



---

3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • [www.bellevuecollege.edu](http://www.bellevuecollege.edu)

---

## *IT Security Standard:*

# **Non-Employee Access to Bellevue College Systems and Data**

### **Introduction**

This IT Security Standard has been prepared in order to implement the specifics of the Bellevue College IT Security Policy. Bellevue College contracts with third party vendors for specific technology services. The intent of this standard is to define the specific steps needed to implement that policy while allowing legitimate vendor access to Bellevue College systems when required. This standard will be reviewed on an annual basis or when changes are implemented.

### **Scope**

This standard defines specific procedural and configuration elements for allowing third party vendors access to computing resources under Bellevue College administrative control in order to assist them in complying with their (contractual) support agreement. This standard addresses all of the tools and protocols used for network management, including computers, servers, routers, hubs, firewalls, switches, and the interconnecting cables.

Throughout this document the term “vendor” is used to refer to a person or company that the College has contracted with to provide service (most often support services) where the vendor requires access to computers under Bellevue College administrative control. This may include hardware, software, and operating system vendors.

### **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 computing systems within the scope of this standard include critical infrastructure to the daily business and operations of Bellevue College. While not true across the board, some vendor access opens another possibility to jeopardize the integrity of the computer system, or its data. Additionally, some vendor access may require direct access to confidential data.

Given the nature of vendor access, the most significant threats are:

1. Accidental loss of service
2. Malicious and/or unauthorized access for "research"
3. Accidental and/or malicious physical damage to components
4. Theft of information

5. Accidental and/or malicious misconfiguration of computer resources, which create an operational or security flaw

Given the nature of the asset and the nature of the threat, the primary risk associated with vendor access is either loss of service or misconfiguration. Both of these have further associated risks: loss of revenue, dissatisfaction of those to whom Bellevue College provides service, interruption of productive work, and to some degree a loss of reputation. In the event of damaged equipment, there will also be a cost risk for the replacement of that equipment.

## **Standard**

Vendors may, in the performance of their contractual obligations for support services, require access to computer systems managed and maintained by Bellevue College. As a general principle, this access will only be granted as required, will be extremely restrictive, and will be carefully monitored.

### **Vendor Access**

1. Generally, the vendor will not be given system administrator (or equivalent) privileges. Any access granted to the computer system(s) will provide the vendor's support person the least security privilege required to accomplish any task(s).
2. Vendor access will be for a defined and short duration, usually the length of time required to address the specific support incident. After the completion of the task, access will be disabled.
3. If a vendor is given access to "standard" accounts (with a password that is shared among support staff) on a computer system, that password will be changed after the vendor completes the work. If the account is especially sensitive, and/or the access requirements are extended in time, the password will be changed more frequently, in accordance with the Bellevue College IT Security Standard addressing "Password Management."
4. Software installations and/or upgrades to be installed by a vendor will be clearly documented and reviewed by the appropriate Systems Administrator responsible for the resource prior to granting access. This review will occur early in the planning phase, but no later than prior to the coordinating the access to perform the work. If necessary, the Bellevue College IT Security Administrator and/or the Dean of Information Resources will be brought into the planning process.
5. Vendor software installations will not be assumed secure. After a vendor installs or upgrades a product, the responsible IT Systems Administrator will review the application and related software systems to assure both are functioning properly and securely. If defects (functional or security) are found, they will be remedied immediately. If an obvious course of action is not apparent, the system will be returned to a known safe state while a solution is worked through with the vendor and site management
  - a. A known safe state will be achieved in several ways, and will be left to the discretion of the appropriate IT Systems Administrator. Options may include blocking ports at the firewall, disabling services on the computer, uninstalling the update, or restoring the system from backup.
6. To the extent possible, the activities of the vendor will be monitored. This may take many forms depending upon the technology available and the nature of the vendor's work, but could include visual supervision, review of command history, and operating system level processes auditing. All remote access to Bellevue College systems by vendors will be monitored by appropriate IR personnel.

### **Contractual Issues**

1. All vendors will be required to sign the Non-Employee Agreement with Bellevue College prior to gaining access to restricted areas and sensitive data.
2. Support requirements, including computer system access, will be spelled out clearly in the negotiated contract with the vendor. (This may, in some cases, be an appropriate RFP item.)

3. Vendors that have access to potentially sensitive data (e.g., student or employee records) will be required to sign a document that clearly defines Bellevue College's expectations and the vendor's legal obligations regarding the protection of that data.
4. Bellevue College will define procedures to assure that the vendors can perform their contractual obligations as efficiently as possible without putting the security and integrity of the Bellevue College computer systems we at undue risk.

## 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 Dean of Student Services (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. CIS IT Security Standard – Vendor Access to CIS Systems, March 24, 2003
2. Bellevue College Acceptable Use of Bellevue College Computers Policy
3. Bellevue College Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy
4. Bellevue College Acceptable Use of State Resources Policy

Effective Date:	July 2003
Date Last Modified:	July 10, 2009