California State University Northridge	**Information Technology** Desktop Security Lockout	**Page** 1 of 2	
		SOP#: 500-02	**Revision#:**

Prepared by: Unknown **Date:** October, 18, 2004	**Approved by:** Previously approved by President as policy 500-02 **Date:** October 18, 2004
Last revised by: Chris Olsen, ISO **Date:** November 7, 2011	**Last approved by:** Chris Olsen, ISO **Date:** November 7, 2011

1.0 INTRODUCTION

Desktop computers are a key entry point into the Campus' Enterprise systems. The Enterprise systems provide the individual with access to both private and confidential information in addition to the data located on the computer's hard drive. A password-enabled screen saver helps to protect the information displayed on your screen, stored on your computer's hard drive, and the information that is accessible from your computer when you walk away from the desktop computer.

2.0 PROCEDURES

University-issued desktop computers shall be configured to have a password-enabled screen saver. This security- lockout feature shall automatically initiate after the desktop computer remains idle from user interaction for a defined period of time, as follows:
Classroom Computers: The screensaver security-lockout will be invoked after a 1 hour and fifteen minute period of inactivity. The user must then reenter their password to gain access to the computer.
User computers: The screensaver security-lockout will be invoked after a fifteen-minute period of inactivity. The user must then reenter their password to gain access to the computer.

- Users are encouraged to explicitly lock their desktop computer prior to leaving the computer unattended.

The Information Security Officer (or designee) may grant a larger time period in which that security lockout feature is initiated when sufficient security safeguards exist to protect the information accessible from the computer. Such safeguards include (but are not limited to):

- The computer is located within a secure environment.
- The computer is highly restricted to a limited set of functions that do not involve campus protected data systems.

- Local College or department IT units may select an appropriate password-protected screen saver based upon local needs (e.g., a screen-saver with auto-logout capabilities can be configured for open laboratories).

Requests for a larger time period shall be submitted via the IT Help Center (helpcenter@csun.edu).

3.0 APPLICABILITY AND AREAS OF RESPONSIBILITY

Users are responsible for taking steps to protect the information that is viewable on their computer screen, that is located on the computer's hard drive, and that is accessible from the computer. Users are also responsible to maintain and update their passwords in accordance with campus password standards to preserve the integrity of both confidential and sensitive data.

The Information Security Offices (ISO) is responsible for ensuring that the time periods for the security lockout feature are sufficient to meet prevailing standards for data integrity and for ensuring that these standards meet the needs of the Campus.

When an exception is granted, IT is responsible for making appropriate changes to the Enterprise Identity Management system to enable desktop-level screen-saver controls. College and department IT staff are responsible for updating the security protocols on the desktop computer to match the approved time periods.

4.0 RESOURCES AND REFERENCE MATERIALS

500-07 Campus Password Policy

500-10 Use of Computing Resources

500-8045 Network Security and Security of Devices Connecting to the Network

CSU Data Classification