ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY RESOURCES

1.0 Overview

Davis College provides its students, faculty, staff and guests (hereinafter referred to as users) with Internet and E-Mail access to help in the fulfillment of job responsibilities and for educational services.

Users must understand that any connection to the Internet offers the opportunity for non-authorized users to view or access school information. Therefore, it is important that all connections be secure, controlled, and monitored.

2.0 Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to Davis College's network are authenticated in an appropriate manner, in compliance with school standards, and are given the least amount of access required to perform their job function or meet their educational needs. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3.0 Scope

The scope of this policy includes all who have access to school-owned or school-provided computers or require access to Davis College's network and/or systems. This policy applies not only to employees and students, but also to guests, contractors, and anyone requiring access to the college's network. Public access to the college's externally-reachable systems, such as its website or public web applications, are specifically excluded from this policy.

4.0 Policy

4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources, the Registrar's Office, or the Student Development Office (in regards to guests) is required.
- Users will be granted the least amount of network access required to perform his or her job function or meet their educational needs.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

4.2 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc)

- Accounts must be password protected (refer to section 4.3 Password Policy for more detailed information).
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.
- Occasionally guests will have a legitimate need for access to the college's network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.
- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the IT Manager or Operations Team, or as required by applicable regulations or third-party agreements.

4.3 Password Policy

All accounts must be password protected. Passwords are unique for each user and are not to be shared with anyone. Appropriate passwords must contain the below information:

- Must be at least eight characters in length.
- Must contain at least one upper case letter.
- Must contain at least one lower case letter.
- Must contain at least one number or special character. Examples of special characters are $, %, @, or * etc.
- May not contain your name. For example, if your name is John Doe, your password can not be John1234.

4.4 Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources and Registrar's Office so that when an employee or student no longer works at or attends Davis College, that account can be disabled. Please refer to Human Resources and the Registrar's Office's policies for more detailed information on how the IT Manager is notified in the event of employment terminations or disenrollment.

4.5 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users should update their antivirus software, as well as other critical software, to the latest version before accessing the network.

Any network access equipment connected to the network in the dormitories or apartments (such as wireless routers, etc) must be secured with a wireless password. Any devices that are broadcasting unencrypted wireless signals will not be allowed access to Davis College's network.

4.6 System Use and Ownership

Users should be aware of the following when using any systems at Davis College and should report any violations to staff, faculty, or a network administrator:

- Users at Davis College should have no expectation of privacy while using college-owned or college-leased equipment. Information passing through or stored on college equipment can and will be monitored. Users should also understand that Davis College maintains the right to monitor and review Internet use, Intranet use, and E-Mail communications sent or received by users as necessary.
- Users are to respect the intended usage of an account. Users are not to use their Davis College provided email account or network access to operate a business unless these activities are approved as a project for the college. These accounts are created for Davis College business or educational use only. In regards to E-Mail, users should not send spam, chain letters, or other mass unsolicited mailings.
- Users are expected to respect and protect the privacy of others. Every user is assigned an account for access to Davis College's systems. This information is not to be shared with others. Also, users are not to use another's account for any reason. Users should not intentionally seek information on, obtain copies of, or modify files or passwords belonging to other users of Davis College, or represent others, unless explicitly authorized to do so by those users. Please refer to the Academic Integrity Policy for more detailed information.
- Users are to respect and protect the integrity, availability, and security of all electronic resources. This includes observing all network security practices as listed in this document. Users should not purposely damage or destroy any resources that do not belong to them without clear permission of its owner. Users shall not intentionally develop or use programs, transactions, data, or processes to harass other users or infiltrate the system or damage or alter the software or data components of a system. Users shall not develop or use any unauthorized mechanisms to alter or avoid charges levied by the college or its providers.
- Users are to respect and protect the intellectual property of others. This includes abiding by copyright laws and not plagiarizing. Most software, music, games, movies and books are copyrighted materials and copies of these should not be created or downloaded using Davis College's systems.
- Users are to respect and practice the principles of community. This includes abiding by Davis College's code of conduct. Users should not intentionally access, transmit, copy or create any material that is illegal or obscene, and they shall not use resources to further

other acts that are criminal. Users shall comply with Davis College policies regarding sexual, racial, and other forms of harassment.

4.7 Consequences for Violation

Davis College network administrators and their authorized employees maintain the right to monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the college's information networks in order to further the health, safety, discipline, or security of any student, employee, or to protect property (physical and intellectual).

Any suspected violations of this policy will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more of the above use regulations, disciplinary action may occur.

- Disciplinary action may include suspension, restriction of access, or more severe penalties up to and including termination of employment (in regards to employees) or expulsion (in regards to students).
- Where illegal activities or theft of college property (physical and intellectual) are suspected, Davis College may report such activities to the applicable authorities.