Bittner Research Group
Policy and Procedures
Usage of Research Group Computers and Services
November 25, 2005

1 Policy

To better serve the members of our group and to provide our group with the best tools to do their research, the Bittner Research Group (the Group) and the University of Houston makes available to our research community access to one or more forms of electronic media and services.

This policy refers to all information resources, whether controlled or shared, stand alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or contracted by the Bittner Research Group. This includes word processing equipment, personal computers, workstations, laptop computers, e-mail, telephones, voicemail, fax machines, online services, Internet, and associated peripherals and software, regardless of whether used for administration, research, teaching, or any other purpose.

The University of Houston encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information about members and attendees, vendors, technology, and new products and services. However, all employees and everyone connected with the organization should remember that electronic media and services provided by the group are property of the University of Houston and the State of Texas and their purpose is to facilitate and support group research and business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

To ensure that all users of these services are responsible, the following guidelines have been established for using e-mail and the Internet. No single policy can lay down rules to cover every possible situation. Instead, it is designed to express our group's philosophy and set forth general principles when using electronic media and services.

These policy statements are in addition to any standing policy of the University of Houston and we defer to the University's policy where these are in conflict.

2 Access

The computers, electronic media and services provided by the group are primarily for research use to assist group members in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, nonbusiness/nonresearch purposes by group members is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their research/business purposes. However, group

members are expected to demonstrate a sense of responsibility and not abuse this privilege.

Access to the information resource infrastructure within and beyond the UH campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at UH is a privilege and must be treated as such by all users of the system.

The UH IT or the group itself may gather logs for most electronic activities or monitor employee communications directly, e.g. telephone numbers dialed, sites accessed, call length, and time at which calls are made, for the following purposes:

- Resource allocation;
- Optimum technical management of information resources; and
- Detecting patterns of use that indicate employees, volunteers, or others are violating university policies or engaging in illegal activity.

We reserves the right, at its discretion, to review any users electronic files and messages stored on or sent from church computers and servers to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other university policies.

Anyone who accesses, uses, deletes, destroys, or alters any group information, resources, properties, or facilities without authorization, may be guilty of violating the privacy of others, of injuring or misappropriating the work produced and records maintained by others, and threatening the integrity of information kept within these systems. Purposely doing so is unethical and unacceptable.

3 Procedure

1. Research group members are encouraged to use computers and the Internet to accomplish job responsibilities more effectively.
2. We reserves the right to screen computers to determine business appropriate usage at any time.
3. All assigned computers are to be pass coded with secure and non-obvious passwords. Each computer will be locked down at the close of business each day. The server system area will be secured when not in use.
4. All computers will have protective environment software installed. All remote access is to be through secure shell (SSH or SFTP). Attempting to override protective software is prohibited.
5. Use of the Internet is a privilege, not a right, and may be revoked at any time for inappropriate conduct. Inappropriate or illegal use of the Internet may also result in disciplinary or legal action.

6. Vandalism will result in immediate cancellation of user privileges and will require restitution. Vandalism is defined as any deliberate attempt to harm or destroy data of another user, including (but not limited to) uploading or creation of a computer virus.
7. Violations may result in revocation of Internet privileges and any other applicable disciplinary action.
8. All group members must adhere to confidentiality and release of information policies when communicating on the Internet.
9. Group members must be aware that electronic mail is not private communication. Care must be taken to protect confidential information.
10. Any files downloaded from the Internet must be scanned for viruses.
11. In the event that an inadvertent infraction occurs, the System Administrator and/or PI is to be notified immediately.
12. All users must conform to the legal restrictions, standards of conduct, and specific rules of etiquette when accessing the Internet.

4 Prohibited Communication

Electronic media cannot be used for knowingly transmitting, retrieving or storing any communications that is considered inappropriate. Inappropriate conduct includes (but not limited to) the following:

- Use of the Internet for unlawful activities
- Use of the Internet for commercial activities not related to the organization
- Activities that interfere with the ability of others to make effective use of the network
- Violation of copyright, trademarks and licensing programs, or license governing the use of software
- Intentionally accessing or downloading any text, picture (including video), graphic, or sound clip, or engage in any conference that includes material that is obscene, sexually explicit or pornographic, libelous, indecent, vulgar, profane, lewd, derogatory to any individual or group, or which advertises any product or service not permitted to minors by law.
- Use of inappropriate language or language that is discriminatory or harassing, vulgar, profane, lewd, derogatory to any individual or group, or defamatory or threatening
- Sending of messages which include insulting or aggressive language, or expressions which are designed, intended, or likely to injure or harass others
- Sending of personal information about yourself or others
- Engaging in social Chat Rooms

- Engaged in for any purpose that is illegal or contrary to UH policy or research/business interests.

5 Software

To prevent computer viruses from being transmitted through the church's computer system, unauthorized downloading of any unauthorized software to church computers or servers is strictly prohibited. Only software registered through UH may be downloaded. Employees and volunteers should contact the system administrator if they have any questions

6 Security/Appropriate Use

Employees and volunteers must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by church management, employees and volunteers are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other group members or third parties;
- Hacking or obtaining access to systems or accounts they are not authorized to use;
- Using other people's log-ins or passwords; and
- Breaching, testing, or monitoring computer or network security measures.

One person (other than the PI) in our group will have the responsibility of being the group System Administrator. This person, preferably a senior member of the group or post-doctoral fellow, will have the additional responsibility of overseeing the "health and well-being" of our group computer resources. This person is also charged with educating less experienced members in the Unix computing environment and eventually training a replacement. SysAdmin knowledge is best shared amongst multiple group members. Administrative privilege carries the responsibility of knowing what to do and what not to do. If you have SysAdmin privileges and you do not know what to do, find some one with more experience (such as a senior group member or the PI).

All root level access to a given computer is to be done at the computer itself. Users may use "sudo" when logged in remotely (via ssh) through a normal user account.

You are not at any time to write down your password.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

WiFi access is allowed via the group's WiFi hubs. These are to be setup and maintained in accordance with the UH IT's policy regarding these hubs. Access will be password protected and SysAdmin level passwords will written down and stored in a secure location.

7 Encryption

Group members can use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Group members who use encryption on files stored on a group computer must provide the PI with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files

8 Participation in Online Forums

Users should remember that any messages or information sent on church-provided facilities to one or more individuals via an electronic network – for example, Internet mailing lists, bulletin boards, and online services – are statements identifiable and attributable to UH

We recognize that participation in some forums might be important to the performance of an group member's research and job. For instance, you might find the answer to a technical problem by consulting members of a news group devoted to the technical area.

9 Backups and Archives

Most of our group computers have a second high capacity hard-drive either internal or external. These are for weekly backups of any important data and files. Backups are to be performed weekly at the very least and one should keep a 3-4 week running archive. By and large, this is accomplished via a shell-script which is automatically executed by the computer on a weekly basis. Other backup software may be used, however, we have found the simple shell command to be the most reliable. If you computer does not automatically back itself up, please ask the SysAdmin to set this up for you.

Archival and important data should be burned on to CD or DVD disks. This is especially important

for long simulation data, and data pertaining to publications. All group members should prepare a set of DVDs or CDs of all their user files before leaving the group.

Electronic versions of papers (especially figures) should be uploaded to a common archive. This provides a secure backup of your paper and it allows others (especially the PI) to use your figures in other publications and presentations.

The group maintains a CVS server (eiger.chem.uh.edu). All production versions of group software along with input files and sample output should be archived here. This is important since you may need to be able to reproduce a figure or set of data at some future date. Also, we may want to release your code to other users.

All codes release to the public domain are to be release under the GNU Public License. This must first be done in accordance with UH policies regarding Intellectual Property.

10 Violations

Any user of group computers or services who abuses the privilege of their access in violation of this policy will be subject to corrective action, including possible termination of employment, expulsion from the University, legal action, and criminal liability.

11 Miscellaneous

Usage of group computers or services automatically implies acceptance of this policy.

This policy is subject to change at any time. In the event of change, the group will use all reasonable means, including email lists and web sites, to communicate these changes to our users.