California State University Northridge	**Information Technology** Protection of Confidential and Internal Use of Electronic Information	**Page** 1 of 2	
		SOP#: 500-52	**Revision#:**

Prepared by: Unknown **Date:** April 9, 2003	**Approved by:** Previously approved by President as policy 500-52 **Date:** April 9, 2003
Last revised by: Chris Olsen, ISO **Date:** November 7, 2011	**Last approved by:** Chris Olsen, ISO **Date:** November 7, 2011

1.0 INTRODUCTION

This document establishes uniform, campus wide procedures for protecting all confidential and internal use information in CSUN's custody, and assures compliance with existing CSUN and CSU Information Security Policies. It addresses information that includes, but is not limited to, passwords, confidential stored data, and confidential data that pass over campus networks and the Internet.

2.0 PROCEDURES

- All University personnel are required to be aware of the appropriate Family Educational Rights and Privacy Act (FERPA) regulations and all University policies and procedures regarding confidential and internal use information. These include, but are not limited to, all CSU Information Security Policies, CSUN Information Security Policy, the Acceptable Use Policy, and CSUN Policies and Procedures on Student Records Administration.
- All University Colleges and other Administrative Units must make sure to observe uniform password policies and controls in accordance with University password standards.
- Confidential and internal use information in CSUN's custody, may be copied and temporarily saved only when necessary for the business of the University, -

    - When saved, confidential information must be saved only on an encrypted device that requires authentication and/or password protection and the data itself must be encrypted. All temporary copies must be deleted as soon as they are no longer being used. Computers that contain confidential information must be wiped clean (deleted and erased) when they are no longer in use for that purpose.
    - All confidential data, and private, personal, or sensitive information including passwords, that passes over the campus wireless networks or the campus Internet boundary must be encrypted by employing appropriate encryption software or protocols, such as Virtual Private Network (VPN), Secure Shell (SSH), or HTTPS, that ensures the confidentiality of data transfers. This includes data that is automatically transferred over the network to off-campus vendors.

3.0 APPLICABILITY AND AREAS OF RESPONSIBILITY

- Individual University personnel are responsible to make sure that they understand the regulations, policies and procedures regarding confidential information, including but not limited to private, personal, or sensitive information, and are responsible for using a secure computer and appropriate security software when accessing such information.

- IT is responsible for the maintenance and protection of user accounts and passwords, via the campus directory, and is responsible for providing the appropriate infrastructure for secure network connections, both on campus and across the campus/Internet boundary.

- Local IT units are responsible to insure that all computers, both on and off campus, that are used to access confidential information in CSUN's custody including but not limited to private, personal, or sensitive information, are configured to support proper password maintenance and the appropriate security software, such as Virtual Private Network (VPN) or Secure Shell (SSH). They are responsible to ensure that all computers that contain confidential information are wiped clean of this information when they are no longer in use for that purpose.

4.0 RESOURCES AND REFERENCE MATERIALS

500-10 Use of Computing Resources

500-8025 Privacy of Personal Information

500-8065 Information Asset Management

Family Education Rights and Privacy Act (FERPA)

650-30 Student Records Administration Policy