California State University Northridge Information Security	CSUN Desktop Security Guidelines October 16, 2006 **DRAFT**

Overview

California State University Northridge (CSUN) desktops and the information that resides on them are critical assets for the university. These critical assets need to be protected to ensure their availability, confidentiality, and integrity. This document is intended to provide a set of guidelines for the installation of desktops that are part of the CSUN network so that they meet a minimally acceptable level of security. For every operating system, it is important to follow the general guidelines below. The actual details used to implement these guidelines may vary, but the concepts are the same regardless of the operating system.

Guidelines

Before you connect the desktop to the CSUN network for the first time or upgrade to a new operating system, please review the following steps:

Review the purpose or the role of the desktop

1. Determine the purpose or role the desktop will play within the organization

Will the desktop act as a...

   a. "Private" workstation containing and/or working with confidential information
   b. "Private" workstation not containing and/or working with confidential information
   c. "Public" lab workstation

1. When setting up the operating system (OS), look for specific OS configuration options that will enhance the security of the server in this role
2. Ensure that the latest campus-supported stable version of the operating system is running
   a. Windows XP SP2
   b. Mac OSX 10.4.8
3. Harden the operating system (Windows, MAC OS, etc.)
   a. Disable unnecessary services, protocols, and ports

      i. Do not remove programs that are part of the CSUN standard desktop installation

   b. User privileges should be configured as low as possible while still meeting business needs

Determine authentication requirements

1. Use the campus identity management system
    a. CSUN has established a campus identity management system, a unified directory service and authentication infrastructure. It is intended to provide campus departments with a centralized means by which departments can validate users who need or wish to access departmental applications, as well as to obtain authoritative information about users. The infrastructure can be used by applications for public directory service, lookups, authorization, and authentication.
2. All accounts should have strong passwords
3. Local accounts (as opposed to accounts from Active Directory) are strongly discouraged due to the difficulty of managing such accounts centrally
4. Assign a unique account and unique password to each individual to better distinguish activities between multiple users
    a. While shared accounts are generally not allowed, some specific software programs require that such an account exist
        i. Obtain authorization for all exceptions and document them
        ii. Create inventory of any such created accounts and each user that has access it
5. Require re-authentication by users after idle periods

Secure access control

1. Restrict the level of privileges to only those which are necessary for a user to perform their job function
2. An administrator should regularly review the access list or log for users
    a. Look for unexpected rights or changes

Install only required software and keep operating system current

1. Run software that is current. The operating system and other installed software should be supported for the latest security patches
2. When installing software, ensure that only required software is installed, making sure to install the latest versions of all software including all recommended and security patches that are available.
3. Use the automatic update program relevant to the operating system to keep the desktop fully patched – use of a centrally managed patch management solution is preferable

4. After installation, all computers should be routinely maintained and updated
    - This includes the installation of operating system patches and new versions of installed software.

Run minimum number of services

1. Make sure to configure all installed software, disable all unused features and be sure to limit the availability of any features that are enabled
    a. Any user not in the Administrators group should not have access to serve shared files unless a user of the desktop specifically needs
2. Use secure protocols such as RDP or SSH to access the desktop remotely

Configure firewall

1. Configure the firewall that comes with your operating system
    a. The rules should reflect the acceptable use and security policies that have been defined for the computer
2. Operating system filters that deny or permit certain traffic should be used if available
3. Periodically review the filters for inappropriate or unneeded access

Set up and review logs

1. Configure all services so that they log all connections and authentication information
2. Enable local auditing of security events
    a. Changes to user account and permissions
    b. Failed attempts to logon
    c. Failed attempt to access resources
    d. Changes to systems files
    e. Unsuccessful attempts to connect through the firewall
3. An administrator should be assigned the responsibility of monitoring/reviewing and as appropriate following up on possible security violations identified in the system logs – typically these should be reviewed on a monthly basis
    a. For important desktops (eg. Those containing confidential information) this should be as often as weekly

Install security related software

1. Install anti-virus software with daily updating for the latest virus definitions
2. Install anti-spyware software with daily updating for the latest spyware definitions – many current anti-virus solutions also include an anti-spyware element
3. Validate that antivirus definitions and engines are being updated
4. Run security analyzer software such as MSBA from Microsoft
5. SSH, RDP, or other encrypted and secure method of access should be installed if remote access or remote administration services are needed

   - SSH improves the security of user accounts by encrypting all login sessions and allowing the forwarding of X11 and other arbitrary network traffic

1. If the machine is off-site, ensure that the latest Cisco VPN client is installed from the ITR downloads page
   - This allows for a secure connection to the campus from off-site

Maintain physical security

1. Ensure that the desktop is in a locked area when unattended
2. Utilize "keyboard locking" software or password protected screen savers to prevent keyboard activity when the user is not at their computer

Request a network-based vulnerability scan

1. Request a network-based vulnerability scan from CSUN Security to look for common vulnerabilities - these scans are highly recommended for important desktops, such as those containing confidential information
   a. Send requests to security@csun.edu
2. Review and correct vulnerabilities found or implement a risk-mitigation strategy, concentrating first on the items marked as high

Where to go for help

If you have questions or concerns about the security of the data you store, please contact the Information Security department at extension 6100. The Information Security department can make arrangements for security tests to be run on critical servers or desktop machines to identify potential security risks. We can also schedule meetings with departmental IT personnel to talk with security analysts to help them improve the security of the systems they support.