State University of New York

Upstate Medical University

Academic Computing

Student Computing Policies

College of Medicine College of Health Professions College of Nursing College of Graduate Studies

Table of Contents

Introduction

SUNY Upstate Medical University information is a critical asset, therefore it must always be protected from unauthorized modification, destruction, and disclosure. The Information Security department of IMT, is responsible for providing a secure technology infrastructure to protect the confidentiality, integrity, and availability of information on SUNY Upstate systems. To ensure our systems are properly secure, it is our department's responsibility to communicate the importance of security to protect our information.

As a student with access to SUNY ResNet you will have the opportunity to connect your personal computer to the Upstate Medical University high speed data network. As part of being granted access to the ResNet, it is your responsibility to become familiar with Upstate's security policies and procedures to protect our information and to be aware of the security threats and vulnerabilities associated with access to our information.

This policy guide has been developed to document the information security policies as well as the various ways to secure and protect information you will have access to throughout your studies at Upstate.

ResNet Access

1. Support

Academic Computing will provide support in purchasing and installing Network Interface Cards and connecting your computer to the network. Support will only be provided if your computer meets the minimum system requirements. While every reasonable effort will be made to connect your computer to ResNet, correcting any problems with the operation of the computer related to the hardware, network interface card, system software, or application software is the ultimate responsibility of the owner. Application (how to use software) or system (problems with your computer) support will not be available.

2. Limitations

ResNet connections are primarily intended to be used for academic, educational, and professional uses. It is understood that Clark Tower is your home and limited personal use of the Internet is permitted. Keep in mind that you are behind the University Firewall and certain applications such as web-cams, Internet telephones, messenger programs, and file-sharing may not function correctly. Students are not permitted to host a web or file server using their ResNet connections.

3. Personal Networking Equipment

Unauthorized networking equipment (including but not limited to switches, routers, and wireless access points) are not to be installed for any reason without the express written permission of the Manager of Academic Computing. These devices can expose the University network to unauthorized use, intrusion, and monitoring and could potentially expose protected information to the Internet. Violation of this rule will result in the immediate termination of your connection followed by a review from Academic Computing, IMT, and Residence Life.

4. ResNet Virus Protection

SUNY Upstate policy requires antivirus software for all computers connecting to the Upstate network. All Clark Tower residents must install and run Antivirus software on their personal computers in order to connect to the Upstate Network. Academic Computing recommends and supports McAfee virus protection for the PC and Virex for the Macintosh. Both of these applications are provided free of charge to Upstate students. McAfee provides automatic updating to the most current virus definitions.

Students are also permitted to use Norton Antivirus as long as the student has a current up-to-date subscription and keeps the virus definitions up-to-date. Norton Antivirus will not be supported by IMT. No other virus protection software is permitted. Students must uninstall all other antivirus software and install either McAfee (provided by Academic Computing) or purchase and install Norton.

5. Antivirus Information Web site

Students must visit the Antivirus Information for Clark Tower Residents Website located at: http://www.upstate.edu/academic/virus/ before accessing any other Internet resources using the Upstate Network. This website contains antivirus software and installation instructions. All Clark Tower residents must then fill out the form acknowledging that the software has been installed. If it is discovered that student has not installed antivirus software, their ResNet connection will be terminated.

6. Spyware

Academic Computing is also providing SpyBot software to help students combat spyware that is running on their computer. This software is also available on the above website. It is recommended that all students install and run SpyBot.

ResNet Appropriate Use

1. Copyrighted Material

The sharing, hosting, or transfer of copyrighted files or materials on the Upstate network will not be permitted, except by the owner of the copyright. Students in the past have been caught violating this policy. While IMT has no desire to act as “data police”, we must act when notified that illegal activity is occurring on the Upstate network. Please review the General Policy Statements on pages 5-8. Page 6 deals with unacceptable misuse of computers and network systems with subsection (i) dealing with copyright violations. All ResNet users are expected to familiarize themselves immediately with this policy. Subsequent use of the Upstate computer network will be taken as an indication that you have read, understood, and agree to follow this policy.

2. Peer-to-Peer Use

In recent years there seems to have been an increasing trend of ResNet users more peer-to-peer applications, such as Bit Torrent, Gnutella, FastTrack, and others for peer-to-peer file sharing. While most of these programs can be used for legitimate purposes, we have found these programs have been used to share copyrighted materials like music, movies and books.

These applications are capable of using a significant amount of Internet bandwidth, and it can make it impossible for other Upstate faculty, staff, and students to get e-mail or do academic work over the network. Most of these programs are known to use bandwidth regardless of whether you are using the computer program or not. This means that just having the program loaded on the machine whether open (or minimized in the system tray like many are) they will allow others in the world to use your bandwidth.

3. Enforcement

At the receipt and/or notification that an individual is using inappropriate software to download or upload copyrighted material without the owner’s permission OR Upstate’s IMT department identifies a significant amount of bandwidth use for a particular student, the following actions will occur:

1. Students will immediately have their ResNet connection deactivated for an indeterminate period of time.
2. Students will be referred to Student Affairs for disciplinary review.
3. If requested, Upstate will forward information on the copyright violation to the owner of the copyright.

GENERAL POLICY STATEMENTS

1. Acceptable Use

SUNY Upstate computers and information systems are shared resources, essential to the instruction, research, and/or administrative functions of the University. The use of these resources is governed by federal and state laws, as well as SUNY Upstate policies and procedures.

Those who use SUNY Upstate computers and information systems are expected to do so responsibly. The continued use and availability of these systems requires that they be legitimately used and treated with care and good sense. Accordingly all users should exercise reasonable care when using any SUNY Upstate computer or information system.

a. All students must act honestly and responsibly. Every student is responsible for maintaining the integrity of these information resources.
b. All students must use and access information only as appropriate in connection with assigned work, study, or clinical-related duties and responsibilities.
c. All students must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements related to SUNY Upstate information systems.

d. All students shall act in accordance with these responsibilities, and the relevant local, state and federal laws and regulations, as well as SUNY Upstate policies and procedures.
e. Failure to comply may result in denial of access to SUNY Upstate Information Systems and/or disciplinary action in accordance with Student Academic Policy Handbook.

Use of any SUNY Upstate Medical University's computer or information system shall constitute an acknowledgement on behalf of the student accessing such systems to abide and be bound by the provisions of this Policy.

The use of any Upstate Medical University computer and information systems should be related to university business, including academic pursuits in support of the teaching, research, and patient care components of SUNY Upstate's mission, and the administrative functions that support this mission.

2. Inappropriate Use

Inappropriate use of SUNY Upstate information systems is prohibited. This includes the following.

a. Logon - Circumventing logon or other security measures.
b. Sharing User Accounts and/or Passwords – Sharing your account and/or password with other students or allowing use of your account by others. This includes family and other household members when work is being done at home.
c. Viruses/malicious software – Introducing or propagation of malicious programs or viruses into the SUNY Upstate network (e.g., viruses, worms, Trojan horses, email bombs, etc.).
d. Illegal or Unauthorized Purpose - Using information systems for any illegal or unauthorized purpose.
e. Personal Use for Personal Gain - Personal use of information systems or electronic communications for non-University consulting, business, or employment.
f. Fraud - Sending any fraudulent electronic communication.
g. Harassment - Using electronic communications to harass or threaten students or other users in such a way as to create an atmosphere which unreasonably interferes with the education experience. Similarly electronic communications shall not be used to harass or threaten other information recipients, in addition to SUNY Upstate users.
h. Disclosure of Proprietary Information - Using electronic communications to disclose proprietary information without the explicit permission of the owner.
i. Disclosure of Protected Health Information - Using electronic communications to disclose Protected Health Information without consent from the patient.
j. Misusing University Records - Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards, or other documents or property).
k. Abuse of University Resources - Using electronic communications to hoard, damage, or otherwise interfere with academic resources available electronically.

l. Inappropriate Use of Bandwidth - Bandwidth both within campus and connecting to the Internet is a shared, finite resource. SUNY Upstate users must make reasonable efforts to use this resource in ways that do not negatively affect others.

m. Theft - Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work.

n. Violation of Law - Violating any state or federal law or regulation in connection with use of any information system.

o. Unauthorized Infrastructure Changes - Changing wiring, connections, or placement of computing resources is prohibited.

p. Impersonation and Anonymity/Falsifying E-mail (see Electronic Mail) – Any attempt to falsify the source of an e-mail message (i.e., make a message appear to come from someone who did not send it) and/or intentionally violate the provisions set forth in the SUNY Upstate Medical University Electronic Mail Policy.

q. Hacking - Attempting to obtain unauthorized access to computer accounts, software, files, or any other SUNY Upstate IT resources. Attempts to browse, copy, or modify files or passwords or attempts to discover passwords belonging to other people organizations, whether at SUNY Upstate Medical University or elsewhere.

r. Copyrights and License Agreements – Using electronic communications to violate the property rights of authors and copyright owners. Willfully violating the terms and conditions of software licensing agreements signed by SUNY Upstate.

s. Software Licensing – Downloading and installing software that is not licensed to SUNY Upstate Medical University, that is in violation of software license agreements of the vendor. IMT should be consulted prior to downloading and installation of any software on SUNY Upstate computer systems.

t. Commercial, Political, and/or Non-University Activities - Use of SUNY Upstate computers and information systems to sell or solicit sales for any goods, services, or contributions unless such use conforms to University rules and regulations governing the use of University resources. No one may use SUNY Upstate computers and information systems to represent the interests of any non-University group or organization unless authorized by an appropriate SUNY Upstate department.

u. Other Activities not specifically cited above that may be illegal, harmful, destructive, damaging, or inappropriate use of SUNY Upstate computers and information systems as determined by the Chief Information Officer (CIO) is also prohibited.

3. Privacy

Students should be aware that SUNY Upstate cannot and does not guarantee user privacy. In addition to the threat of malicious users finding ways to access your files, IMT may monitor account activity of any student to ensure compliance with this policy and/or to carry out State operations, and users should be continuously aware of this fact.

Students should be aware that on occasion, IMT personnel have authority to access individual student files or data in the process of performing repair or maintenance of computing equipment SUNY Upstate deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for SUNY Upstate needs.

Response to a Public Records Request, Administrative, or Judicial Order or Request for Discovery in the Course of Litigation – Students should be aware that certain records, such as unpublished research in progress, proprietary information, personal information in personnel and student records are protected from disclosure. However, most other SUNY Upstate records contained in electronic form require disclosure if a public record request is made. Students should remember this when creating any electronic information, especially e-mail.

Students should also be aware that SUNY Upstate will comply with any lawful administrative or judicial order requiring the production of electronic files or data stored in SUNY Upstate's computers and information systems. SUNY Upstate will provide information in electronic files or data stored on SUNY Upstate's computers or information systems in response to legitimate requests for discovery of evidence in litigation where SUNY Upstate is involved.

4. Ethics

While Upstate Medical University aspires to provide the highest quality IT environment, during peak periods, the demand for IT resources may exceed the supply of workstations or computer connections. Responsible computing demands that one be sensitive to the needs of all who seek to use such resources and that during such peak periods, one must limit one's use of computing technology to performing only the most essential tasks. Consideration for others should also be a priority when one is using limited resources, such as central computer disk space, dial-up phone lines, network bandwidth, tape drives, printer capacity, etc. Users of open student labs and user facilities must comply with the posted and published policies with regard to time limits, conduct, etc.

Within the broad context of free academic discussion and debate, communications between members of the SUNY Upstate community are expected to reflect high ethical standards and mutual respect and civility. It makes no difference whether the communications medium is a face-to-face exchange, or via a local or national computer network. Vulgar, racist/sexist, harassing, or threatening language or actions, for example, clearly violate ethical standards, and are as inappropriate for computer-mediated communications as for other forms of University discourse.

USER ACCOUNTS AND PASSWORDS

Your user ID is your identification, and it’s what links you to your actions on each SUNY Upstate system. Your password authenticates your user ID. Protect your user ID and password. Remember, you are responsible for all actions taken with your user ID and password. The following best practices should be followed:

1. Your password should be changed periodically, even if your system does not force you.
2. Don’t reuse previous passwords.
3. Memorize your password, don't write it down or post it somewhere

4. Don't use passwords that can be easily guessed such as family or pet names, user IDs, birthdays, or words that can be found in the dictionary.
5. NEVER tell or share your password with ANYONE.
6. When your computer prompts you to save your password, click on “No.”
7. If you think your password has been compromised, CHANGE it immediately. Immediately notify the Information Security Coordinator if this occurs.
8. Make passwords as long as possible – eight or more characters. Create a password that’s hard to guess, but easy for you to remember. When possible, use a mix of numbers and letters, special characters, or use only the consonants of a word. If you have difficulty in creating a password, try using the first letter of each word in a phrase, song, quote, or sentence. For example, **My favorite Car is a 79 Corvette!** becomes MfCia79C!

ELECTRONIC MAIL USE

1. Individual Expectations

Those students who access and use SUNY Upstate Medical University electronic mail services are expected to do so responsibly. Accordingly, all students should observe all laws relating to copyright, trademark, trade secrets protection, as well as following the normal standards of professional and personal courtesy and conduct when using email services.

Users of SUNY Upstate Medical University electronic mail services should expect all electronic mail messages shall be delivered to the addressees, and would not be accessed or intercepted except as provided by this policy. Students should also be aware that any email communications sent might be forwarded to other individuals or third parties.

2. Permissible Use

The use of any Upstate Medical University communication resources should be related to university business, including academic pursuits in support of the teaching, research, and patient care components of Upstate’s mission, and the administrative functions that support this mission.

University electronic mail services may be used for incidental and occasional personal use of electronic mail, providing that use is not excessive or illegal; does not interfere with university operation of computing facilities or electronic mail services; does not violate the conditions set forth in this policy or other SUNY Upstate Medical University sanctioned policies; or does not burden the university with incremental costs.

3. Prohibited Use

Prohibited use, includes but is not limited to the following:

General Restrictions:

Electronic mail services shall not be used for:

- Any purpose in violation of any law, regulation, or policy;
- Sending copies of documents or the inclusion of the work of others in violation of copyright laws;
- Personal monetary gain or for commercial purposes that are not directly related to university business;
- Personal use inconsistent with this policy;
- Uses that violate other University or campus policies or guidelines, including harassment, intimidating others, or interfering with the ability of others to conduct university business; and
- Adding an individual to an email mailing list for other than official university business. Mailing lists may be used only for their intended purposes.

False Identity:

All materials sent by campus email must identify the individual, office, or organization sending the material. It is a violation of this policy to originate email in such a manner as to create the impression to the recipient that the mail was originated from another source or individual.

Interference:

Electronic mail services shall not be used for purposes that could cause excessive strain on email systems or facilities, or unwarranted or unsolicited interference with others' use of electronic mail services. As such, users of electronic mail services shall not: (i) send or forward electronic mail chain letters or their equivalents; (ii) exploit or distribute unsolicited electronic mail communications (e.g. spam); or (iii) send an extremely large message or send multiple communications that may interfere with the recipients' use of electronic mail system and services.

Unauthorized access:

Users of electronic mail services shall not attempt to access the electronic mail of others for any purpose without proper authorization or in emergency situations. Access to another individual's account should be performed through the proxy function in the email services application.

4. Privacy and Confidentiality

Due to the nature and technology of electronic communication, the university can assure neither the privacy of an individual user's use of the university's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored. Since all electronic mail systems, addresses, account information, and services are the property of Upstate Medical University, there should be no expectation of privacy or confidentiality for documents and messages stored on university-owned equipment.

5. Patient Information

Email users must be aware of the inherent risks associated with sending email with patient health information (PHI). In cases where a patient care or operational need arises that requires PHI to be sent in email, only the minimal amount of PHI should be included to convey the message and the message should be sent to the appropriate parties. The minimum amount of information may include any of the following: patient name, medical record number, patient account number, or date of birth.

If it is necessary to send external email outside SUNY Upstate (ie. non-Groupwise user or an email address that is not <username>@UPSTATE.EDU) with patient information, the transmission of a patient's protected health information (PHI) must be limited to circumstances in which the information is required to provide treatment, for payment purposes, or to conduct healthcare operations. Whenever feasible, all external email containing confidential information should be secured prior to being sent, through use of password protected documents and attachments.

VIRUS PROTECTION

1. General Virus Information

Viruses or malicious code such as worms or Trojans can cause significant disruption to Upstate computing resources. They can hide behind an infected web page or disguise themselves in downloadable games, screen savers, executable programs, or email attachments. **Computer viruses** are programs that spread or self-replicate. They usually require interaction from someone to be activated. Viruses may arrive in email messages, through attachments, opening emails, or going to a malicious web site. If a virus infects a computer, all the information of the hard drive may be lost or compromised. Also, a virus on a PC may easily spread to other machines on the Upstate network. All Upstate computer systems have virus protection installed to protect the network from these harmful programs. **Worms** are similar to viruses because they self-replicate, however they do not require any user interaction to be activated. Worms spread because of vulnerabilities or holes in software. **Trojans** are malicious codes hidden in a legitimate program that when executed performs some unauthorized activity or function. It is IMT's responsibility to protect the Upstate network from these programs by keeping all computers and systems patched and updated.

2. Virus Scanning and Updating

To assure continued availability of a computer, the anti-virus software must periodically scan all system and data files on a computer. All anti-virus software installed by IMT will be set to periodically update and scan for viruses on a regular basis. All students must not bypass, disable, or remove the anti-virus software programs, since this could result in the propagation or transmission of computer virus or malicious software program.

3. Virus Infection

If a student suspects an infection by a computer virus, they should stop using the suspected computer immediately and contact the IMT Help Desk. Symptoms of virus infection include slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of personal computers.

The IMT department is responsible for the removal of viruses/malicious software from infected computers, and verifying sources of all infections. IMT reserves the right to disconnect any computer that has been infected with a virus until such a time that IMT can remove the virus from the computer.

4. Virus Eradication

If it is determined a computer has been infected with a virus or other malicious program, users must not attempt to eradicate viruses themselves. The IMT department is responsible for completing this task in a manner that minimizes both data destruction and system downtime.

USB drives CDs, and other magnetic storage media used with an infected computer must not be used with any other computer on the Upstate network, until eradicated by the IMT department.

5. Virus Guidelines

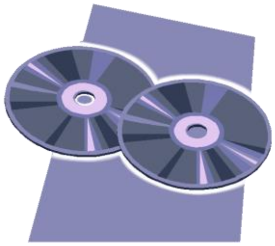
In addition, the following tips will help you to guard against the spread of computer viruses, worms and Trojans in the Upstate network:

1. Do not open any unrecognized emails or attachments. If you receive any unrecognizable or suspicious email, report it immediately to the IMT Help Desk or the Information Security Coordinator.
2. Do not download any games, screen savers, or executable programs.
3. Be aware of any suspicious activity, such as unfamiliar programs appearing on your computer, and contact the IMT Help Desk.
4. Use the virus protection software to scan attachments and other files opened on a computer.
5. Do not disable or remove the virus protection on Upstate computers.

WORKSTATION SECURITY

While protecting information encompasses use of user accounts and passwords, there are also physical components to protecting access using the Upstate computer lab facilities. Proper safeguarding of the physical access and security of computer is one of these most important ways of protecting Upstate information. You are responsible for maintaining the security of information accessed in computer labs under your control and for protecting the confidentiality of the data stored or accessed.

1. Ensure patient and other sensitive information is properly protected is accessing information in computer lab facilities by keeping computer screens tilted away from public areas to protect information.
2. Log off when you leave the computer, otherwise this individual using the computer next will have access to your information.
3. It is important that you DO NOT save any important personal work to public lab computers. All changes to these computers will be permanently overwritten when computers are restarted. It is recommended that all personal work be saved to a USB flash drive or emailed to your Groupwise email account.



PORTABLE AND MEDIA DEVICES

Upstate information is now accessible remotely and can be taken outside the Institution through a variety of means. Laptops, Blackberries, PDAs, and Cell Phones are just some of the portable devices in use. USB drives, CD/DVDs, and external storage mediums are other technologies that could be used to work at home, or when traveling. Some good practices related to security of these devices:

1. Take responsible steps to prevent the loss or theft of the device – you should always remain in the possession of the device in any public places.
2. Be aware of your surroundings when using devices in public areas to avoid the risk of unauthorized persons viewing information
3. Protect our information by not leaving devices out in the open. Place them in a secured and locked office, desk, or filing cabinet.
4. Always use a password to unlock or login to laptops, USB Jump drives, and smart phones.
5. Passwords should be set to lock the device after five minutes of inactivity. The lockout mechanism must require re-entry of the password to obtain access to the device.
6. Always ensure a copy of the data is kept at Upstate. If a portable device is lost or stolen, this will save a lot of time and resources in trying to re-create the information.
7. Encryption of information on the devices is recommended. Software is available from various vendors for encrypting information on these devices.

WIRELESS NETWORK ACCESS

Students must possess an Upstate ID Badge in order to connect their personal computing device to the wireless network. Your wireless account is only permitted to be used on the device that was originally configured by Academic Computing. Wireless access is not transferable to another device without prior approval from Academic Computing.

1. Limitations of the Wireless Network

Users of the wireless network need to be aware that a standard wireless account only allows for limited network connectivity. The standard wireless network is designed to allow a user access primarily to the public Internet. For security reasons, many Upstate internal network resources may be unavailable on the wireless network. If you find a network resource that you are unable to access that you feel should be available, please contact Academic Computing at 464-4860.

2. Wireless Network Use

Wireless network connections are primarily intended to be used for academic, educational, and professional use. Limited personal use of the Internet is permitted. Users of the wireless network must read, understand, and comply with the GENERAL POLICY STATEMENTS regarding appropriate and acceptable use in this manual.

Under no circumstances shall a user operate a file sharing application (such as, but not limited to, Kazaa, Morpheous, or Limewire) to transmit copyrighted material on the wireless network. Violation of this policy will result in immediate suspension of your wireless account. Please be aware that your computer's hardware address will be recorded and associated with your account. This information will allow us to contact you in the event that your computer is adversely affecting the wireless network.

ENFORCEMENT

SUNY Upstate considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information resident on SUNY Upstate systems that may be related to inappropriate use. The Chief Information Officer also reserves the right to authorize disconnecting a user's account if the user represents a serious threat to information systems. Violators are subject to disciplinary action as prescribed in the student handbook.

1. Violations Reporting

Suspected violations of this policy should be reported to the Information Security Coordinator, via an e-mail message addressed to: helpdesk@upstate.edu or by calling 4-4115. In reporting a violation, complainants need to forward all evidence of such violation and cite the specific section of this policy that has been violated. The complaint will be processed in the following way:

(1) Details of the incident will be forwarded to the Student Affairs;
(2) Any student contact will be made by the Student Affairs or by the department of Public Safety; and
(3) All necessary and appropriate action will be taken to address any policy violations.

2. Access Restrictions

SUNY Upstate may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of SUNY Upstate policies, state, or federal laws.

When it has been determined that there has been a violation, SUNY Upstate may restrict or prohibit access by an offending party to SUNY Upstate owned computers and information systems, remove or limit access to information on SUNY Upstate-owned computers or information systems, and, if warranted, institute other disciplinary action, in accordance with student Academic policies and procedures.