3.11.5	COMPUTER AND NETWORK SECURITY AND ACCEPTABLE USE POLICY

Approval Date: May 2009

WHEREAS, the Comptroller's Office audit report with respect to the most recently completed Ulster County Community College audit recommends the creation of Board Policy regarding employee computer and network security policy, and

WHEREAS, the Executive Staff and the Attorney for the College have reviewed the audit recommendation and in turn recommend the amendment of Board Policy to reflect the implementation of the recommendations, now, therefore, be it

RESOLVED, that the attached Computer and Network Security and Acceptable Use Policy hereby is adopted.

Computer and Network Security
and Acceptable Use Policy

1.0 Introduction

SUNY Ulster is committed to protecting employees, students, partners and the College from illegal or damaging actions committed by individuals, either knowingly or unknowingly. The purpose of this policy is to establish basic guidelines for the appropriate use of computing resources (i.e. computers, laptops, electronic mail, the Internet, and related electronic products) at SUNY Ulster.

All Internet/Intranet/Extranet-related systems, wired and wireless, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic services, are the property of SUNY Ulster. These systems are to be used for legitimate

business or academic purposes in serving the mission and goals of the College in the course of normal operations.

Effective security is a team effort involving the participation and support of every SUNY Ulster employee and affiliate who utilizes information and/or information systems. It is the responsibility of every computer user to understand these guidelines, and to conduct their activities accordingly.

2.0 Scope

This policy applies to the following systems:

- All Ulster County Community College ("SUNY Ulster") owned and supported desktop and laptop computers.
- All computers used to access SUNY Ulster Network Resources.
- All voice and data networks, wired and wireless, that are owned and operated by SUNY Ulster, and any equipment directly attached to them (such as personally owned laptops, computers, networking devices, etc.)

This policy applies to the following users:

- Employees, students, contractors, consultants, temporary employees, and guests at SUNY Ulster, including all personnel affiliated with third parties, who are authorized to use the College's computers or networks.

3.0 Acceptable Use

3.1 General Use and Ownership

- Acceptable use of SUNY Ulster's computers or networks is that which serves the mission of the College as defined by the College's administration. Any other use is either neutralc or unacceptable.
- While SUNY Ulster desires to provide a reasonable level of privacy, users should be aware that the data they create whether personal or professional, on the College's systems remains the property of SUNY Ulster. Such data may be requested and possibly disclosed under the Freedom of Information Law (FOIL).
- Due to the need to protect SUNY Ulster's network, the College cannot guarantee the confidentiality of information stored on any computer or network device belonging to SUNY Ulster. Users should not expect, nor does SUNY Ulster guarantee privacy for email or any use of SUNY Ulster's computers and networks, unless such data is protected by Federal, State or Local law.
- All information stored, processed, or transmitted by a user may be monitored, used, or legally disclosed by authorized personnel to others, including law enforcement. Such

monitoring must be conducted properly with a stated purpose, and expose confidential information minimally and only as needed for the stated purpose.

- The President of the college must approve, in writing, the monitoring of any individual's e-mail communications or stored data.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.
- Any information that users know to be sensitive or vulnerable must be encrypted.
- Any information that is considered "Personally Identifiable Information" (PII) and any information that college policy indicates is sensitive or confidential, must be encrypted or otherwise appropriately protected as described in this and other college policies.
- For security and network maintenance purposes, authorized individuals within SUNY Ulster may monitor equipment, systems and network traffic at any time.
- SUNY Ulster reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- SUNY Ulster reserves the right to discard incoming email messages reasonably believed to be unsolicited commercial email ("spam") without notifying the sender or intended recipient.
- For its own protection, the College reserves the right to block all Internet communications from sites, hosts or devices that are involved in disruptive or damaging practices, or that provide services that may expose the College to legal liability.
- In the event that computer or network resources are not sufficient for all current activities, activities that are necessary to the College's mission take priority over those that serve personal interests or are not mission-critical.
- While the Internet provides a wealth of knowledge, there is also a large amount of inaccurate or misinformation on the Internet. SUNY Ulster makes no warranties of any kind for the access being provided, and assumes no responsibility for the quality, availability, accuracy, nature, or reliability of the material.
- SUNY Ulster will not be responsible for any damages suffered by a user resulting from the use of the Internet. Nor will SUNY Ulster be responsible for any unauthorized financial obligations resulting from the use of the Internet.

3.2 Security and Proprietary Information

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Individual users are responsible for any violation of this policy that may originate from his or her computer(s) or account(s).
- Because information contained on portable computers and storage devices is especially vulnerable, special care should be exercised. PII or other sensitive or confidential information must not be stored on laptop hard drives or removable media (including but not limited to floppy disks, PDAs, flash/thumb drives, writable CDs and DVD, portable hard drives).

- Postings by employees from a SUNY Ulster email address to Internet forums should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SUNY Ulster, unless posting is in the course of business duties.
- All devices used by the employee that are connected to SUNY Ulster networks, whether owned by the employee or SUNY Ulster, must be continually executing approved virus-scanning software with a current virus database.
- All devices used by the employee that are connected to SUNY Ulster networks, whether owned by the employee or SUNY Ulster, must have their operating systems and other software fully patched against known security vulnerabilities.
- Mobile computing equipment, such as laptops, must be physically protected from theft and tampering, both on and off campus. Physically lock your laptop when you are not attending to it, even when it is in your office, and when traveling keep it in your personal possession as hand luggage, not as checked luggage whenever possible

3.3. Unacceptable Use
The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (i.e., systems administration staff may have a need to disable the network access of a device if that device is disrupting production services).

Under no circumstances is any user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SUNY Ulster-owned computers or networks.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SUNY Ulster.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or video, and the installation of any copyrighted software for which SUNY Ulster or the end user does not have an active license is strictly prohibited.
- Misrepresenting one's identity or relationship to the College when obtaining or using College computers or networks.

- Modifying or reconfiguring the software or hardware of any College computer or network system without prior notification to, and authorization from, the Office of Information Technology.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a SUNY Ulster computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any SUNY Ulster account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited without prior notification to, and authorization from, the Office of Information Technology.
- Executing any form of network monitoring which will intercept data not intended for the employee's host device, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any device, network or account.
- Interfering with or denying service to any user (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network
- Providing information about, or lists of, SUNY Ulster employees to parties outside SUNY Ulster.
- Using College computers or networks for the purposes of academic dishonesty (plagiarism, cheating, etc).

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email

spam) or who are not directly or indirectly associated with the program or department sending the message.

- Using the College's email system to solicit or advertise personal products, productions or other items or events not related to the College's stated mission and goals, unless the user has obtained prior approval from the Dean of Administration and his or her supervising Dean.
- Any form of harassment via email, telephone, instant messaging, or other electronic means, whether through content, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within SUNY Ulster's networks through other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SUNY Ulster or connected via SUNY Ulster's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- College equipment and communication systems may not be used by employees or authorized users to attempt to influence legislation or in any other way lobby elected officials. Therefore, while the College appreciates and encourages faculty and staff to take an active interest in civic affairs, no college resources may be used in engaging in these efforts.

4.4. Blogging

- Blogging by employees or other authorized users, whether using SUNY Ulster's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of SUNY Ulster's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate SUNY Ulster's policy, is not detrimental to SUNY Ulster's best interests, and does not interfere with an employee's regular work duties. Blogging from SUNY Ulster's systems is also subject to monitoring.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of SUNY Ulster and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by SUNY Ulster's Non-Discrimination and Anti-Harassment policies.
- Employees may also not attribute personal statements, opinions or beliefs to SUNY Ulster when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee must explicitly state that such beliefs and/or opinions are theirs alone and do not represent any position of SUNY Ulster. Employees assume any and all risk associated with blogging.

5.0 Network Access

In order to access the SUNY Ulster Network ("Network") a user must first log onto a SUNY Ulster computer, or connect from a personal computer using the Virtual Private Network ("VPN"). Computer and Network access rights may vary based on the computer or network being used, as follows:

Open lab computers: Computers in Open Labs are available for use by all current State University of New York (SUNY) students, staff, and faculty who present current, valid SUNY Identification.
Access to these computers may also be available to former SUNY Ulster students upon request, subject to other applicable restrictions in this document.

Classroom computers: Classroom computers are accessible to all SUNY Ulster students and faculty scheduled in a class in the room at that time. Student access is restricted to "Student" designated computers.

Office computers: Only active SUNY Ulster employees, who hold a Network Account as described in Section 3.0, are authorized to access faculty and administrative office computers, unless otherwise authorized by the area Dean (or his or her designee) and the Dean of Administration for SUNY Ulster.

Remote (Personal Computers used to access SUNY Ulster Networks): All active SUNY Ulster employees, who hold a Network Account as described in Section 3.0, and have a specific documented business or academic need to do so, are authorized to access SUNY Ulster network resources through Virtual Private Networking (VPN). Authorization from the area Dean (or his or her designee) and the Dean of Administration is required for access to VPN.

Internet-only Wireless: All current SUNY students, staff, faculty, and authorized users with proper SUNY or other appropriate identification.

Employee Wireless: Limited to only pre-configured SUNY Ulster equipment assigned to SUNY Ulster employees.

Internet Only Ports: Active, but undedicated network ports will have Internet-Only access for use by Faculty, staff and other authorized users. To prevent unauthorized access, such ports will require that the user authenticate their identity and register their personally owned computer upon connecting to the port for the first time. Registration is required once every semester.

Patching and Updating: Computers joined to the network Domain will have patches and updates automatically downloaded and installed.

6.0 Accounts

Banner Accounts

Banner Forms ('INB') - All current Active Employees who hold a Network Account, with supervisor approval, are authorized to access those areas of Banner INB in which they have a legitimate business interest.
Logging onto Banner with your own account, for the purpose of providing someone else access to the system, is strictly prohibited.

Access to Banner forms related to the Finance module requires written approval from the area Dean (or his or her designee), and the Dean of Administration.

Self Service Banner (Banner Online) - All SUNY Ulster Employees, past and present, will have access to Banner Online. Former employees' access shall be limited to viewing appropriate information such as historical tax related income forms (i.e. W-2 tax forms).

Network and Email Accounts

The following individuals are authorized to hold active Network Accounts and Email Accounts:

- Current, active employees and students of SUNY Ulster
- Members of the SUNY Ulster Board of Trustees
- Faculty Emeritus/Distinguished Staff of SUNY Ulster
- Others as approved by the appropriate area Dean (or his or her designee) and the Dean Of Administration of SUNY Ulster

Former students of SUNY Ulster may request an active network account that enables them to log onto the open lab computers. Such account access will be active for a period of not more than twelve months. Upon expiration, the former student may request access again.

Account Creation

Network Accounts are created via an automated process when an individual is designated as an employee of SUNY Ulster in Banner, by the Human Resources Department. Upon creation of a new account the employee is mailed their Network Account/Email credentials.

Accounts are typically generated with an email address and an individual User's (U drive) folder. Instructor (T drive) and Department (V drive) must be requested in writing by a supervisor.

Account Deletion

Upon notification to OIT by a department chair, manager, or by Human Resources, an individual's account will be restricted or disabled due to separation of employment or end of affiliation with the College.

Password Protocols
All passwords must meet the following standards to be considered valid:

- A minimum of 6 characters
- Can not contain User/Login Name
- Must contain three of the following four characteristics:
    - At least one upper case character
    - At least one lower case character
    - At least one number
    - At least one symbol

Password Expiration
Existing user password will be set to automatically expire at least twice per calendar year. A newly chosen password must not be the same as the previously used password.

Account Security
A user has five opportunities to enter his or her password. If he or she does not enter the correct password after five tries the account will be locked he or she will be prompted to contact a Network Administrator for a reset.

Logging onto multiple machines
Logging on with your own account, for the purpose of providing someone else access to the computer or network, is strictly prohibited.

Sharing account information
Under no circumstances should a user share any passwords with anyone else.

Locking machines
Users must lock their computers when they leave their work stations.

Connecting personal equipment to the network
Personal equipment is not allowed to be connected to the SUNY Ulster network with the following exceptions:

Virtual Private Network ('VPN') - Computers that connect to the SUNY Ulster networks from offsite using the Virtual Private Network must have virus protection installed and be current with all patches or updates for the operating system and other software. By using VPN, users agree that their computers may be remotely inspected to verify the presence of virus protection and patches or updates. Computers may be denied access via VPN should the virus protection be deemed to be inadequate or it is discovered that patches or updates are missing.

Approval from the area Dean (or his or her designee) and the Dean of Administration is required in order to utilize VPN. A written agreement (available from OIT) setting forth the responsibilities of the remote user must be signed by the employee, the area Dean (or his or her designee) and the Dean of Administration.
Semi-annually, the Executive Staff must review a current list of individuals authorized to utilize VPN.

Internet Only Enabled Ports - Access ports not currently dedicated to a SUNY Ulster computer will be either disabled or configured to allow Internet-only access. Personal computers may be connected to the Internet from these specific locations. Those who connect their personal computer to the Internet using these ports will be required to register their computers using a login and password provided by the Office of Information Technology.

Change of Job Duties
In the event that an employee changes jobs within the college, access to computer network resources related to their old job will be immediately discontinued when they assume their new responsibilities. In the event that access to the resources of their former job is still required, written authorization must be obtained from the supervisor for the former job. Requests to extend such access must include an end date upon which that access is discontinued.

If an employee changes jobs, and either his or her old or new job requires access to any forms within the Banner Finance Module, changes in his or her access to Finance related forms must be requested in writing and approved by the area Dean (or his or her designee) and the Dean of Administration.

7.0 Access Rights

Departmental Resources
Individuals will be granted access to a department's network resources (i.e. V drive) upon written approval from that department's chair or head.

Periodic Review – Semi-annually, a report of all individuals who have access to a department's network resources will be provided to the chair or manager of that department for review. Any irregularities in access rights must be reported to OIT immediately for corrective action. The report must be signed by the supervisor and returned to OIT within 30 days of receipt. Departments that fail to return a signed report will risk losing access to the network and their accounts.

Banner INB Forms
Access to forms in Banner INB will be restricted to only those forms that are explicitly required to perform the duties of the individual's job, as determined by the supervisor of that position.

Periodic Review – Semi-annually, a report of all individuals who report to a given supervisor, and which forms within Banner INB they have access to, will be provided to the supervisor for review. Any irregularities in access rights must be reported to OIT immediately for corrective action. The report must be signed by the supervisor and returned to OIT within 30 days of receipt. Departments that fail to return a signed report will risk losing access to the network and their accounts.

Domain Administrator Access
Domain Administrator level access to computer and network systems shall be granted only to specific OIT personnel as authorized by the Chief Information Officer and the Dean of Administration.

Local Administrator Access
Having local administrator access to a workstation means that a user can install and remove software, including inadvertently installing malicious software such as trojans, viruses, keyloggers, etc. Individuals shall not have local administrator access to any workstation unless there is a documented, necessary, legitimate business or academic need, and unless they have the approval of the area Dean (or his or her designee) and the Dean of Administration. Installation of software on any workstation shall be done by OIT, or by providing temporary local administration access for the duration of the installation.

Boot Devices
Being able to boot a computer from the CD-ROM drive, or any other removable device allows an individual to circumvent security settings and policies in place on that computer and the network it is connected to. Booting from such devices could allow an individual to boot an operating system of their choice, free of any restrictions or controls, and provide opportunity to anonymously launch electronic attacks against SUNY Ulster networks and systems. All SUNY Ulster computers must be configured to prevent booting from peripheral devices, and BIOS or CMOS settings must be password protected to prevent changes to boot device settings. Specific computers may have peripheral boot devices enabled provided there is a documented, necessary, legitimate business or academic need, and there is approval from the area Dean (or his or her designee) and the Dean of Administration.

8.0 Sensitive Data

Sensitive data is defined as any data that could provide access to personal information of an individual or institution. Such data includes, but is not limited to, documents and files that may contain Personally Identifiable Information such as Financial, Human Resources, Payroll and Student Information documents and files.

Personally Identifiable Information (“PII”) is defined as any of the following combined with, and able to be correlated to, a person's name:

- Social Security Numbers,
- Passport Number
- Employee Identification Number
- State or Federally Issued ID numbers (driver's licenses).
- Date of Birth
- Maiden Name
- Mother's Maiden Name
- Credit Card or Financial Account Information
- Results of background or criminal history checks
- Payroll and salary information
- Medical Information
- Accommodation requests and related information
- Biometric data (such as fingerprint, voice print, retina or iris images)
- Digital or other electronic signature files.

Storage of sensitive data
Sensitive data must not be stored on desktop or laptop computer hard drives. Such data must be stored on network servers only, unless approved by the area Dean (or his or her designee) and the Dean of Administration. Storing sensitive data on removable media, such as USB drives, CD-ROMS and DVDs, or in a remote location such as cloud services (i.e. Google Docs), is strictly prohibited.

Transmission of sensitive data
Sensitive data must never be transmitted via insecure means, including email and File Transfer Protocol (FTP) unless the data is first encrypted.

9.0 Violation/Enforcement

Individual users are responsible for any violation of this policy that may originate from his or her computer(s) or account(s). An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of this policy.

Violations of this policy will be taken seriously and may result in disciplinary action, including suspension of privileges, possible termination of employment or expulsion from college, and civil and criminal liability. Violations of some portions of this policy may constitute a criminal offense, and may result in the engagement of appropriate law enforcement authorities.

10.0 Periodic Review

This policy shall be reviewed by the Executive Staff and the Board of Trustees at least once per calendar year.

Adopted May 2009 (09-5-71)
Amended September 21, 2010 (10-9-96)
Amended September 20, 2011 (11-9-143)
Amended March 18, 2014 (14-3-53)