There are several policies that users must adhere to when using the Life Sciences Network. Most are derived from federal and state laws or are implementations of regulations set by the University of California Office of the President (UCOP). The remainder is based on our responsibility to provide a stable, reliable, and secure computing environment for our users.

**UCOP Electronic Communications Policy**

In 2000, UCOP implemented the University of California Electronic Communications policy (ECP). This document forms the basic rules regarding how information technology services (email, web services, etc.) will be provided and managed on UC campuses. It is available online at:

http://www.ucop.edu/ucophome/policies/ec/

**UCSB Policy**

UCSB has its own collection of policies and implementation guidelines. The UCSB policy home page is located at:

http://www.policy.ucsb.edu/

More specific guidelines for implementing the ECP are available in PDF format from:


Finally, the UCSB Office of Information Technology (OIT) web server houses the Campus Network Citizenship document. This details the responsibilities for managing a network connected to the campus backbone.

http://www.oit.ucsb.edu/connect/citizenship.asp

**Departmental Computing Policies**

In addition to the ECP, a few department specific policies have been implemented to provide a stable computing environment or implement UC policy.

**Network Acceptable Use Policy**

The computers and data networks at UCSB are to be used primarily for University business. UCOP policy specifies other sorts of "allowable use". To summarize the
document, computing and network resources may be used for non-business purposes with a few restrictions. This document addresses some of the more common issues, but is not an exhaustive list. If you have questions about the ECP, please contact computer-support@lifesci.ucsb.edu.

• **Interference with University Business**

  Network bandwidth is a finite quantity and is expensive to increase. There were several instances in 2001, in which a single computer succeeded it using all of the network bandwidth in a major building. This interrupted mission-critical services such as file sharing and email access for everyone within the building.

  Further, the sending of unsolicited bulk email (spam), forwarding of chain-letter email, or participating in denial-of-service attacks is not permitted.

• **Digital Millennium Copyright Act (DMCA)**

  The DMCA was passed by the U.S. Congress in 1998 in response to arguments that networked computers were making it too easy to exchange unlicensed copies of copyrighted material and that existing law needed to be revised. Among its many provisions is a section that allows service providers to be held liable for the copyright infringements of their subscribers unless the providers follow certain rules when notified of infringement. The University of California agreed to these "safe harbor" provisions.

• **Peer-to-Peer and Distributed Computing**

  The University network is a finite resource intended to support University business and to support the University's mission. While incidental, personal use is allowed under existing policies, certain types of applications consume more network resources. These typically fall into one of two categories; peer-to-peer or distributed computing.

  Peer-to-peer (P2P) applications are those in which every computer acts as both a client and server. Some examples of peer-to-peer applications are Morpheus, Gnutella, and FreeNet. Distributed applications are similar. These applications typically use computers with fast network connections as “reflectors” to reduce bandwidth usage elsewhere. A few examples of distributed applications are BitTorrent, Abacast, and Skype. Commercial businesses may take advantage of P2P and distributed computing technologies and use client computers as part of their business plan to lower distribution costs. The commercial use of UC resources for profit is prohibited.

  Unless these types of applications are within UC guidelines and being used in support of University business, they are not allowed on the Life Sciences Network. When a computer is found to be running such software, its traffic is filtered at the departments’ router, effectively cutting it off from the internet. The filter will remain in place until the software is uninstalled, any unlicensed content removed, and that compliance has been verified by technical support staff. Any
work done by technical support staff to bring a computer back into compliance with policy will be on a recharge basis.

- **Unlawful Activities**

  Use of computers or the Life Sciences network in a fashion that violates federal, state or local law is also a violation of UCOP policy.

- **False Identities and Anonymity**

  It is a violation of UCOP policy to impersonate another person with the exception of an employee using a supervisor's identity at their direction. It is allowable to use a pseudonym so long as it is clearly not an attempt to impersonate someone. A user of University electronic communications resources may remain anonymous (the sender's name or electronic identification are hidden) except when publishing web pages and transmitting broadcasts.

- **Other Violations of Policy**

  Other UC policies (such as those involving harassment, intellectual property, and commercial activities) also apply to the use of the Life Sciences Network. The UCOP website contains information regarding other policy issues at:

  http://www.ucop.edu/ucophome/coordrev/ucpolicies/

**Network Security Policy**

Of primary importance to the Departments is the provision of a reasonably secure computing environment while maintaining flexibility enabling people to get their work done. In accordance with that goal, there are a few requirements imposed on computers attached to our networks. This includes installing anti-virus software, securing the default configuration, and creating accounts allowing technical support access to the computer. A full explanation of those requirements is available at:

  http://www.lifesci.ucsb.edu/compsup/policy/policy.php
  
  http://www.lifesci.ucsb.edu/compsup/policy/network_config

The more general guidelines are discussed below. If you have a question about a potential service, please contact computer-support@lifesci.ucsb.edu.

- **Passwords**

  Passwords are issued to allow users access to various department services. These passwords should not be shared with anyone. As departments become aware that a password has been shared, the password will be changed. Repeated violations can lead to suspension of network account access.

  It is strongly recommended that any service that allows read-only access to confidential information be password protected. It is required that all read/write services which may be used to change operating system files from a remote
location (file shares, FTP servers, Unix command shells, etc.) be password protected. Identification of unprotected read/write services can lead to temporary disconnection of network service.

Furthermore, technical support strongly recommends that encryption be used, whenever possible, to protect the integrity of user passwords.

- **Anti-virus Software**

  The Departments coordinate a volume purchase of anti-virus software. The purchase is large enough to provide anti-virus software for every computer owned by the organizations and provide a home-use license for our faculty, staff, and graduate students. The current versions are capable of automatically updating virus definitions. Technical support requires running anti-virus software on all desktop computers attached to the Life Sciences Network. The software should be configured for automatic, daily updates.

- **Operating System Patches**

  Every operating system currently available contains software flaws. In some cases, these flaws create conditions where a malicious piece of software on a remote system can be used to take control of the local computer. Software vendors release patches for these vulnerabilities as they become known. Most desktop operating systems (Windows 98, Windows ME, Windows 2000, Windows XP, and MacOS 10.x ) provide mechanisms to automatically check for and install patches. These patch automation tools should be enabled whenever possible.

- **Unused Services**

  Most operating systems are capable of providing a variety of network services including web servers, mail servers, file sharing, and remote printing. Each active network service creates another possible route for an intruder to compromise the local computer. The best way to avoid this is to shut down any unneeded services.

  For example, Lifesci can be used to serve personal web pages and is departmentally supported. This generally removes the need to run web and FTP server software on other computers in the departments. The Code Red worm in 2000 exploited the fact that millions of Windows systems were running unpatched web servers. In most cases, the web servers were not needed and could have been disabled.

- **Mail Servers and Unsolicited E-Mail (Spam)**

  One of the largest problems facing campus is unsolicited, bulk email (UBE). In the past, email servers connected to the internet would forward messages regardless of sender or recipient. This redundancy was intentional in order to accommodate localized outages. However, bulk mailers generally exploit these "open mail relays" in order to hide their actual location and to increase their speed of distribution. UCSB policy prohibits open mail relays.
In order to avoid large problems with misconfiguration, the only mail servers generally allowed on the Life Sciences Network are those supported by Biology, Core, Psychology, or organizations with dedicated IT staff.

- **Packet Sniffers, Cracking Tools, and "Spyware"**
  
  Any attempt to circumvent access controls on computers on or off campus is a violation of UCOP policy and federal law. The use of a computer with the goal of gaining unauthorized access to information can lead to University disciplinary action or arrest.

- **System Logs**
  
  Technical support maintains a system that collects Unix system logs in a single location. This allows the detection of hostile probes of the Life Sciences Network. It also provides a repository of system logs in case a computer is compromised and the local copy of systems logs is altered. All Unix-based computers, including MacOS 10, should have a subset of system logs sent to this logging system. For more information, please contact computer-support@lifesci.ucsb.edu.

- **Network Address Translation**
  
  In order to maintain a stable, secure network, campus IT personnel must be able to identify the source of any network traffic in the event of network problems or a security incident. Network address translation (NAT) and any other technology that masks the source address of network traffic is not permitted on the Life Sciences Network.

- **Wireless Networks**
  
  Due to security, configuration, and interference issues, wireless networks are not supported on the Life Sciences Network. If you believe you need a wireless network to meet a specific academic or research goal, please contact computer-support@lifesci.ucsb.edu.

---

**Electronic Privacy Policy**

The University of California has very strict guidelines regarding the distribution of personal information. State law requires that we make available contact information for all employees, with the exception of student employees. All non-student employees are listed on the various staff and faculty web pages and such information is available to the public.

Contact information for graduate students is handled differently; there are two levels of access for information regarding graduate students. All graduate students will have their name and photograph made available on a directory which is only available to computers physically located within biology buildings. This is to facilitate communication within the department. There is a second, public directory. Graduate students may opt not to
have contact information contained in the public directory.

More generally, students (both undergraduate and graduate) must agree before their name or photograph is displayed to the public on any university owned server. This includes laboratory or personal web pages as well as those maintained by the departments.