

IT Security Standard:

SSH Configuration

Introduction

This standard defines configuration elements and procedure for management and use of Secure Shell (SSH) for connecting to the Bellevue College network, as needed to support Bellevue College policy # 5250: Information Technology (IT) Security. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

The use of SSH includes, but is not limited to, the network connections established by college staff accessing shared Internet processors located at Bellevue College and Bellevue College staff telecommuting or providing after-hours support.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat, and Vulnerability Analysis

The network components within the scope of this standard are important infrastructure for protection of the integrity and privacy of the college's data.

Given the importance of protecting the data, the most significant threats are:

1. Malicious and/or unauthorized disclosure of data via eavesdropping (sniffing)
2. Malicious and/or unauthorized disclosure of authentication (login) data via eavesdropping (sniffing)
3. Malicious and/or unauthorized modification of data via insertion, replay, or relaying.

Given the nature of the asset and the nature of the threat, the primary risk associated with these types of threats is unauthorized disclosure of information. This disclosure could lead to compromised computer accounts or release of protected personal information. The associated risks include loss of reputation and potential litigation.

Secondary to these threats is the potential of direct unauthorized modification of the data. While this is not a sophisticated attack, the methods are well-known. The associated risks are the same.

Standard

A. SSH Usage

1. SSH will be used at all times in preference to telnet, ftp, or the Berkley "r" commands. It is recognized, however, that this may not always be possible.
2. SSH may be used to access Bellevue College servers through the firewall (for instance, from home), but those servers accessible in this manner will be limited in number, carefully secured, and monitored by the system administrator(s) or authorized designees.
3. Configuring SSH to perform a password-less login (using the authorized keys file with a null passphrase) will be used for the purposes of automating processes. As this does increase the level of vulnerability and the need for caution, each of these instances will be documented as an exception with the Bellevue College IT Security Administrator and/or Dean of Information Resources (IR). SSH Password-less login will be monitored by the system administrator(s) or authorized designees assigned to the server(s) being accessed.

B. SSH Server Configuration

1. The server will be configured to use only the SSH2 version of the protocol. If necessary, changes to this standard will be noted in a supplemental document "SSH Server Configuration - Exceptions" and changes will later be reflected in the annual review of the standard.
2. The timeout for the initial establishment of a connection (i.e., waiting at a login prompt) will be set to no longer than 300 seconds.
3. The server will be configured to ignore Rhost and all other forms of authentication based solely on hostname or IP address.
4. The server will be configured to ignore (or fail on) access to files that are not properly secured with the correct permissions.
5. The use of privilege separation (if the server supports it) will be required.
6. Direct root logins, via SSH, will not be allowed. They will be over-riden for specific remote command execution, such as backups.
7. Logging will be configured to use the syslog auth facility with a priority of info or greater.
8. Password or Public Key authentication is required.
9. Login banners will be configured to display prior to the login prompt being issued.
10. The "UseLogin" option will be turned off, as there are known vulnerabilities with it. A sample sshd_conf file can be found in Appendix B (below).

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Associate Dean of Student Success (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. SBCTC-IT IT Security Standard: SSH configuration, CIS, 2002

Effective Date: July 2003
Date Last Modified: April 12, 2009

Appendix B – Sample sshd_conf

```
Port 22
Protocol 2
ListenAddress 0.0.0.0
KeepAlive yes
ClientAliveInterval 60
ClientAliveCountMax 5

LoginGraceTime 300
Subsystem sftp /opt/ssh/libexec/sftp-server
# ServerKeyBits 768 # v1 only
# KeyRegenerationInterval 3600 # v1 only

IgnoreRhosts yes
HostbasedAuthentication no
IgnoreUserKnownHosts no
PermitRootLogin forced-commands-only
StrictModes yes
UsePrivilegeSeparation yes

SyslogFacility AUTH
LogLevel INFO

PubkeyAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
# RhostsAuthentication no # v1 only
# RhostsRSAAuthentication yes # v1 only
# RSAAuthentication yes # v1 only
# SkeyAuthentication no
# KbdInteractiveAuthentication yes
# KerberosAuthentication no # Kerberos
# KerberosOrLocalPasswd yes # Kerberos
# KerberosTicketCleanup no # Kerberos
# KerberosTgtPassing yes # Kerberos
# AFSTokenPassing no # AFS authentication

X11Forwarding no
X11DisplayOffset 10

Banner /etc/issue
PrintLastLog yes
PrintMotd yes
UseLogin no
```