

## *IT Security Standard:*

# **Remote Access to Bellevue College Systems**

### **Introduction**

This standard defines the specific requirements for implementing Bellevue College policy # 5250: Information Technology (IT) Security regarding remote access to the Bellevue College internal networks and/or the computers on those networks. This standard will be reviewed on an annual basis or when changes are implemented.

### **Scope**

This standard applies to all remote connections by any means to any Bellevue College network or its constituent components. These components include client and server computers, switching and routing infrastructure, and application and server software. The specific college networks include, but are not limited to, the HP 3000 production processor, the re-hosted environment scheduled to replace the HP 3000, and the administrative and student networks, whether wired or wireless. Temporary networks set up for testing and/or educational purposes are not exempt from this standard; users making remote connections to such networks will comply with all its elements. Nothing in this standard is intended to limit access to Bellevue College resources through appropriately configured web-based applications.

### **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**

Unauthorized access by any means to the Bellevue College computing networks is a serious security threat. Because the components making up the Bellevue College computing networks are critical infrastructure to the daily business and operations of the college, precautions and control mechanisms are in place to prevent such access.

In consideration of the high level of dependence on the Bellevue College networks, protecting these components and limiting access to the data stored, maintained and shared among those components is a top security priority. In light of this need, the most significant threats in providing remote access are:

1. Unauthorized access to data and/or processes, allowing theft of information, fraud or misinformation.
2. Malicious and/or accidental destruction, modification and/or disclosure of critical protected data.
3. Malicious and/or accidental use of remote access to interfere with the operation of Bellevue College systems.
4. Unauthorized modification of networking system components or software.

The primary risk associated with these and other related threats is unauthorized disclosure of information Bellevue College is required to protect, including the personal information of students or staff, and information which could lead to compromise of the network and its accounts. Problems resulting from this kind of disclosure include: loss of the network itself, loss of revenue, loss of reputation and the potential for litigation.

Secondary threats created by granting remote access include the potential for inappropriate use of this state resource, uses inconsistent with the Bellevue College mission, or uses in violation of Bellevue College policies and/or state and/or federal law.

## Standard

### A. Introduction

1. "Remote access" is defined as end-user access to Bellevue College computing resources through a non-state controlled network, device, or medium. Permission to remotely connect to the Bellevue College network is a privilege that may be exercised by Bellevue College network users, and is managed through a Virtual Private Network (VPN).
  - a. Only users holding network accounts and passwords authorized in accordance with Bellevue College policy #5150, Acceptable Use of Bellevue College Networks and Systems will be allowed remote access.
  - b. All remote access will meet the expectations for appropriate use as described in Bellevue College policy #4400, Acceptable Use of State Resources, policy #5150, Acceptable Use of Bellevue College Networks and Systems, and policy #5000, Acceptable Use of Bellevue College Computers.
  - c. Remote access may be terminated at any time for a violation of this standard or if—in the judgment of authorized IT support personnel—the connection puts the Bellevue College network at risk.
  - d. All remote connections to the Bellevue College network will be monitored and logged.
2. The first ("User Access") section of this standard applies to users who wish to access the Bellevue College network remotely. The remaining sections of this standard ("*Virtual Private Network Configuration*" and "*Modem Configuration*") apply to the configuration and support for remote access by IT support personnel.

### B. User Access

#### 1. General Responsibilities

- a. Remote access is contingent upon users assuming certain responsibilities when connecting a remote workstation to the network. These responsibilities include:
  - i. The computer used to access the Bellevue College network will have current, high-quality antivirus software installed and running. Furthermore, virus pattern and signature files will be current, and full disk scans performed frequently.
  - ii. The connecting computer is expected to be running all security patches appropriate for the workstation's software. Updates will be installed in a timely manner, keeping the computer current with both operating system and application patches.
  - iii. The remote computer should have personal firewall software configured and running.
  - iv. The connecting computer is subject to all applicable Bellevue College, State Board for Community and Technical College – IT (SBCTC-IT), and state Department of Information Services (DIS) networking security and acceptable use policies, just as if it were connected directly to the campus network.

- v. One very common use of remote access is to work with files and data stored at Bellevue College. In addition to complying with all requirements of the Bellevue College IT security standard addressing “Data and Database Management”, remote users will:
  - Use extreme care to assure both the confidentiality and integrity of Bellevue College data. Though the Bellevue College VPN connection should be set up to not allow transfer of data to a remote workstation's hard disk, it may be possible to unintentionally transfer data.
  - Whenever possible, sensitive data should not be transferred to the employee's home workstation's hard disk, but rather be accessed on the Bellevue College storage device (e.g., drive, directory, or folder) where it resides.
  - If data must be copied to a remote workstation by any means, either through the remote connection or directly through portable storage media, it will be carefully protected and deleted from the workstation as soon as possible.
- b. Bellevue College IT support personnel may configure a VPN server to manage remote access and to verify that a remotely-connecting computer is up-to-date with all virus software and patches before allowing access to the network.

## 2. Procedure

- a. Authorized users of the Bellevue College network may remotely access a desktop computer **individually assigned** to them without permission from the Dean of Information Resources, under the following conditions:
  - i. From one on-campus computer to another on-campus computer.
  - ii. From a computer off-campus to an on-campus computer through the Bellevue College virtual private network (VPN), provided both the following conditions are met:
    - The software providing the remote access is configured to NOT allow connections between the on-campus computer and the off-campus drives, printers, or peripherals during the remote session, and
    - The user does NOT have access to the HP 3000 from the computer they are accessing remotely (through terminal emulation or database connectivity software such as Minisoft). The user's intent to use or not use the available access to the HP doesn't matter; if the software is installed on the computer to which the connection is made, permission as described below is required.
- b. Individuals assigned to a shared computer on campus are specifically prohibited from remotely accessing that computer because of the impact remote access has on other users who are accessing the computer.
- c. A task must be submitted to Request Center before any remote access may be configured.
- d. Only software built into the operating system (or Bellevue College's VPN solution) can be used to make remote connections to the Bellevue College network. No third party applications of any type (PCAnywhere, GotomyPC, VNC\*\*\*, etc.) may be used.
- e. No one other than the authorized Bellevue College user may utilize any remote access to Bellevue College systems.
- f. Printing, saving or copying of any confidential or sensitive data to the computer used to remotely access a Bellevue College computer is expressly prohibited.

**g. Restricted Information Access**

- i. In addition to meeting the general criteria described above, individuals with HP 3000 terminal emulation or database connectivity software installed on their desktop must have approval from their **Vice President (or higher)** and the **Dean of Information Resources** before remote access will be configured.
- ii. Such remote access for an individual with HP software installed on their desktop must be requested using the "Remote Access to Bellevue College Systems Request Form".
- h. As a standing exception, remote connections are allowed for IR IT support personnel performing official duties, following appropriate procedures.

**3. Non-Employee access**

**a. Students**

- i. Students will not be granted remote access to any Bellevue College systems from off-campus unless requested by a faculty member as a part of the standard curriculum for a specific course. Such access will be configured and documented as an exception to this standard under the direction of the Network Server Group.

**b. Others**

- i. Once regular access to Bellevue College systems has been appropriately authorized by complying with the Bellevue College IT security standard addressing "Non-Employee Access to Bellevue College Systems," non-employees may in some circumstances be granted remote access to the Bellevue College network to perform services for the college.
- c. All remote access by non-employees will follow the user access and configuration standards established in this standard, but must be specifically approved by the Dean of Information Resources or an authorized designee. All exceptions to this standard for this class of users must be documented before such access is configured or allowed.

**C. Virtual Private Network Configuration**

- 1. All VPN connections will be configured as follows:
  - a. VPN solutions implemented at Bellevue College will use industry standard protocols.
  - b. All VPN solutions will be configured to require a centralized authentication and validation process before granting access, such as a log-in name and password.
  - c. If the VPN connection to the college is lost or disconnected for more than 120 seconds, the VPN session will be terminated. This connection timeout occurring because of a non-responsive VPN device is based on loss of the signal from the device, not on user idle time.
  - d. The standard Bellevue College login banner will be displayed to the workstation VPN endpoint at the startup of the VPN client software. If a user acknowledgement option such as clicking on an O.K. button is available, it will be enabled.
  - e. Logs of all remote connections will be maintained, including records of all unsuccessful password or authorization code access attempts.
  - f. Security measures established to mitigate the threat or risk posed by allowing remote access must not be subject to end user modification.
- 2. **Administrative User VPN Access to HP 3000 at SBCTC-IT**
  - a. Bellevue College's HP 3000 server under the control of the SBCTC-IT is remotely accessed by VPN. Because of this, Bellevue College employees will adhere to the standards and procedures identified in the SBCTC-IT security standard addressing "Virtual Private Network Configuration" in addition to following this standard.

- i. SBCTC-IT will give Bellevue College a unique group for authentication to access the HP3000.
- ii. The authentication group is restricted to a specific range of source IP addresses associated with Bellevue College. SBCTC-IT expects this range to be defined as restrictively as possible and limited to just administrative applications users.
- iii. The workstation VPN endpoint, via the assigned group membership, will be allowed to connect only to the Bellevue College HP3000 production processor at SBCTC-IT.
- iv. The Bellevue College group will have a unique password (shared secret) used for authenticating to the SBCTC-IT VPN endpoint. (CISCO VPN only)
  1. The authentication scheme used will be shared secret.
  2. Passwords (group authentication shared secrets) will be random character strings of 28 to 32 characters in length.
  3. Passwords (the shared secret) will be changed every six months.
  4. Passwords will be distributed via a secure channel to designated staff at the college for implementation at the endpoint workstation.
- v. Administrative users on campus may have access to the Bellevue College network while connected to the SBCTC-IT through the VPN—this is often referred to as 'split-tunnel' mode. Given that professional systems administrators on the campus manage the workstation VPN endpoint, this is considered an acceptable risk. Off-campus connections will not have this ability.
- vi. When making authorized off-campus access to the HP, an administrative user connecting from a remote computer will be prompted by the VPN server for a user name and password, and the VPN server will give the user a local IP within the authorized range and connect them to the HP3000.

### 3. VPN Access to Bellevue College Internal Network

- a. The remotely connecting computer will be allowed to connect to the Bellevue College internal network as a VPN endpoint. The Bellevue College endpoint of the VPN tunnel will terminate on a protected subnet. This protected subnet will be granted fairly liberal access to the Bellevue College internal networks, but will be appropriately filtered.
- b. Radius type authentication (user-ID and password, at a minimum) will be required. This will be NT account-level authentication which meets the strong password expectations identified in the Bellevue College IT security standard addressing "*Password Management*."
- c. Bellevue College will use Encapsulating Security Payload (ESP) mode of IPsec, using a Triple-DES or stronger encryption algorithm.
- d. The connecting computer will not be allowed to have direct access to the Internet via means other than through the VPN—this is often referred to as "non-split tunnel" mode.

## D. Modem Configuration

1. Because of the high level of security risk they present, few modems remain deployed at Bellevue College. Dial-up ports may be used only if there is no other way to satisfy a business need, and all modem connections will be approved by the Dean of Information Resources and/or an authorized designee. Dial-up connections through a modem may not be used as a general connection granting remote users access to the Bellevue College network in place of the college VPN solution.

## 2. General

- a. Modems will only be set-up and maintained by authorized Bellevue College IT support personnel, in compliance with this standard. Installation and modem change management will adhere to the Bellevue College IT security standard addressing "Network Device Configuration." No other users may establish modem connections to or from a computer on the Bellevue College network.
- b. Only users holding network accounts and passwords authorized in accordance with the Bellevue College "Acceptable Use of Bellevue College Networks and Systems" policy will be allowed access to dial-up connections. Choice of secure passwords for modems and management of those passwords will adhere to the Bellevue College IT security standard addressing "Password Management."
- c. IR will maintain and review a log of remote connections made through dial-up modems.
- d. If dial-up is used, all security features (dial back, etc.) appropriate to the operating environment shall be used.

## 3. Modem Access Technology

- a. The following four types of modem installations are allowed to be installed, when appropriately approved and configured:
  - i. Direct Host-Terminal Connections
    - This is a connection with a host through a standard character-based port on the host, and is frequently used by vendor organizations providing emergency access for support contracts.
    - This type of connection can also be used for emergency maintenance modems established to provide access to systems if the primary network fails and can only communicate through a serial line. All such connections will use the existing host user authentication mechanisms.
  - ii. American Standard Code for Information Interchange (ASCII) Terminal Servers
    - A terminal server is essentially a serial-to-IP (Internet Protocol) multiplexer, sometimes in the form of a Data Terminal Controller (DTC). Bellevue College has a DTC used to connect to the HP 3000 host through a modem via an Ethernet segment, with all serial connections routed directly to the host. This DTC has multiple serial ports to which modems have been attached, essentially making it a bank of direct host-access serial ports, as described above.
    - However, the terminal server is not the destination host; users connect to the destination host using common IP communications protocols. When users dial into one of the modems, they are authenticated using the existing host user-authentication mechanisms in addition to an additional remote access DTC password.
  - iii. Remote Access Servers (RAS)
    - A RAS device is special-purpose networking equipment specifically designed to support remote or mobile computing. As with a terminal server, the RAS supports multiple dial-in modems.
    - A RAS will handle static and dynamic IP allocations, Automatic Number Identification (if supported), as well as additional security mechanisms such as Remote Authentication Dial In User Service (RADIUS) authentication.

iv. Dial-out modems connected to desktop computers

- In some very rare incidents a specific computer needs to be connected directly to a vendor or outside support source. If this type of connection is configured, the modem should be connected only to outbound analog lines.
- An outbound-only analog line is accomplished by disabling the Direct Inbound Dialing (DID) feature at the Bellevue College telephone switch when the analog line is installed. In addition, only approved remote sites will be accessed by this dial-out modem.

## 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. VPN Client Administrator Guide, Cisco, 2002 (Release 3.5.1)
2. SBCTC-IT IT Security Standard: Virtual Private Network Configuration
3. Bellevue College Policy # 4400: “Acceptable Use of State Resources”
4. Bellevue College Policy # 5150: “Acceptable Use of Bellevue College Networks and Systems”
5. Bellevue College Policy # 5000: “Acceptable Use of Bellevue College Computers”
6. Bellevue College Policy # 5250: “Information Technology (IT) Security”
7. Bellevue College IT Security Standard: Password Management
8. Bellevue College IT Security Standard: Network Device Configuration
9. Bellevue College IT Security Standard: Data and Databases Management

Effective Date: May 2006  
Date Last Modified: April 12, 2009