Nunez Community College
Information Security Policy

INTRODUCTION

Computer information systems and networks are an integral part of business at Nunez Community College. The college has made a substantial investment in human and financial resources to create these systems. All parts of this system - software, storage media, and information about Nunez Community College and its students or its vendors, remain the property of the college at all times.

The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the image of the college.

POLICY

The college provides information technology resources to further the institution's mission of instruction and public service. The ethical use, efficient performance, and safety of this technology rely upon users adhering to established standards of proper conduct in the usage of these resources. This usage should be consistent with the mission of the college and this policy. Generally, each user has a responsibility to obey applicable laws and policies, respect the rights of fellow users, and cooperate with the college in the support and maintenance of computing and network systems.

A. Applicable Laws and Policies – All users are to abide by all applicable federal, state and local laws and regulations, college policies, and policies of the LCTCS Board of Supervisors and the Louisiana Board of Regents. Prohibited activities include but are not limited to the following activities:

- Reproducing, storing and/or distributing copyrighted materials such as photographs, articles or computer software without proper permission.
- Reproducing, storing, creating and/or distributing images, sounds or other type of files that may violate community decency standards.
- Using the college's computer resources for commercial purposes or political campaigning.
- Academic dishonesty.
- Violating policies of other computing systems accessed from Nunez Community College.
- Theft, fraud or other activity that could result in a civil or criminal cause of action.

B. Rights of Users – Every user of college computing resources and the users of other systems deserve respectful treatment. Users must not participate in activities that harass others or invade their privacy. Some specific activities that are not permitted include, but are not limited to:

- Reading, deleting or modifying other people's e-mail, data files or printouts.
- Assuming another's identity in the sending of e-mail, web surfing, etc.
- Posting or e-mailing harassing materials.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.

- Impeding others from accessing their e-mail or data files or usurping their computing resources.

C. Cooperation in Support and Maintenance - Users are expected to refrain from unauthorized activities that might jeopardize the normal, secure, and most efficient operation of information technology at the college. Some specific activities that are not allowed include, but are not limited to:

- Running non-academic/non-administrative processes or software that wastefully consumes system resources or bandwidth, such as Internet radios, streaming video, games, etc.
- Attempting to evade, disable or crack password or other computer and/or network security provisions.
- Knowingly modifying or deleting files essential for the normal operation of the system.
- Installing software or propagating viruses, worms, Trojan horses or other destructive software.
- Vandalizing or theft of hardware, software or documentation.
- Allowing others to use one's own account or participating in other activities that compromise security.
- Modifying or manipulating personal computer workstations or network hardware.

PROCEDURE

The college reserves the right to inspect any and all files stored on college owned systems and to monitor and record computer usage in order to assure compliance with applicable laws and college policies.

The use of college equipment and resources is a privilege and not a right. The college reserves the right to stop unauthorized activity whenever possible, to revoke computing privileges, and to refer offenders to appropriate administrative or student judicial processes. Illegal activities involving technology may also result in referral to law enforcement authorities.

The college may occasionally require new registration and account information from users to continue providing services. Inactivity of an account may result in its being disabled.

The college requires, that upon an employee's leaving for any reason, the immediate return of the original and any copies of any and all software, computer materials, or computer equipment that may have been received from the college This includes items that are either in the employee's possession or those otherwise directly or indirectly under the control of the employee leaving.

The Computer Services Department will prepare and publish (electronically via the college web site) a handbook for Standards and Guidelines for Computer Usage at Nunez Community College. This document will provide additional detail as to the provisions set forth in this policy. This document is to be reviewed and updated annually or more frequently if appropriate.

EXCEPTIONS

None of the provisions of this policy are intended to interfere with academic freedom or other bona fide administrative or academic activity that is consistent with the institution's mission, direction, and goals. Accordingly, with the exception of illegal activity and other issues restricted by law, certain policy provisions may be waived. Approved requests for waiver should be forwarded by the appropriate executive officer in writing to the Director of Computer Services for implementation.

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, the Nunez Community College Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return <u>this page only</u> to the Director of Human Resources for inclusion in your personnel file.
4. Retain the Information Security Policy for your referral.

Signature

By signing below, I agree to the following terms:

i.   I have received and read a copy of the "Information Security Policy" ;

ii.   I agree that any computers, software, and storage media provided to me by the college contains proprietary and confidential information about Nunez Community College and its students or its vendors, and that this is and remains the property of the college at all times;

iii.   I agree that I shall not duplicate (except for backup purposes as part of my job here at Nunez Community College), otherwise disclose, or allow anyone else to duplicate any of this information or software;

iv.   I agree that, if I leave Nunez Community College for any reason, I shall immediately return to the college the original and copies of any and all software, computer materials, or computer equipment that I may have received from the college that is either in my possession or otherwise directly or indirectly under my control.

Employee signature:_____

Employee name:_____

Date: _____

Department: _____