Network Use Policy

Last Updated: 8/6/2014

Purpose / Scope

SUNY Broome is committed to safeguard the confidentiality, integrity and availability of all electronic information assets of this institution to ensure that regulatory, operational and contractual requirements are fulfilled. This policy is in place to ensure that important SUNY Broome teaching, research, administrative data and other confidential information is protected from theft or unauthorized disclosure.

SUNY Broome computing resources are provided to facilitate a person's work as a member of staff or student of SUNY Broome and are for educational, administrative, training or research purposes. *Persons who break this policy or code of conduct are subject to SUNY Broome's disciplinary and/or criminal procedures*. All users of SUNY Broome's computing and networking facilities are expected to read and abide by the respective regulations.

SUNY Broome reserves the right to update or revise this policy or implement additional policies in the future. Users are responsible for staying informed about SUNY Broome policies regarding the use of computer and network resources and complying with all applicable policies.

The overall purpose and scope of this policy is as follows;

a. Establish guidelines for access to and the use of SUNY Broome's information technology resources.

b. Applies to all faculty, staff, students, and contractors associated with SUNY Broome. It also applies to anyone that has a wireless or personal device on SUNY Broome's campus since they may be automatically interacting with SUNY Broome's wireless network.

c. Applies to any/all of SUNY Broome's information technology resources as well as any/all personally owned devices that interact in any way with SUNY Broome's information technology resources.

d. Please read the following carefully prior to using your SUNY Broome Computer Account. This is a legally binding document.

e. All terms and conditions as stated in this document are applicable to SUNY Broome. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of New York and the United States of America. Violations that break state or federal laws are subject to prosecution.

f. SUNY Broome makes no warranties of any kind, whether expressed or implied, for the service it is providing. SUNY Broome will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via SUNY Broome is at your own risk. SUNY Broome specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Back to top

Definitions (Applicable to this policy)

a. “Information Technology Resources” – All computers, printers, communication devices, networks, servers, wiring, and other technologies or devices that are managed, maintained, and/or provided by SUNY Broome.

b. “Confidentiality” - Assurance that information is shared only among authorized persons or organizations.

c. “Integrity” - Assurance that the information is authentic and complete.

d. “Availability” - Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

e. “SUNY Broome’s Campus” – Any buildings/facilities, parking lots, and/or land belonging to or used by SUNY Broome.

f. “Personally Owned Devices” – Any device that is owned by a person or company other than SUNY Broome. This includes, but is not limited to: computers, laptops, tablets, PDAs, smart phones, portable hard drives, thumb drives, or any other network device.

g. “Authorized User” – Any user that has been provided with a username and password for the purposes of pursuing their education or employment through the use SUNY Broome’s information technology resources.

h. “Guest User” or “Third Party” – Any temporary employee, contractor, vendor, agent or visitor not registered as a SUNY Broome staff member or student.

Back to top

Rights and Responsibilities

a. Access to and/or use of SUNY Broome's information technology resources is a privilege, *not a right*, and as such may be revoked should circumstances warrant such an action.

b. Any person issued a username and password in order to access SUNY Broome's information technology resources is responsible for all activity that takes place with that account. It is prohibited to let another person use your username and password. DON'T give your password to any other person.

c. All users of SUNY Broome information technology resources are obligated to manage and use institutional data in a manner that is compliant with all applicable laws and regulations.

d. All users of SUNY Broome information technology resources must respect the work product and copyrights of others.

e. As a user of SUNY Broome's information technology resources, it is your responsibility to notify the administrator (administrator@sunybroome.edu) if any violations are observed.

f. SUNY Broome Information Technology users who violate this policy may be denied access to institutional data and systems and be subject to other penalties and disciplinary action.

Back to top

Password Guidelines

Passwords are an important aspect of computer systems security. They are the first line of protection for user accounts. A poorly chosen password may result in a serious breach.

As such, all SUNY Broome employees and students (including contractors and vendors with access to SUNY Broome systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

a. A password should not be easily guessed and should be difficult to figure out.

b. Don't use your name, birthday, address, or other obvious information that could be easily found out.

c. Passwords must:

1.1. Be 8 digits in length
1.2. Include at least one capital letter
1.3. Include at least one number
1.4. Include at least one special character

d. Change your password every 120 days.

e. New passwords cannot be any of your previous 4 passwords.

f. Passwords must not be inserted into email messages or other forms of electronic communication.

g. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

h. Do not share your passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Back to top

Acceptable Uses

This section sets forth the standards by which all students, faculty, staff and authorized guests may use their assigned computer accounts, email services and the shared network. The use of SUNY Broome's computer and network resources including all electronic communication systems and equipment is a revocable privilege.

a. The Office of Information Technology grants access in the form of computer accounts to registered students, faculty, staff and others as appropriate for such purposes as research, education or administration. All access is denied unless expressly granted or joining the guest network.

b. The purpose of a computer account is to support educational initiatives and SUNY Broome campus services by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and/or academic research. Transmission of any material in violation of any U.S. or state regulation is prohibited.

c. Authorized users may connect personally owned devices to SUNY Broome's wireless network provided that they have an active anti-virus software program and the latest operating system patches running on the device.

Back to top

User Responsibilities

The following activities are specifically prohibited. Access to SUNY Broome's information technology resources may be revoked if an account is used in an unacceptable way. Unacceptable uses include, but are not limited to:

a. Attaching any personal computer via any cable to the SUNY Broome network.

b. Disconnecting a network cable from any computer.

c. Playing video games on or through the use of any of SUNY Broome's information technology resources.

d. Viewing or accessing offensive material. Any material may be considered offensive in nature if someone experiencing/witnessing it, whether intentional or not, is offended by it.

e. Viewing, watching, or listening to any explicit/obscene material. This includes, but is not limited to, pornography and other such material. In some cases, simply possessing the material is illegal (ex. child pornography).

f. Attaching any unauthorized network devices or extenders to the wired or wireless campus network.

g. Transmitting any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.

h. Use for product advertisement, political lobbying and activities deemed illegal by law, are strictly prohibited.

Users may NOT:

1. Give your password to or offer your SUNY Broome Computer Account to anyone. Remember, you are responsible for any activities associated with your account. Administrators, employees or other students should never ask for or be given your password. Under no circumstances should you give your account access information to anyone or log in as anyone else.

2. Install any software on any SUNY Broome Computer. This includes remote control software such as: GOTOMYPC, TeamViewer, etc.

3. Break in, attempt to break, or use a SUNY Broome account that is not assigned to you.

4. Create, share, or distribute computer viruses.

5. Set up a server on the network or use the network for any unapproved purpose.

6. Do not save work or school files on any computer. Use the network Z: drive (provided by SUNY Broome); or if the data is not confidential use removable media or Google drive.

7. Never save confidential data or data with personably identifiable information on any portable device or laptop that is not encrypted, or on a cloud service such as dropbox, idrive, etc.

8. Attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization.

9. Attempt to intercept, monitor, forge, alter or destroy other Users' communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of the owner.

10. Attempt to bypass computer or network security mechanisms. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt. The unauthorized scanning of the SUNY Broome Network is also prohibited.

Back to top

Monitoring

SUNY Broome reserves the right to review and/or monitor any emails, data or transmissions sent or received through the SUNY Broome network, at its sole discretion.

Penalties for violating the this policy may include restricted access or loss of access to the SUNY Broome Network, termination and/or expulsion from SUNY Broome and in some cases, civil and/or criminal liability.

Back to top

Penalties / Laws

By logging into your account, each person agrees to abide by and comply with ALL the Terms and Conditions set forth in this document and in the Digital Millennium Copyright Act.

Failing to follow any guidelines that are outlined in this policy could result in access being denied, disciplinary actions, and/or legal action if such is warranted.

SUNY Broome does not protect anyone in violation of New York State, Penal code 156 - Computer Crimes or other local, state, or federal laws that may or may not be listed in this policy.

Back to top

Some Laws Described

Family Education Rights and Privacy Act (FERPA)
FERPA is a federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing "personally identifiable education information," such as grades or financial aid information, without the student's written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action, the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law. (FERPA)

Electronic Communications Privacy Act (ECPA)
The ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications. In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA. (http://epic.org/privacy/ecpa/)

Computer Fraud and Abuse Act (CFAA)
The CFAA criminalizes unauthorized access to a "protected computer" with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. In light of the "interstate or foreign commerce" criterion, the act of "hacking" into a secure web site from an out-of-state computer, which may have occurred when the Princeton admissions officer accessed Yale's "secure" web site, could be considered a CFAA violation (although both schools took pains to say that they were not seeking any civil or criminal prosecutions). The fact that both ECPA and CFAA are criminal statutes considerably raises the ante. (CFAA)

USA Patriot Act
The USA PATRIOT Act, passed six weeks after September 11, 2001, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA), in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of

law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can seize with a court order certain business records pursuant to an investigation of "international terrorism or other clandestine intelligence activities," and record-keepers are prohibited from disclosing the FBI's action to anyone "other than those persons necessary to produce the tangible [records] . . . ." The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources - thus, librarians may not even reveal that an inquiry has been made. (http://www.justice.gov/archive/ll/highlights.htm)

Digital Millennium Copyright Act (DMCA)
The 1998 enactment of the Digital Millennium Copyright Act (DMCA) represents the most comprehensive reform of United States copyright law in a generation. The DMCA seeks to update U.S. copyright law for the digital age in preparation for ratification of the World Intellectual Property Organization (WIPO) treaties. Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability (including details on safe harbors, damages, and "notice and takedown" practices). (http://www.copyright.gov/legislation/dmca.pdf)

Health Insurance Portability and Accountability Act (HIPAA)
Health Insurance Portability and Accountability Act of 1996: U.S. government legislation that ensures a person's right to buy health insurance after losing a job, establishes standards for electronic medical records, and protects the privacy of a patient's health information.

Back to top

Third Party Access

This section of the policy defines the standards for all third parties seeking to access the SUNY Broome network. It also serves to minimize the potential exposure to the SUNY Broome from risks associated with Third Party Access.

Being a SUNY Broome enterprise, SUNY Broome maintains a monolithic network infrastructure. The community expects ease of use and easy access to the SUNY Broome network as it is primarily a teaching and learning network and not designed for PCI compliance nor access by non-SUNY Broome entities.

Therefore, access to the SUNY Broome data infrastructure, either locally or remotely, by third party entities is prohibited. These parties may bring their own network, (BYON) if desired. Example 3G/4G Cradlepoint routers, Time-Warner Road Runner. These parallel networks will not be directly connected to the campus network in any manner and are completely supported and paid for by the vendor.

In the event that the information technology services management grants access for a Third Party to the SUNY Broome network, the Third Party must agree to the following policies and procedures;

a. Compliance with this published Network Use Policy.

b. The right of the SUNY Broome to monitor and revoke user activity.

c. Responsibilities with respect to legislation including but not limited to the Data Protection Act.

d. The right to audit contractual responsibilities.

e. Measures to ensure the return or destruction of information at the end of the contract.

f. An acknowledgement that access to SUNY Broome systems and information will be granted for approved purposes only. The use of this access for personal use or gain is strictly prohibited.

g. When a Third Party is logged into the SUNY Broome network they should not leave the host they are logged onto unattended.

h. Up to date virus checking software must be installed on any relevant devices that are being used to access the SUNY Broome Network or attached devices.

i. The Third Party is solely responsible for ensuring that any username(s) and password(s) that they are granted remain confidential and is not used by unauthorized individuals

j. All hosts that used for remote access to the SUNY Broome network must use the most up-to-date antivirus software and be protected by a corporate or private firewall and not be used by for unauthorized third parted. The systems must be made available for inspection by the SUNY Broome Information Technology service group if requested.

k. All Third Parties must sign and date the Third Party Access Agreement in appendix A prior to authorization.

Back to top

Appendix A - Third Party Access Agreement

1. Introduction

The purpose of this contract is to agree on the conditions for third party access by (**Third Party Name)** to the SUNY Broome data network.

Third party access is defined as all local or remote access to the SUNY Broome Data Network or devices attached to the SUNY Broome network for any purpose.

Access to the SUNY Broome network facilities will not be provided until a signed copy of this contract has been returned to SUNY Broome IT Director/Manager.

2. Access Request

Access to the SUNY Broome network has been requested by (**Requester Name**). The requester has agreed to sponsor the third party company/individual (**Third Party Name**) and takes responsibility for monitoring the third party when accessing the SUNY Broome data network or attached device.

2.1 Access Details

Access is granted to;
(**Specify name and contact details of company/individual**)

Access is granted in the form of;
(WebEx, Teamviewer, Logmein, etc)

Access is granted to the following device(s)/data;
(**Specify Device / Data)**

Remote Access will be granted to;
(**Specify remote access Details)**

3. Security Conditions

The Third Party agrees to and is expected to comply with all relevant security and operational policies (including the Network Use Policy) when connected to the SUNY Broome network.

Signed

_____

_____

Date

_____