California State University Northridge	**Information Technology** Server Security Baseline Standard	**Page** 1 of 4	
		SOP#: ITIS 90-09-030	**Revision#:** Version 0.7

Prepared by: Leigh Lopez **Date:** May 5, 2009	**Approved by:** Chris Olsen, ISO **Date:** June 8, 2009
Last revised by: Chris Olsen **Date:** June 6, 2009	**Last approved by:** Chris Olsen, ISO **Date:** January 11, 2012

1.0 PURPOSE

California State University, Northridge (CSUN) servers 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.

2.0 SCOPE

This document is intended to provide a minimum-security standard and a set of guidelines for the installation and support of servers that are part of the CSUN network.

3.0 RESPONSIBILITY

	Role (Title)	Responsibility
1	Information Security Officer (ISO)	• The ISO maintains the campus-level server security standards which are based on best practices, and an assessment of the current threats and risks to the University.
2	Information Security Analyst/ Administrator	• Advises server administrators on best practices to secure servers. • Conducts vulnerability assessments prior to servers being deployed.
3	Server Administrators	• Ensures that all existing and new servers are configured to support the minimum standards, or that an alternate plan for risk management is provided. • Requests vulnerability assessments for new servers. Mitigates vulnerabilities.

4.0 STANDARDS

The following security standards apply to servers that connect to the CSUN Network. It is recognized that exceptions may be needed for one or more of the outlined standards. Exceptions will be reviewed and documented by the Information Security Office and mitigating actions will be taken to address risk.

- Use of anti-virus software with up-to-date virus definitions;

- Enable logging and alerting sufficient to identify and track breaches/security incidents;
- Up-to-date vendor/OS/application security patches;
- Host-based firewall to block non-allowed traffic;
- Disable insecure remote access protocols, and use only secure remote-access protocols such as SSH, SFTP, SCP, RDP w/ strong encryption, and VPN;
- Restrict unauthorized physical access by using a screen-saver lock-out after 15-minutes of no activity;
- Prior to deployment, conduct a vulnerability assessment in conjunction with the Information Security Office to identify security vulnerabilities. Remediate or mitigate vulnerabilities.
- Connect to CSUN's Network Time Protocol (NTP) server.
- For Internet-accessible servers, comply with CSUN Policy 500-03, the "Registration of Internet Servers."
- Report security incidents involving the potential breach of server access to the Information Security Office.

<u>Active-Directory Enforced via Root-Level Policy (Windows servers)</u>

- Screen-saver timeout (15 minutes of inactivity);
- Synchronize time to the campus Network Time Protocol (NTP) Server;
- Disable server access following 20 invalid password attempts within a 10 minute period;
- Record logon/logoff events.

5.0 GUIDELINES

It is also important to follow the general guidelines outlined below. The steps to implement these guidelines vary by operating system, but the concepts are the same. Protecting a server from compromise involves 1) securing the underlying OS, 2) the server application(s)/services, and 3) access to the server both physically and via the network to prevent malicious entities from attacking servers or obtaining access to protected information.

- Identify the purpose/role of the server; this will drive decisions regarding access, services, security, recovery, logging, monitoring, and other server parameters.
- Connect to a secure, central authentication system (LDAP, Active Directory);
- Disable "local" accounts unless required;
- Install only required, tested, and where feasible, certified software;

- Limit the number of services/applications to those required;
- Establish a review cycle for event and alert logs;
- Install and configure secure services and protocols;
- Enable backups of critical data/applications and prepare/test business continuity plans;

6.0 DEFINITIONS:

File Transfer Protocol (FTP) – is a network protocol used to exchange and manipulate files over a TCP computer network, such as the Internet.

Secure Copy Protocol (SCP) - is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol.

Secure File Transfer Protocol (SFTP) - SFTP, or secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network.

Secure Shell (SSH) - Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels.

Remote Desktop Protocol (RDP) - is a multi-channel protocol that allows a user to connect to a networked computer.

Virtual Private Network (VPN) - is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks, such as the Internet, as opposed to running across a single private network.

6.0 REFERENCES:

- Digital Media Sanitization Procedure
- Log/Event Management Guidelines
- CSUN Standard – Registration of Internet Devices

7.0 FURTHER INFORMATION:

- Payment Card Industry (PCI) Data Security Standards (DSS)
- These websites and publications have more information on protecting a server from compromise:
  - National Institute of Standards and Technology (NIST)'s Server Security Resource Center – *www.csrc.nist.gov*
  - Risk Management Guide for Information Technology Systems – *www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*

- Guidelines on Securing Public Web Servers – http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities – *www.sans.org/top20*
- United States Server Emergency Readiness Team (US-CERT) – *www.us-cert.gov*
- Center for Internet Security (CIS) – *www.cisecurity.org*
  - A compilation of security configuration actions and settings to "harden" the operating system can be found here:
    - Microsoft Windows (All Versions)
    - Mac OS X
    - Solaris 10
    - Red Hat Linux 1.0
    - Debian
- OnGuard Online – *www.OnGuardOnline.gov*
- IT Compliance Institute – http://www.itcinstitute.com/index.aspx