or contractual agreement, University policy, or any federal, state, county, or local law or ordinance; nor degrade the performance of the University community. Access by non-University members is subject to approval by and at the discretion of the system administrator(s) responsible for the information resource(s) involved.

Every authorized user is responsible for the integrity of these resources. All users of computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.

**Responsibilities**

**User Responsibilities**

A user is one who has authorized access to University computing resources. Everyone on or off-campus who accesses a University computing resource, through whatever authorized (or unauthorized) means, is considered a user and is bound by the user responsibilities stated in this policy.

A. You are ultimately responsible for the effect(s) of computing activity when using a computer.
B. Accounts created for an individual is for the use of that individual only. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use of their account.
C. Use only those computing resources for which authorization has been issued. Do not attempt to obtain system privileges to which they have not been granted or give unauthorized access to others.
D. Do not violate the security policy on any computer or network facility, interfere with the authorized computer use of others, or interfere with the normal running of services on any computer system or network. This includes unauthorized modifications to software or hardware of any computer or network, propagating viruses, or excessive network traffic that interferes with the use of others.
E. Responsible for the data and information that they are entrusted with and must not disclose confidential or sensitive information without authorization from the data owner. Confidential data transferred over networks should be encrypted to ensure security.
F. Never attempt to intercept, capture, alter, or interfere in any way with the normal transmission data on any computer or network, without prior authorization from the person or persons responsible for that resource.
G. Observe all applicable policies of external computers or networks when using such resources.
H. Report unauthorized use of computing resources or observed gaps in system or network security to your project director, instructor, supervisor, system administrator, or other appropriate University authority immediately upon discovery. Provide system administrators with information about computing activities when a reasonable request is made.
I. Protect their password so that others cannot gain access to their account.

Application Developer Responsibilities
An application developer is a user who has access to a University computing resource for the purpose of developing software for use on that system or for any other system deemed appropriate and permissible. Application Developers may be employed by the University in this capacity and/or other capacities as well. For the purposes of this security policy, an Application Developer is one who does any of the following:

• Writing program code
• Writing HTML, CGI or other World Wide Web-based content
• Writing SQL code or other user interface-related tasks
• Facilitating data transmission routines
• Any user performing any like functions as part of the regular curriculum or their course of study

Application Developers are additionally bound by all the user responsibilities. They may also be bound by other responsibilities and definitions herein as appropriate to their designated tasks. Application Developers shall:
A. Ensure that applications are written in a method consistent with this and other applicable security policies.
B. Apply data transfer methods that maintain the integrity and security of the data using encryption methods when applicable.
C. Apply security patches and close security holes in applications when they are known.
D. Test applications for common security risks.
E. Document code so that others can maintain it.
F. Document software installations so that others can perform maintenance.

Acceptable Use Policy

Department
1) Do not install any software on the lab machines. If you have a need for additional software see the CESAR technical staff for assistance.

2) Don’t lock the screens on the lab machines for any longer than an hour. If for some reason you feel you need to lock the screen for an extended period of time, please make arrangements with the technical staff.

3) Room SH-324 is a lab/classroom. At times SH-331, SH-337 and SH-339 are used for lecture/labs. The labs and classes have priority during the scheduled time.
4) At this time there is no charge to the students for printing and plotting. Don’t print multiple copies of documents. Please be aware of file types and sizes. Sending images or large files to the printer clogs the queue and wastes a lot of printing resources.

5) Playing games or viewing offensive or obscene material is not an appropriate use of department computers.

6) The Windows C:/ drive is never to be used to store data. Data found on this drive will be deleted immediately. There are Temp workspaces on the computers for local processing. Please move data you wish to keep to your network drive after processing. The Temp areas will be cleaned out regularly without warning.

7) Most of the data are backed up, however the interval differs based on current limitations. If your data needs to be backed up more often it becomes your responsibility. Please check with the technical staff to determine your backup needs.

8) Do not remove any manuals from the lab, and please return them to the shelves when you finish with them.

9) NO FOOD or DRINK is allowed in the lab at any time.

Violations of department computing policies will be reported to the class instructor, principal investigator, and/or committee chair, and may result in the disabling of an account or loss of computing privileges.

**University**

To view the full University Acceptable Use Policy, see [http://security.sdsu.edu/policy/aup-operational.html](http://security.sdsu.edu/policy/aup-operational.html).

In accordance with the University Policy File, section VII-A-9 (also available at [http://security.sdsu.edu/policy/aup.html](http://security.sdsu.edu/policy/aup.html)), the Instructional Technology Committee is charged with developing and reviewing the operational aspects of the Computing Acceptable Use Policy.

The computing and network resources at San Diego State University are intended to support the mission of teaching, research and day-to-day communications related to service to the community. All users of SDSU computing and communications systems, whether directly or indirectly managed by the campus, must respect the rights of other computing and communications users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements.

SDSU Computing users should:

- Keep shared resources, such as network and servers in mind during peak usage times and not unduly overload such resources.
- Use University computing and communications resources only for the University-related activities for which they are assigned, and for incidental personal and/or day-to-day communications related to service to the community. (Note: most assigned computer accounts are not intended to be shared. Consult your system administrator before sharing a password, there may be a better way.)

SDSU Computing users should not:
• Use University computing and communications resources for non-University commercial activities without prior written authorization from the University. If the University grants such authorization, the University may assess appropriate charges to recover the costs of providing such services. This applies to all University-owned and University-leased computers, network resources, and computing and communications facilities related to funded research. Substantial use of computing resources for off campus activities (web sites, mass e-mailings, ...) also requires prior written authorization.

• Post material to electronic bulletin boards, news groups, chat rooms, or mail lists which is illegal, inappropriate or otherwise at variance with accepted codes of network etiquette (e.g., Usenet rules published in news.announce.newusers).

SDSU Policies do not supersede federal or state laws. Actions that are illegal and may result in prosecution include, but are not limited to:

• Violation of applicable federal or state laws and campus regulations, including but not limited to the transmission of threats, harassment, defamation, obscenity, and pornography.

• Copyright infringement. This includes activities such as making software available for copying on your computer and connecting that computer to the SDSU network.

• Making unauthorized copies of computer data or documentation. CA PC 502(c)(2)

• Using a computer system without permission or authorization. CA PC 502(c)(3)

• Adding, deleting, altering or destroying data or software without authorization. CA PC 502(c)(4)

• Disrupting services or causing a denial or service to a computer system or network without authorization. CA PC 502(c)(5)

• Introducing a contaminant into a computer system or network. CA PC 502(c)(6)

Violations of SDSU computing policies may result in the disabling of an access/account and/or loss of computing privileges. A student whose access has been disabled or suspended or revoked may appeal the University's action to a review committee (see Computing Disciplinary Action Appeals Procedures). Additionally, violations may subject the user to disciplinary action under University regulations, and criminal prosecution under applicable statutes. SDSU reserves the right to disable or deny access without notice to halt or prevent suspected violations of computing policies. If you are unsure about the permissibility of any behavior or use, send mail to aup@sdsu.edu to request clarification.

See also: http://security.sdsu.edu/policy/aup.html.