Table of Contents

ECSU Policy on Computer Use

Section A - Rules and Regulations

1. Availability and use of computer resources is restricted to actively enrolled students, current employees, and emeritus faculty and staff of Eastern Connecticut state University. Use of computer resources is a privilege, not a right. Therefore access to computer resources may be immediately disabled, suspended or revoked if abused.

2. Computer accounts are not to be shared with other users; when evidence of account sharing is found, all parties involved will be considered to be in violation of this policy.

3. Users are responsible for the security of their own account and password. Consequently, account owners are responsible for actions taken from their account by any person, whether or not the action was taken with the owner's knowledge or permission. Actions that violate these policies can result in immediate disabling, suspension, and/or revocation of the account owner's privileges.

4. All computer resources and facilities of Eastern Connecticut state University shall be used solely for legitimate and authorized academic, instructional,research, administrative and public service purposes.

5. Any unauthorized or illegitimate use of computer accounts, resources or facilities will subject the violators to appropriate disciplinary, criminal and/or legal action by the University and/or the State. This includes any type of physical abuse to hardware, software, data, or facilities, as well as the deliberate violation of any of the policies described in this document.

6. Any person who has been authorized to use the computing resources shall be expected to regard all copyrighted personal or proprietary information which may thereby become available to him/her as confidential, unless he/she obtains from the owner written permission to copy, modify, or otherwise use any part of it. Any software for which the the University or the state has obtained a license, will be used in accordance with the terms of the license.

7. Each user's programs and data are considered his/her private property.Users shall therefore not attempt to access, copy, modify, replace, delete or otherwise make use of any other user's account or its contents. Users also shall not harass or annoy other users, nor subject other users to obscene or offensive language through the campus network.

8. Users shall not attempt to copy, modify, replace, delete or gain unauthorized access to any software component or data file that is part of, or is used by, the computer operating system and/or other computer management programs.

9. The Data Center reserves the right to access user data and programs for appropriate management purposes, such as performing backups, and to ensure system integrity and security, subject to the limitations of Connecticut General Statutes.

10. Users must not attempt unauthorized modification or repair of any equipment owned or controlled by the University. No equipment will be connected to or disconnected from the network without prior, written permission from the Data Center.

11. Computer resources shall not be used for non-academic work without the written permission of the appropriate authorities. Non-academic work includes,but is not limited to: personal record-keeping, game-playing that is not assigned class work, and any task related to the management of a private business.

12. The University and its authorized personnel reserve the right to perform computer resource management functions, which include but are not limited to: setting priorities on the use of University computer facilities, establishing expiration dates for user files and accounts. and limiting or denying access to computer resources when system maintenance or repairs are required,or when environmental conditions present & risk to users or equipment.

13. User programs and data are considered his/her private property, and therefore are his/her responsibility. While efforts are made to ensure that reasonable security and backup procedures are carried out, the University and its personnel shall not be held liable for damage to, theft of, or loss of, user programs and data by means of procedural error, equipment malfunction, vandalism, or natural or man--made disaster.

Section B - Consequences of Policy Abuse

- The Data Center reserves the right to immediately disable any account in possession of programs, procedures or other information that presents a security threat to the system, network and/or other users. Examples include,but are not limited to any program or procedure that is designed to: obtain other users' passwords; obtain access to restricted programs, systems or data; modify restricted programs, systems or data; obtain system privileges beyond those initially granted to the user account by authorized Data Center or University staff; deceive system management personnel or inhibit system management efforts.

  Use of the system to harass other users, transmit obscene or offensive language, or otherwise threaten system users or resources shall be cause for immediate disabling of the account. Possession of unauthorized information,such as confidential student, personnel or financial data will also because for immediate disabling of the account. When a student account is disabled by the Data Center, the account will remain disabled until the situation is investigated and appropriately resolved. If the investigation results in charges being filed against the account owner, the account will remain disabled until a final disposition is determined through the campus Student Conduct process. Punishable offenses, sanctions and the Student Conduct process are described in the ECSU student Handbook under 'Connecticut State University offenses and Maximum Sanctions - Proscribed conduct " and "The Connecticut State University Guidelines for student Rights and Responsibilities and Student Conduct Procedures. "

  University employees are expected to comply with university policies and regulations. when such is not the case, the university may take action through the disciplinary process of the appropriate collective bargaining agreement. Criminal charges may also be filed by Eastern Is University Police under state and/or federal computer crime laws. For example, Connecticut law states:

"A person is guilty of the crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization. "
[Connecticut General Statutes, Sec. 53a-2511]

"A person is guilty of an attempt to commit a crime if ... he [is in] possession of materials to be employed in the commission of the crime,which are specially designed for such unlawful use or which can serve no lawful purpose of the actor under the circumstances
[Connecticut General Statutes, Sec. 53a-491]

"A person is guilty of conspiracy when, with intent that conduct constituting a crime be performed, he agrees with one or more persons to engage in or cause the performance of such conduct, and any one of them commits an overt act in pursuance of such conspiracy. I
[Connecticut General Statutes, Sec. 53a-481]

CSU Policy on Student Use of University Computer Systems and Networks

1. University computer systems and networks are provided for students as a part of the University academic program. Students are encouraged to become proficient in the use of the computers as a means of enhancing their educational experience. However, widespread student use also necessitates certain rules of computer conduct. Computer misconduct can result in restrictions on or revocation of computer access privileges.

2. University computer systems and networks constitute an expensive and valuable resource. The capacity of this resource to fulfill all the legitimate academic and administrative needs of students, faculty and staff is limited.

3. Students users have a responsibility to use University computer resources in an efficient, ethical, and lawful manner.

4. The University has a right and duty to protect its valuable computer resources and to restrict student access to uses that are strictly related to the students' academic programs as well as reasonably limited in time. The University reserves the right to define what are unauthorized student uses.

5. The Chief Computer Administrator or designee(s) at each University in the CSU System and at the System Office may monitor student user accounts, files, and/or log-in sessions for appropriate management purposes. Such purposes include but are not limited to performing archival and recovery procedures, evaluating system performance, and ensuring system integrity and security.

6. Upon identifying a violation of this policy which constitutes an immediate, clear danger to the University computer systems or networks the Chief Computer Administrator or designee(s) at each University and in the System Office may immediately limit or suspend a student's access to University computer resources with immediate notification of charges and actions to the appropriate Chief Student Affairs Administrator or designee(s). This emergency suspension of computer use will then follow the student conduct procedures for "Interim Suspension" as provided in the CSU Student Rights and Responsibilities and Student Conduct Procedures document.

7. Violations of University computer policy which do not constitute an immediate, clear danger to the University computer systems or networks will be referred to the regular student disciplinary process.

8. Student computer offenses, which are included as number 25 in the Appendix of Punishable Offenses in the CSU Student Rights and Responsibilities and Student Conduct Procedures document are as follows:

    1. Unauthorized use of University computers and/or peripheral systems and networks;

    2. Unauthorized access to University computer programs or files;

    3. Unauthorized alteration or duplication of University computer programs or files;

    4. Any deliberate action to disrupt the operation of University computer systems which serve other members of the University community, including all networks to which University computers are connected;

    5. Use of University computer systems and networks for committing crimes, violating civil laws, or violating University rules.

9. UNAUTHORIZED USES for students include but are not limited to the following:

    1. Computer games which are not assigned course work;

    2. Development or transmitting of chain letters;

    3. Entering or transmitting of commercial advertisements or solicitations;

    4. Entering or transmitting of political campaign material relating to elections to be held outside the University;

    5. Entering or transmitting of obscene material;

    6. Sexual harassment or other forms of harassment aimed at others or otherwise threatening others;

    7. Sharing one's own computer account with others or using another person's accounts;

    8. Violation of copyright laws or using or copying software in ways that violate the terms of the license;

    9. Entering or transmitting computer viruses or any form of intentionally destructive programs;

    10. Intentional disruption of network services;

    11. Connecting any device to the network without permission;

    12. Copying, modifying, replacing, or deleting any other user's account or any software used for system management;

    13. Harming University computer equipment;

    14. Uses which violate rules developed at each University which are necessitated by facilities limitations or other circumstances unique to each University.

Notice on Electronic Monitoring

This notice is the University's practice to address all faculty, staff, and student employees each semester about the CSU policy concerning the use of various information technology devices. Use of the information technology infrastructure has become commonplace at Eastern, as it has in virtually all businesses and institutions. Please read carefully the following statement about privacy issues and legal considerations in that regard. The statement below is released from the Connecticut State University System Office and includes the attached Public Act 98-142.

The Connecticut State University System deems it necessary and advisable and in the best interest of the university communities of Eastern, Central, Southern and Western Connecticut State Universities and the System Office, to again raise awareness and re-emphasize legal considerations concerning information technology devices in use throughout the system.

There are several information technology devices in use in the CSU System. These devices are the property of the State of Connecticut and use thereof by the user is restricted to the performance of official State business or activities approved through the collective bargaining process. Information related to usage and utilization of these devices and the overall CSU technological environment is constantly being collected.

The Connecticut State University System information technology infrastructure includes a telephone system, a communications network, Internet access, computer servers and computer workstations. Information related to the usage of this infrastructure is collected and logged. All users of these devices are hereby advised and notified that these devices produce data and reports related to information stored, sent and retrieved for the purposes of recording usage and utilization. While system personnel do not review the contents of this material except when necessary in the course of the discharge of official duties and as permitted by law, each user should know and is hereby notified that all such information is subject to subpoena, discovery, the Connecticut Freedom of Information Act and such other disclosure processes as may be authorized by law.

This notice is issued pursuant to the provisions of Public Act 98-142.

- -- -

Substitute House Bill No. 5398

PUBLIC ACT NO. 98-142

AN ACT REQUIRING NOTICE TO EMPLOYEES OF ELECTRONIC MONITORING BY EMPLOYERS.

Be it enacted by the Senate and House of Representatives in General Assembly convened:
(NEW) (a) As used in this section:
(1) "Employer" means any person, firm or corporation, including the state and any political subdivision of the state which has employees;
(2) "Employee" means any person who performs services for an employer in a business of the employer, if the employer has the right to control and direct the person as to (A) the result to be accomplished by the services, and (B) the details and means by which such result is accomplished; and
(3) "Electronic monitoring" means the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems, but not including the collection of information (A) for security purposes in common areas of the employer's premises which are held out for use by the public, or (B) which is prohibited under state or federal law.
(b) (1) Except as provided in subdivision (2) of this subsection, each employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur. Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice.
(2) When (A) an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice.
(c) The Labor Commissioner may levy a civil penalty against any person that the commissioner finds to be in violation of subsection (b) of this section, after a hearing conducted in accordance with sections 4-176e to 4-184, inclusive, of the general statutes. The maximum civil penalty shall be five hundred dollars for the first offense, one thousand dollars for the second offense and three thousand dollars for the third and each subsequent offense.
(d) The provisions of this section shall not apply to a criminal investigation. Any information obtained in the course of a criminal investigation through the use of electronic monitoring may be used in a disciplinary proceeding against an employee.

Approved June 4, 1998

Residence Hall Network Connection Policy

The following is a list of rules and regulations established by Connecticut State University governing student connections to the campus computer network from within the Residence Halls.

1. The student will agree to abide by all CSU and ECSU policies governing the use of campus computing facilities.

2. The student will provide a microcomputer or terminal capable of a network connection. (The University will provide, upon request, a list of typical equipment, cables, terminal emulators, and operating systems that can be used to connect to the network.)

3. The student is responsible for all installation configuration, and repairs to personal computers and peripheral equipment, including cables, network cards, and software used to connect to the network. The student is responsible for troubleshooting and maintaining their own equipment.

4. The student shall follow and implement any instructions given by the Data Center as regards network configuration and addressing. Failure to do so can have a detrimental impact on other students in the residence hall. The Data Center reserves the right to disconnect without notice any equipment which is judged to be causing network problems or does not conform to our recommended configuration.

5. Any attempt by the student to break into other's computers, accounts, or other similar destructive behavior on the network will result in the immediate loss of network connection plus result in disciplinary and/or legal action.

6. The student will not tamper with or modify in any way, university-owned equipment or the wiring connection in the wall of their Residence Hall room. Failure to comply will result in the discontinuance of network services to the room, as well as any necessary disciplinary and/or legal action. The severity of the violation will determine the type of action that the University and/or the State will take against the violator.

7. The University will not store student computer addresses in its Domain Name Servers.

8. Network users must comply with all copyright laws or agreements governing the use or duplication of software or other proprietary data.

At the January 7, 2009 meeting of the Council of Presidents, the CSUS Email Policy - Email as an Official Correspondence, was approved with an effective implementation date of August 1, 2009. Attached please find a copy of the policy.

CSUS Email Policy

University Relations would ask anyone who administers a social media site in connection with Eastern to make sure that they have done the following essential tasks associated with Eastern-related social media pages.

1. Any official page of the University (see link to the full policy for definition) must have a disclaimer that clearly indicates that the site is an official communication of the University and is managed by a University employee. This disclaimer language is referenced in the full policy statement.
2. Student clubs, personal faculty accounts, and faculty classroom-based accounts are exempt from the policy, but are asked to include a disclaimer that indicates that the page is not an official communication of the University. This disclaimer language is also referenced in the full policy statement.
3. Links to all official social media pages, including those for any academic or administrative departments, must appear on the University website's Social Media ("Connect With Us") page found at http://www1.easternct.edu/universityrelations/social-media/ If you administer an official social media account and it is not found on this page, please let me know so that we can add you.
4. While student clubs do not have to post social media accounts on "Connect With Us," they are welcome to do so-the additional exposure could be helpful.
5. To update our records, we ask any faculty member or staff person one who does administer an official social media account to respond to this email.

Our goal is to update http://www1.easternct.edu/universityrelations/social-media/ as well as our list of social media account administrators. Thank you in advance for your cooperation.

Full Social Media Policy

As of May 23, 2011, Eastern Connecticut State University will no longer provide telephone service or voice mail service in student residence hall rooms except in those student rooms designated to conform to ADA requirements. House phones are located on each residence hall floor which may be used for incoming calls and to place 911, campus, local and toll free access calls. Students may use their own cellular phone service or Internet phone providers using their PCs.

Residence Hall House Phones

Emergency (911), on campus, local, long distance and "800" toll free calls may be made from house phones as described below. House phones can also receive incoming calls. Each phone is labeled with the telephone number assigned to it.

To place a call for emergency assistance:

1. Pick up handset (hear dial tone)
2. Dial 911

To place a call to another number on campus:

1. Pick up handset (hear dial tone)
2. Dial the 5-digit extension (last 5 digits of the telephone number)

To place a local call:

1. Pick up handset (hear dial tone)
2. Dial 9 + area code + telephone number (do not dial "1" after the "9")

To place a long distance call:

1. Use a telephone calling card with a toll free access number
2. Follow the dialing instructions on the calling card

To place an "800" toll free call:

1. Pick up handset (hear dial tone)
2. Dial 9 + 1 + 800 + telephone number (current toll free area codes are 800, 866, 877 and 888)

Cell Phones

Cell phones may be used in residence hall rooms. ECSU does not provide its own cell phone service and does not guarantee cell phone coverage or quality of service from any particular cell phone carrier.

Internet Phone Providers*

Phone calls may be made from a PC to a phone or another PC. There are several Internet phone plans that allow free calling within the United States and to Canada such as Skype (www.skype.com), Google Talk (www.google.com/talk) and iCall (www.icall.com). Information about the types of calls that can be placed from a PC, software that may be needed (usually downloadable for free) and rates that may apply for various types of calls can be found on the websites for these and other providers.

NOTE: A free Internet phone cannot be used to place an emergency call to 911. Emergency 911 calls should be placed from a land line or cellular phone.

**ECSU is not affiliated with and does not endorse any particular Internet phone service. The providers listed are for example purposes only.*

Rev. May 2011
Jody Barr
ITS-Telecommunications
barrj@easternct.edu
860-465-0025

The Blackboard Section purge process will be executed biannually every January and June. Blackboard section content will be available in the production system for faculty use for a duration of two years. Section data more than two years old, calculated by the start of the current semester, will be removed from the production system. Faculty will be sent a reminder regarding the biannual purge process no less than 30 days prior to the date of the purge. This notification will provide faculty time to export Grade Book and any other pertinent section data prior to the purge, if necessary.

To learn how to export the grade book go to Article 94: Working Offline with the Grade Center

Export a Blackboard Course Backup:

- Go to the course you want to backup.
- On the Control Panel Menu click on Packages and Utilities.
- Click on Export/Archive Course.
- Click on the Export Package button.
- Under Select Course Materials click Select All.
- Click Submit.
- Click Refresh to see the link to the file (this may take a while if the course is large. You should receive an email when the file is ready if you don't want to wait).
- Put your mouse over the file name listed and pull down the menu using the arrow that appears to the right of the title.
- Choose Open.
- You should be prompted by your browser to Open or Save the file.
- Choose Save and save it to a location you can find again when you require it.

Your export file can only be used in another Blackboard Learn System. You can not open and extract individual content from it. If you want to import it into another system/course use the instructions below.

Import a Backup into Blackboard Learn:

- Go to the blank course you want to import the content to.
- Click on Packages and Utilities at the bottom of the left menu (Control Panel).
- Click on Import Package/View Logs.
- Click the Import Package Button
- Click Browse My Computer and navigate to the saved export file you stored previously.
- Click Select All.
- Click Submit.

For inclusion in student handbooks, program manuals, departmental statements of policies and procedures, etc.:

This ____[handbook/manual/etc]___ is provided to students and applicants for their general information and guidance only. It does not constitute a contract, either express or implied, and is subject to revision at the University's discretion

For inclusion in undergraduate and graduate course catalogs:

Students should be aware that additional requirements may be imposed for certification or licensure (even once a plan of study has been prepared) if such requirements are imposed by outside licensing or accrediting agencies. A plan of study may be subject to revision to reflect such additional requirements.

Securing Sensitive Information

Management of Portable Media Devices and Sensitive Documents

Overview:

The University must take every reasonable precaution to secure both sensitive personal data and paper records, under federal and state law. Threats to the security of sensitive items come in several forms and each threat must be dealt with a unique countermeasure. An important element in Information Security is an effective ongoing security education and training program. The CSU system has access to a number of security training programs available online at http://csuso.cosaint.net, such as the Security of Mobile Devices, along with a general awareness program. All members of the campus community with access to sensitive personal data will take the Information Security Awareness program within csuso.cosaint.net. These individuals will be identified by the University's Information Security Officer. Initial training through Cosaint will be followed up annually by visits from the security officer to document ongoing efforts to secure sensitive data. Access to these programs can be arranged via the HR office on campus.

Definitions:

Sensitive data:

- Any information, which through loss, unauthorized access, or a modification could adversely affect the privacy of individuals.
  - For example: security numbers (SSN), driver's license number, credit card number, bank account number, tax information, date and location of birth, and all such personally identifiable information as specified under FERPA, and counseling records.

Portable Device:

- An electronic device that is capable of storing data. A portable media device includes, but is not limited to laptop and desktop computers, USB storage devices, DVD, CDs, tape or portable hard-drives. Also included are point of sale or (POS) devices used to process credit cards.

Data Security:

- The most effective procedure to limit exposure of Sensitive Data is to consolidate the storage of this information in a secure environment. Eastern's policy will prohibit the storage of Sensitive Data on any portable media devices. All digital material of a sensitive nature required for business operations will be stored on a designated network server drive, with password protection, within the University's secure datacenter. If necessary, this data will be encrypted to further enhance security. The university will not allow this data to be removed from the network drive and placed on a portable device. However, remote access is possible if a legitimate business requirement exists.

- The use of Virtual Private Network (VPN) for remote access to data on Eastern's servers over the Internet will be required instead of copying information to portable media. Training on the use of the VPN and other technologies will be provided by ITS. When employees are off-campus and engaged in the VPN accessing sensitive material, they must never leave the computer unattended. This may result in compromising data shown on the screen.

Transmission Security:

- No data will be transmitted from the University without taking appropriate security measures. For example, Sensitive Data cannot be transmitted via EMAIL unless encrypted. Encryption devices can be obtained from ITS. Transmitting data to a third party or contractor will require a legal review and contract language stipulating the data must be destroyed at the end of the contract period or when the project is complete, whichever is sooner.

Records Security:

- Several offices on campus are required to maintain paper and digital copies of important records that contain sensitive personal data. Paper and digital records must be secured and access limited to a need to know basis when conducting official University business. The paper records will be secured in a lockable cabinet. The cabinet will be located on University property with the office area having lockable doors and windows. All records will be destroyed based on the state of Connecticut records retention schedule using an approved contractor or on-campus shredding machines.

Security Breaches:

- Whenever an ECSU computing device, storage media, including but not limited to laptops and desktop computers, is found missing, stolen or lost, the individual responsible for the device or media will report the loss to his or her supervisor and the Information Security Officer within one hour of ascertaining the loss. In the event of a breach, the CIO will process the event following the Universities ITS Incident Response Team protocol to ensure a full record of the event is documented.

- Paperwork will subsequently be filed with the Property Control Unit to appropriately track the asset. The president and Chancellor will be notified through a separate reporting channel, by the CIO.

Policy Exceptions:

- If there is a compelling business need to store Sensitive Data on a portable media device the following actions must be completed. The respective area Vice President will conduct and document a risk analysis outlining the threats, benefits, and countermeasures for allowing Sensitive Data to be stored on a portable media device. The business case and risk assessment will then be presented to the President or designee for review and authorization. Unless it cannot be done, Sensitive Data stored on portable media will be encrypted with a CSUS-approved encryption method.

Contact Information:

- Chief Information Officer: Garry Bozylinsky, bozylinskyg@easternct.edu, 860-465-5750

ITS/CIO

April 28, 2008
October 10, 2019

Software Internal Control Policy

Purpose:

This control is established to ensure Eastern Connecticut State University meets the standards for governing the use of approved and/or licensed software by State agencies, to maintain inventory control of software and to establish a uniform policy for the prevention of software copyright infringement.

Policy:

1. The Budget Authority completes requisition to purchase software and sends requisition to purchasing. (During this process the end-user may consult with Analysis & Support Technician, CIT for technical assistance).
2. Purchasing forwards a copy of the requisition to the Analysis & Support Technician, CIT for analysis and approval. CIT approves or modifies requisition, in consultation with end-user and returns to purchasing.
3. Purchasing issues a purchase order, which indicates the software, will be shipped to CIT.
4. The Analysis & Support Technician at CIT receives software package or authorization codes from the vendor and notifies the Budget Authority or end-user the product has arrived on campus. The end-user coordinates installation with the Helpdesk or CIT.
5. The Analysis & Support Technician at CIT provides control information and media to ITS Administrative Assistant for inventory purposes.
6. The Administrative Assistant provides the Helpdesk with installation information for standalone applications. For lab installs, the ITS Admin Assistant will provide an email with installation instructions.
7. Helpdesk or lab technician provides inventory information to the ITS Admin Assistant to finalize the transaction.
8. The ITS Admin Assistant maintains Critical Data Element and media for inventory control purposes.

Critical Data Element:

The software inventory will contain the following property control items.

1. Assigned Identification Number: a numerical number assigned sequentially per fiscal year. For example: 06-001. 06 fiscal year, 001 first entry of fiscal year.
2. Title of Software:
3. Description: software name or functional application.
4. Version:
5. Manufacturer/Reseller:
6. Software Serial/Registration Number(s) (if applicable)
7. Acquisition Type: (leased, purchased, loan, gift)
8. Acquisition Detail: purchase order number, donation source or gift source)
9. Initial Installation Date:
10. Location and Identification Number of Computer:
11. Cost:
12. Disposal: Upgraded (list new serial number), transferred, sold or destroyed.

Media Storage:

All media and keys will be stored in a central ITS location and tied to the Critical Data Element inventory. Combining the policy and Critical Data Element will ensure a closed process for software inventory. ITS will maintain the Critical Data Element using QueTel's TraQ Software. The media from the purchases will be stored in a lockable cabinet, inventoried in TraQ and a backup copy stored in a remote location. Under no circumstances will access keys or media be removed from storage without an authorized Helpdesk work order. Coordination will be required between CIT and the Critical Data Element administrator, the ITS Administrative Assistant.

Administrative Procedures:

The Chief Information Officer, working with Associate Vice President for Administration and Finance will be the responsible party for monitoring and establishing the software inventory. The ITS Administrative Assistant working with CIT will establish and be responsible for the administration of the Critical Data Elements, physical security of software media and manuals. Annually, a software inventory report will be produced and act as a basis for comparison with a physical inventory of the software library.

All software purchased by the University will be registered to Eastern Connecticut State University, or the Connecticut State University System. Under no circumstances will an individual be named as licensee holder of any software bought, leased or owned by the State of Connecticut, or purchased with non-State funds for use by the State. Personal software is software that is not licensed to the State of Connecticut or its subdivisions. Personal software may not be installed on any computer owned or leased by the State or the Federal Government or purchased with Federal Funds for use by the State, except in those specific instances covered in "License Agreements" found in Chapter 7 of the State of Connecticut Property Control Manual. Any installation of personal software may compromise the integrity of the State's compliance with copyright laws and may expose the stand-alone computer or network file server to the introduction of computer viruses. Faculty may purchase software for use on computers at the University through the ECSU Foundation. Freeware, shareware, and software used at no cost to the University in the pursuit of the academic mission is covered under the Academic Freedom rules of the collective bargaining agreement. If an individual faculty member wishes to download such software for use on a University-owned computer, they must determine the level of security risk associated with the product. If assistance is required on the security classification of non-purchased software, individuals should contact the CIO via email. For additional restrictions on software contact the University CIO.

This policy shall be incorporated into the University's technology plans and employee orientation program.

JRT:

12/12/08

Eastern Connecticut State University Residential Computing Fact Sheet

The ECSU residential computer network, better known as Resnet, provides network connectivity for all residential students. Resnet is designed to be as reliable as is possible in providing learning services plus office and building operation.

Use a standard ethernet cable to connect your PC to Resnet. Ethernet cables are available in Media 252 (no cost).

Personally owned computers must meet certain criteria to be given Internet access. They must:

- Have properly licensed and UPDATED operating systems and application software.
- Be configured to receive automated operating system updates.
- Have anti-virus software running that is configured to receive automated updates.
- Not have peer to peer software, viruses, or spyware actively running.

When your PC is physically connected to the network and turned on, it will be checked to determine if it meets these requirements. If the PC needs to be updated, directions will be provided. If you need more information about configuring your PC browse to http://help.easternct.edu where you will have access to software upgrades and instructions.

Until these criteria are met, access to the Internet will be blocked. Local services from ECSU, such as E-mail and Blackboard Vista will remain available.

Personally owned computers that have active peer to peer applications, viruses, or spyware will be quarantined: browsing to any external web site will return a page explaining that the PC is quarantined. Please see the above Help Page for details and information about how to get out of quarantine.

Students are responsible for maintaining the configuration of their PC. ITS staff cannot repair or reconfigure personally owned computers.

Several network security tools are in use which helps provide enhanced reliability for Resnet. There are a number of network gateway devices, such as Packeteer and Interspect that screen for illegal applications or activities consistent with virus activity. The Cisco Clean Access product enforces basic personal computer hygiene. Anti Virus software is required, which further enhances personal computer hygiene. While these are common requirements in an enterprise computing environment, they may at first pose an obstacle for the home user. ECSU Information Technology Services (ITS) is committed to helping the Resnet computer user succeed in this enterprise environment.

Local services such as the Blackboard Vista course management system, student E-mail, on-line course registration, anti-virus software, and directions for self-directed help are all available online even when the PC is blocked or quarantined.

Web Policy

Incident Handling: An Orderly Response to Unexpected Events

Copyright

Sharing Online Songs, Videos and Documents

The U.S. Department of Education has issued new regulations regarding the distribution of copyrighted materials such as songs, games and videos through uploads and downloads over computer networks. The regulations are focused on combating the unauthorized, illegal distribution of copyrighted materials via Peer-2-Peer file sharing networks.
Higher education institutions are now required to develop and implement plans to deter the unauthorized sharing and distribution of copyrighted materials. The information in these Articles and FAQ sections detail elements of ECSU's plan including:

- Information about legal and illegal methods of sharing copyrighted materials
- The significant penalties associated with copyright violations
- Statutory fines within a range of $750.00 - $150,000.00 per infringement.
- Possible University sanctions: any of the following or any combination of the following: expulsion, suspension, disciplinary probation, disciplinary warning, residence hall separation, residence hall probation and residence hall warning.

How you will be identified if your computer is used to illegally share copyrighted materials: You are not anonymous on the network.

Please review and become familiar with the materials in these related articles and the FAQs below:

- What is P2P or Peer 2 Peer file sharing?
- What is copyright infringement?
- What are the consequences of illegally sharing videos and songs?
- How Does Eastern Respond illegal file sharing?
- How can I legally share copyrighted materials?
- How can I acquire legal copies of songs and videos?

ECSU Policies and Information About P2P File Sharing

Subject: Peer-to -peer File Sharing (P2P) - You are Not Anonymous on the Network

Many students at Eastern download music, videos, games, software and other materials and store them as files on their computer for their personal use. Much of this material is copyrighted, that is, federal law protects the people who create these materials granting them exclusive use or ownership of the material for specified time periods. Copyright law establishes rules that govern who and how copyrighted material can be accessed and used. Generally, the permission of the owner of the material is required before it can be legally copied or distributed.

Online sources that provide legitimate, legal downloading services are available through Eastern's link to the internet. Click here for a list of legitimate online sources from which you can download materials.

If you are storing and using copyrighted material on your computer, it is your responsibility to insure that the material is not illegally shared with others. One way of illegally sharing material is to install Peer-to-Peer File sharing software (P2P) on your computer and allow others to upload copyrighted materials from your computer to theirs. It is also possible for your computer to become infected with a 'virus' that allows others to illegally upload materials from your computer. You may not be aware that your computer has this 'virus' and that you are illegally sharing protected materials.

In either case you are violating federal law and University policies. There are significant federal criminal and civil penalties for doing so. Eastern and the CSUS also have penalties in place that apply to copyright infringement. They include expulsion, suspension and other possible disciplinary sanctions.

It is important to realize that copyright violations will be discovered and that they can easily be traced to the specific computer that is the source of illegal uploading. Several copyright enforcement organizations continuously monitor and search the Internet for violations. When they determine the source of the material they can require the organization hosting the computer on its network to provide additional information that will identify the individual using the computer. They may then initiate civil or criminal proceedings to protect their copyright.

The Higher Education Opportunity Act of 2008 requires that colleges and universities combat the unauthorized distribution of copyrighted materials.

Please review the related articles and learn how to legally access and use copyrighted materials avoiding the penalties associated with copyright infringement.

Consequences of Copyright Infringement

What is copyright infringement?
As a general matter, copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner." - http://www.copyright.gov/help/faq/faq-definitions.html

Both the federal law and the Connecticut State University System's Student Code of Conduct policy specifically prohibit copyright infringement. Each imposes significant penalties for doing so.

It is important to note the following:

> Recognizing the author of a specific statement such as footnoting or attributing authorship of material is not the same as getting permission from the copyright owner to reproduce the material. Even with such recognition, copyright infringement can occur.
>
> Students are subject to federal and state laws in addition to University policies. University disciplinary processes do not exempt a student from federal and state civil and criminal processes.
>
> You are responsible for any copyright violations that occur from your computers address. A friend or roommate using your computer for illegal activities can place you in jeopardy.
>
> Even if you have legally purchased copyrighted material such as a song, it is still illegal to share your copy of the song with others unless you have the copyright holders permission to do so.

What are the Consequences of Copyright Infringement?
In the case of Federal law, several possible consequences for copyright infringement have been specified. Content owners are entitled to actual or statutory damages when copyright infringement occurs. They are entitled to recover actual damages and any profits of the infringer that are attributable to the copyright infringement. Or they may choose to recover statutory damages within a range of $750.00 - $30,000.00 per infringement. In the event that the copyright owner proves that you willfully (with knowledge of the existence of a copyright) committed an infringement, the court may award damages as high as $150,000.00 per infringement.

The Connecticut State University System's Student Code of Conduct and Statement of Student Conduct Procedures Policy on Student Use of University Computer Systems and Networks includes "...unauthorized peer-to-peer file sharing of copyrighted materials..." as a prohibited conduct subject to disciplinary sanctions (Part III, Section 22). Possible sanctions are any of the following or any combination of the following: expulsion, suspension, disciplinary probation, disciplinary warning, residence hall separation, residence hall probation and residence hall warning (Part V). The Code specifies the Student Conduct procedures that will be used to determine sanctions.

Fair use: Legally Sharing Copyrighted Materials

There are limits to the exclusive use rights granted by a copyright. These limits are generally referred to as the 'fair use' of copyrighted materials. Fair use permits the use of copyrighted materials without the specific permission of the copyright owner. The distinction between fair use and infringement is often unclear and difficult to establish.

Federal law provides some guidelines to use in establishing fair use. Portions of a particular work may be reproduced and considered fair use if the purpose of doing so is criticism, comment, news reporting, teaching, scholarship, or research. So, including short passages of someone else's written work in your report or paper is allowed under the fair use provision. Don't forget the footnote! Showing portions of a film or listening to portions of someone's musical composition in class are also fair use of video or musical material.

If you subscribe to a service that provides legal copies of copyrighted work such as iTunes, you are required to use all downloaded materials (songs) in accordance with the service's rules of usage. Generally these rules prohibit you from sharing your downloaded files with others. You cannot make files you legally downloaded available for others to copy to their computers. Doing so is a violation of copyright laws and you will be subject to fines, legal actions and penalties.

There are guidelines for legally sharing someone else written materials, songs or videos. However, the guidelines are not clear or easy to apply to many cases.

The Best Rule of Thumb: When in doubt, get permission!

The CUSU system has more details about copyright at https://www.ct.edu/copyright

ECSU Response to Copyright Infringement

How Does Eastern Respond to Copyright Infringement Notices?

Copyright holders and their agents search the Internet for copies of their material that is illegally being made available for sharing via P2P software. When they find such activity they are able to identify the IP address of the computer sharing their material. They may then contact the network provider, in this case the CSU System, issuing a copyright infringement notice requesting that action be taken to prevent further infringement of their copyright. They may also begin a process which may result in the payment of a substantial infringement fee or the initiation of a criminal charges.

When Eastern receives a copyright infringement notice, the network access of the computer associated with the IP address included in the notice is restricted and its access to the Internet is blocked. Residence Life is notified of the restriction and a campus conduct process is begun. A hearing occurs to determine if the student has violated the University's policies regarding illegal file sharing. If a violation has occurred, disciplinary sanctions may be imposed. Sanctions include any of the following or any combination of the following: expulsion, suspension, disciplinary probation, disciplinary warning, residence hall separation, residence hall probation and residence hall warning. (Student Code of Conduct, Part V Disciplinary Sanctions)

Internet access remains blocked until a formal recommendation for access reinstatement is issued through the conduct process.

Students are subject to federal and state copyright laws in addition to University regulations and policies. The consequences in copyright infringement are significant. See this section for a summary of possible University sanctions and civil and criminal penalties for violation copyrights: Article 42: Consequences of Copyright Infringement

Peer-2-Peer Software and File Sharing Summary

P2P software such as eDonky, LimeWire, and BitTorrent enables computers on a network to share files containing content such as music, movies and games. For example, the software can be used to search the network for a copy of a specific song that is available for 'sharing'. Once located, the song can then be downloaded and enjoyed.

If the material being copied is 'in the public domain', P2P software can be legally used to copy and share it. However, if the material is copyright protected, sharing it without the permission of the copyright holder violates federal laws and University policies. For more information about copyright violation see the section on Article 42: Consequences of Copyright Infringement.

Copyright owners often specifically target university networks and search for unauthorized file sharing activities. When they find computers engaging in this activity they can and will take steps to identify the person who has registered that computer for use on the network. Lawsuits have been filed against thousands of individuals using P2P software. Many of these individuals have had to pay significant fines to avoid even more severe penalties.

Some P2P software companies claim that they provide users of their software with anonymity. However, if you use Eastern's network for P2P file sharing, you are not anonymous. Information about your P2P activities and the identity of your computer is available to those searching for unauthorized file sharing. This information can be specifically linked to you.

Reputable P2P software services are available and legal to use. These services have secured the permission of the copyright owner to distribute copies of their work. For a list of Internet sites that provide legitimate file sharing services see Article 44: A List of Sources for Downloadable Materials.

A List of Sources for Downloadable Materials

The Higher Education Opportunity Act requires that Universities "offer alternatives to illegal downloading". The list of Internet sites (below) from which legitimate copies of music and videos can be downloaded was created by EDUCAUSE. It may not include all sources of legal copies of these types of materials. However, it does establish that there are many legitimate sources of copyrighted materials available. No endorsement or evaluation of these sites is intended.

Typically these sites will charge for their services. They will also have usage agreements that you must follow. These agreements may permit your exclusive use of the material and prohibit copying or sharing the materials with others.

Even in these cases, it is important to take several steps to protect your computer from being used for illegal file-sharing:

- Enable a software firewall on your computer
- Install antivirus software and keep it current
- Install antispyware software and keep it current
- Regularly update your operating system and other software programs on your computer
- If you legally purchase copies of copyrighted files, do not store them in a P2P file-sharing folder
- If you legally purchase copies of songs and videos, do not allow others to copy them from your computer

The ECSU Help Desk can assist you in implementing these steps.

- ABC.com TV Shows
- Amazon MP3 Downloads
- Amazon Video on Demand
- Amie Street
- AOL Music
- ARTISTdirect Network
- AudioCandy
- Audio Lunchbox
- BearShare (version 6 or higher)
- Best Buy
- BET
- Blip.fm
- Blockbuster Online
- Bravo Videos
- Buy.com
- Cartoon Network Video
- Catsmusic
- CBS Video
- CD Baby
- CinemaNow
- Clicker (formerly Modern Feed)
- Comedy Central Video
- Criterion Online
- The CW Video
- Dimple Records
- Discovery Channel Videos
- Disney Videos
- Download Fundraiser
- The Electric Fetus
- eMusic.com
- ESPN360
- EZTakes
- Fancast
- FOX on Demand
- FX Networks Video
- FYE
- Gallery of Sound
- GameFly
- GameTap
- Hulu Movies & TV
- iLike
- iMDb Video
- imeem
- iMesh
- Independent Records & Videos
- iTunes Movies, Music, & TV
- Jaman
- Jamendo
- Joost Movies & TV
- Lala
- Last.fm
- Latinoise
- LifeWay Music
- Liquid Digital Media
- Listen.com
- Magnatune
- MediaNet
- Mindawn
- MovieFlix
- MP3.com
- MTV Video
- Music Millennium
- MusicRebellion
- myLifetime Video
- MySpace Music
- Napster
- NBC Video
- Netflix Movies & TV
- Neurotic Media
- Nick Jr. Video
- Pandora
- PBS Kids Go! Video
- PlayStation Store
- Pro-Music
- Public Domain Torrents
- Qtrax
- Record & Tape Traders
- Reeltime Television Network (RTVN)
- Rhapsody
- Slacker
- South Park Episode Player
- Spinner
- Spotify
- Steam
- Superpass
- TBS Videos
- TheWB
- TidalTV
- TNT DramaVision
- Top Hits Entertainment
- TV.com
- TVLand Video
- USA Network Videos
- VH1 Videos
- Walmart Movies & TV
- Walmart MP3 Music Downloads
- Windows Media Guide
- Xbox Live Marketplace
- Yahoo! Music

Plan to Combat the Illegal Distribution of Copyrighted Materials
Eastern Connecticut State University
Information Technology Department

Introduction:

In accordance with DOE P2P regulation requirements regarding copyright protection, ECSU has created this plan to combat illegal file sharing.

This plan will be reviewed yearly with emphasis on the following:

- New or changed DOE regulations and federal copyright compliance laws
- New technologies available to deter illegal file sharing
- New or changed CSUS and ECSU policies and the Student Conduct Code
- The list of legal download service sites
- Legal methods of Sharing Files

Plan Outline:

1. Semi-Annual Notice to Students and Faculty Regarding Copyright Compliance

   Under the direction of the CIO, the Campus Information Security Officer will distribute an email to all students, faculty and staff summarizing the requirements of current copyright law, DOE regulations and University policies. The summary will include notice of available sources for legally downloading copyrighted materials. Links to additional sources of information about file sharing will also be included. This notice will be sent at the start of the fall and spring terms.

2. Web Based Compliance Information Available to Students

   The semi-annual email will be accessible on the student portal. Additional information about the following compliance topics will also be available on the portal:
   - A description of Peer-2-Peer file sharing technology
   - A statement of how ECSU will process infringement complaints
   - A detailed statement of the federal, state and University penalties for copyright infringement
   - A list of alternatives to illegal file sharing
   - A summary of 'fair use' of copyrighted materials

3. Other Campus Sources of Information about Copyright Law and Compliance
   - The University will include information about illegal file sharing in new student orientation programs.
   - The IT help desk and student support center will assist students in their efforts to comply with copyright law and University policies

4. Technology Based P2P Deterrents

   DOE regulations require that the university use at least one technology based deterrent to Illegal P2P file sharing. This section of the plan documents the deterrent (s) that ECSU is currently using to comply with DOE requirements. Eastern continuously monitors developments in the area of P2P deterrent technology. A formal review of this technology and update of this section of the plan occurs yearly.

   Technology Deterrent: Packet Shaping

   Current Methodology:

   - The packet shaper is regularly updated with known P2P traffic signatures (patterns). It is configured to block all traffic that includes a P2P signature.
   - The packet shaper is also used to block all internet traffic from all computers that have been identified as engaging in illegal file sharing. The Specific MAC and IP address associated with the computer is used to establish a 'rule' prohibiting the shaper from allowing traffic from this source to pass on to the internet.
   - The packet shaper monitors traffic levels from individual sources. Limits have been set to restrict traffic levels far below those typically associated with P2P activity.
   - The compliance document 'How Does Eastern Respond to Copyright Infringement Notices' details the University's response procedures to complaints from sources such as the DMCA.

   Planed Changes and Upgrades to Eastern's P2P Deterrent Technology:

   - Currently, the task of associating the IP address and time stamp provided by copyright protection organizations with the MAC address of a specific computer and the name of the owner of the computer is very time consuming for Eastern's staff. This inefficiency can be eliminated through the use of identity management software. This software can be used to register a computer for use on Eastern's network capturing the owners name and the MAC address of the unit. Thus, two of the three items in the linked chain would be immediately available to staff through a simple query of the identity management database. ECSU should implement this software as soon as possible.
   - A prerequisite for a useful identity management system and a second major P2P compliance related issue for Eastern is a lack of sufficient IP addresses. The shortage of addresses forces Eastern to use NAT protocol (Network Address Translation). This protocol allows a small number of public IP addresses to be shared by a large number of computers. Eastern must acquire more IP address. If available for use, IPv6 addressing would enable the University to implement an IP addressing scheme that supported an effective identity management system.

5. Annual Plan Review

   Under the direction of the CIO, the Campus Information Security Officer will conduct an annual review of this plan. Various members of the IT staff and other campus departments will participate in the plan review process.

A draft revision will be reviewed and formally approved in accordance with University procedures.