1 USER RESPONSIBILITIES

Effective systems security is a team effort involving the participation and ongoing support of all employees, students, and other individuals who use College IT resources. It is the responsibility of every IT resource user to know IT security requirements and to conduct their activities accordingly. Inappropriate use exposes the College to risks including virus attacks, compromise of network systems and services, damage to reputation, and legal issues.

These policies do not impose restrictions that are contrary to the College’s established culture of sharing, openness, trust, and integrity. However, the College is committed to protecting users and the College from illegal or damaging actions committed by individuals, either knowingly or unknowingly.

1.1 Users are accountable for their actions.

- Users are accountable for activities on College information technology resources accessed via their assigned UserIDs (Netids) and secret passwords. They shall not violate, aid, abet, or act in conspiracy with others to violate College policies or procedures and applicable state and federal law or regulations.

- Users shall abide by College policies and procedures pertaining to information security, confidentiality, and privacy when handling College owned or managed information. Copies of those policies and procedures are maintained on the College website.

- Users are responsible for helping to maintain the security of IT resources and protecting them from unauthorized access and malicious software, such as viruses, Trojan horses, worms, and spyware. Users shall be cautious of all file attachments and consult with the Helpdesk staff for appropriate precautions if they have questions about appropriate precautions to take.

1.2 Passwords will be protected.

- Users shall be continuously aware that all credentials (e.g., the combination of UserIDs, passwords, and/or access tokens) that allow access to any College information, data, or system are explicitly the property of the College and shall only be used for conducting official business.

- Users are responsible for the protection of all passwords, badges, and other Access Tokens. Each person is responsible for protecting the access token(s) assigned to him or her and shall not share the token(s) with anyone else. If a computer password has been compromised or forgotten contact the Helpdesk at
524-8119 for instructions on how it can be reset. If an Access Token has been lost, or stolen, the individual shall report it to their immediate supervisor as soon as possible to avoid unauthorized access or misuse.

- Users may use the same password on internal systems, network devices, or applications, but should not use their internal password for external systems, such as for accounts on an external web site, in case these web sites do not protect passwords in an acceptable manner.

1.3 Incident Response

- Users will contact the Help Desk at 524-8119 if they suspect a security policy violation, system intrusion, virus, or other malicious software on a College system.

1.4 Expectation of privacy

- There shall be no expectation of privacy when using College-owned information technology resources (including computers). Accordingly, users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on any College-owned information technology resources.

- Users shall respect the privacy of others when handling their personal information and shall take appropriate precautions to protect Restricted information transmitted or received via computer networks and other communication devices, not limited to but including faxes, PDAs and smart phones.

1.5 Intellectual property shall be protected.

- Users shall not violate intellectual property laws (this includes copyrights, patents, trademarks, trade secrets, and/or proprietary works) and must abide by the terms and conditions associated with the use of the intellectual property. Violations can include but are not limited to illegally copying, distributing, downloading, and/or uploading information from the Internet (or any electronic source). Examples of commonly copyrighted items are audio materials, movies, videos, software, video games, pictures, and images. Free access to intellectual property does not mean it comes without protection requirements. All applicable software copyright and licensing laws must be followed.

- Users shall not repost personal communications without the author’s prior consent.

1.6 Resources shall be used appropriately

- Users shall not use the Internet to stalk others, post, transmit, request, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable law.

- Users shall not access or attempt to gain access to any computer account to which they are not authorized. Users shall not intercept or attempt to intercept data transmissions of any kind for which they not authorized.
• Users shall not use College IT resources for financial gain or commercial use without prior approval of the President and in no case shall the resources be used for illegal activity. Users shall not use College IT resources for using or accessing pornography, obscenity, profanity, or language offensive to another user. Users shall not use College IT resources to knowingly access material or make individual contacts or communications, which are inappropriate, and of no educational value in the context of the mission of the College.

• Users shall not play games or use software not licensed to the College on College-owned resources.

1.7 E-Mail

• Users shall not send unsolicited commercial advertising or product advertisement for anything other than College official business.

• Users shall not send any type of mass mailing that does not pertain to College business or results in network spamming.

See Attachment A – E-mail Etiquette.

• Electronic mail is a useful tool if it is used wisely. The College encourages its use both for in-college correspondence and over the Internet. No general e-mail is allowed, by that we mean no one is allowed to send e-mail for general distribution to all students, faculty, and staff. Faculty and staff may send to all faculty or all staff but not all students. A unit may want to send an email to all students in a program and that is a valid use. System resources are substantially impacted when general delivery e-mail is used.

• This policy applies to all faculty, staff, and students. Only the president of the College is authorized to allow deviations from this policy. Persons who violate this policy may have their e-mail account deleted.

2 COMMUNICATIONS AND OPERATIONS MANAGEMENT

2.1 Anti-virus (AV) Software Provisioning and Maintenance.

• The College recognizes that the cost to recover from a virus attack is much greater than the cost of prevention, therefore, the College shall provide anti-virus software and the means to keep it up to date, without cost, to their faculty, staff, students, and other authorized users for their remote or on-campus desktop, laptop, or server class computers. In return and as a condition of resource use, on College-provided devices, all users shall have anti-virus software installed, enabled, configured for maximum protection, and up to date at all times if they intend to connect to a College network or network service at any time. If non-College-owned devices connect to the network, the device must have either College-provided or individually-owned up-to-date anti-virus software installed.

• AV software is provided “as is.” Students, faculty, staff, and others installing College-furnished anti-virus software on personal computers shall acknowledge
that the anti-virus software is provided “as is” and that the College has no expressed or implied liability for its use.

- AV software configurations. Anti-virus software should be configured to scan for malicious software at start-up without user intervention. Users shall not exit from this scan nor circumvent the anti-virus configurations. The software shall scan inbound and outbound e-mail and attachments.

- Maintaining current virus definition files. Resource users shall ensure that their anti-virus software is up to date. Virus definition files shall be updated when new definition files (signatures) are released by the software vendor or announced by College OIT. Pre-set configurations to automatically or routinely update signature files shall not be changed or circumvented.

- Personnel who choose to use non-College anti-virus software in their personal PCs (that connect to the College network) shall obtain their AV software, virus signatures and virus removal files from the vendor or reputable source.

2.2 Monitoring

2.2.1 Monitoring and filtering College systems.

The College reserves the right to monitor and filter, at any time, the use of any College owned, controlled, or managed system. Monitoring will be done to ensure that systems are performing as required and that published policies, guidelines, and/or procedures are being followed.

2.2.2 Filtering inbound and outbound Internet traffic.

The College reserves the right to:

- Monitor the use of College systems.
- Identify unacceptable activities and/or instances of misuse, whether malicious or not.
- Collect system audit information to ensure that published policies, standards, and procedures are being followed.

3 ACCESS CONTROL

3.1 Passwords.

User Identification and Authentication are essential to ensure only authorized users obtain information. Identification is a User ID, a sequence of characters that uniquely identifies the person to whom it is assigned. UserIDs typically follow an organizational convention and are quite guessable. Passwords provide Authentication that the person presenting the password is the same person that belongs to the UserID. Passwords are secret and should only be used by the personnel who create them. Users shall be held strictly accountable for any and all activities that occur as a result the use of their UserID.
that is authenticated by the use of their password. Since security tokens and biometrics have not been incorporated to any appreciable level within the College technical environment, the key technical control to ensure authorized personnel get in and unauthorized personnel are kept out is the user-created password. This is why we place great emphasis on the creation and maintenance of strong, secret passwords.

- Passwords shall be constructed in accordance with standards and used to validate the authenticity of the person presenting the UserID.

- When passwords are used as the primary authentication mechanism, they shall be checked by the system when they are created to ensure they adhere to password construction standards.

- Any time the password is reset by someone other than the user, the operating system or database shall prompt the user to change their password before granting access. This includes initial passwords issued by network administrators for the user’s first access.

- When a password expires, a message will be displayed notifying the user that there are X number of grace logins remaining and asking if the user would like to change the password. Users should always answer “Y” to this question.

Note: Names make poor passwords because often they are the name of a spouse, child, or some other easily discernible person. Good passwords are composed of alphabetic, numeric, and special characters. Students are required to follow guidelines for good password creation in order to protect and safeguard College data assets.

- Passwords are personal in nature and should never be written down, or given to another person.

- Passwords shall be at least 8 characters in length and have 3 out of 4 of the following attributes:
  - A letter
  - A number
  - An uppercase
  - A special character

- College systems will permit three (3) consecutive attempts to enter a correct password when the system allows that option. After those 3 attempts, the system shall:
  - Suspended the user’s access privileges until reset by the helpdesk.
  - Temporarily disable the user for no less than three minutes.
ATTACHMENT A - E-MAIL ETIQUETTE

E-mail can become counterproductive when you don’t follow basic e-mail etiquette. Consider the following when using e-mail.

- Don’t send "flame" messages in the heat of anger. After the fact, they are usually regretted.
- If you have bad news to convey, consider not using e-mail.
- If there is a possibility that what you have to say may be misunderstood, consider a communication method other than e-mail.
- Do not make personal remarks about people. Sarcastic or angry e-mail can come back to haunt you. Smiley faces and “just kidding” don’t always undo what has been written.
- Avoid the use of upper case. It is typically synonymous with SHOUTING AT SOMEBODY.
- Craft a relevant subject line and keep to it. If there are other things to discuss, create a new e-mail and subject line.
- When replying, keep only the applicable parts of the original message. Nothing is more annoying that an “I agree” to a long message.
- Don’t forget to say “please” and “thank you”.