

IT Security Standard:

Remote Computer Servicing

Introduction

Information Resources (IR) technical support personnel may at times need to connect remotely to a computer assigned to another campus user in order to provide appropriate technical support services and configuration assistance. This standard articulates the expectations required to implement Bellevue College Policy # 5250: *Information Technology (IT) Security* when such remote access is made. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to all users of the Bellevue College network and computing systems, with specific duties and responsibilities placed upon IR technical support personnel. It applies to one-on-one remote access to Bellevue College-owned computers directly connected to the Bellevue College network assigned to individual campus users.

Lab or classroom computers on the Student network and Administrative network computers remotely accessed by IT support personnel in groups for the purpose of software installations and/or for updates to installed software are not subject to the expectations of this standard.

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 computers used on campus to conduct the educational and business functions of the college are a vital part of the overall campus infrastructure. In some cases, users of campus computers have a legal responsibility to protect sensitive and confidential data under their stewardship, thus creating an intrinsic expectation of privacy associated with their use of the computers.

Enabling remote connections allows the individual assigned to the campus computer to be able to access that computer and its data, but also allows anyone with appropriate credentials to access that computer. IR technical support personnel have such credentials and may access computers so configured.

Though Bellevue College has in place policies which communicate the limitations of individual privacy in the use of Bellevue College computers, it is important to clarify appropriate standards and procedures which protect campus computers from unauthorized access and minimize the negative impact of authorized access when it needs to take place for any legitimate support purpose.

Given these challenges, the most significant threats associated with configuring remote access to computers for servicing purposes are:

1. Configuring remote access may leave a computer more vulnerable to damage or malicious use.
2. Malicious and/or unauthorized access to information.
3. Malicious, accidental, and/or unauthorized changes to, or deletion of, configurations or data.

The primary risk associated with these and other related threats with regard to accessing computers on campus remotely for servicing purposes is unauthorized access to student and/or employee data. The practice of remotely accessing Bellevue College computers assigned to employees has additional potential risks associated with it of: loss of revenue, dissatisfaction of employees and those to whom Bellevue College provides services, interruption of productive work, loss of reputation and the potential for litigation.

Standard

A. Introduction

1. Most Bellevue College-owned computers connected to the Bellevue College network have the built-in capacity for their components and/or resources to be accessed from another computer located elsewhere.
2. In general, this capability is not enabled within the standard campus computing configuration because of the inherent vulnerabilities which exist if this capability is maliciously exploited.

B. User Remote Access

1. In some cases, such remote access to computers assigned to them is provided for a user to facilitate their ability to fulfill their college duties. The processes and expectations for providing this type of *user* access are separately articulated in the Bellevue College IT security standard addressing "*Remote Access to Bellevue College Systems.*"

C. Support Personnel Remote Access

1. Remote connections may also be made to any Bellevue College computer by IR technical support personnel for the purpose of maintaining the operation of the system.
 - a. Only individuals assigned as bona-fide IR technical support personnel are authorized to access another campus user's computer remotely.

D. Restrictions

1. Using elevated login rights for any purpose other than to assist an end-user with a problem or in response to a request for assistance is potentially a breach of trust and subject to the sanctions associated with this standard.
2. IR technical support personnel accessing a computer remotely will maintain confidentiality and will not disclose to anyone information that is viewed or accessed when performing remote computer servicing activities, except as allowed in D.4, below.
3. The expectations for appropriate use as described in Bellevue College policies # 4400: *Acceptable Use of State Resources*, # 5150: *Acceptable Use of Bellevue College Networks and Systems* and # 5000: *Acceptable Use of Bellevue College Computers* will be met when IR technical support personnel remotely access a computer for support purposes.
4. In some circumstances, it may be necessary for IR technical support personnel to remotely access a user's computer without following the below process. Nothing in this standard is intended to impinge on the right, responsibility and ability of Bellevue College network system administrators and/or IR technical support personnel to:

- a. Under the direction of the Vice President of Human Resources, the Dean of Information Resources, or the IT Security Administrator, access and/or monitor Bellevue College systems pursuant to investigations conducted under the auspices of Bellevue College Policy # 4400: Acceptable Use of State Resources or any other applicable Bellevue College policy.
- b. Access and/or monitor Bellevue College systems or any data in response to reported or detected security incidents governed by the Bellevue College IT security standard addressing "Intrusion Detection and Incident Response."
- c. Share information with other IT management or IR technical support personnel in the normal course of their duties.

E. Process

1. The process for activating remote control by IR technical support personnel will be:
 - a. User reports a problem to Request Center or to the Help Desk.
 - i. If reported directly to the Help Desk, the IR support technician taking the request for assistance will enter a Request Center task for the user.
 - ii. All remote access by IR technical support personnel to another user's computer should be documented in Request Center.
 - b. Before taking control of a computer remotely, the IR support technician assigned the Request Center task will personally contact the user and arrange a time to perform the operation.
 - i. Some computers on the Administrative network are assigned to multiple individuals and it would not be feasible to contact all users of that computer prior to access. If one user of the computer requests remote assistance it is sufficient permission for IR technical support personnel to assist.
 - ii. Before proceeding, any IR technical support personnel who are unsure of their jurisdiction concerning remote access to any machine should seek appropriate authorization from the Director of Computing Services or designee, or the IT Security Administrator.
 - c. If possible, IR technical support personnel will fix the problem while the user is present at their computer.
 - i. If not possible, the IR support technician will negotiate with the user a time period within which the remote access to the user's computer will take place.
 - ii. If IR technical support personnel remotely access another user's computer while the user is not present, they will subsequently notify the user by Bellevue College e-mail that the access took place, identifying the reason and the date and time of the access.

F. Restrictions

1. While accessing a computer remotely, IR technical support personnel will not browse the system or attempt to gain access to data or areas of the computer that are not associated with the presenting fault or problem. However, if IR technical support personnel inadvertently find data or information that they believe is:
 - a. *Illegal or evidence of a crime* – they will terminate the remote session and immediately notify the Director of Computing Services and the IT Security Administrator.
 - b. *Confidential or sensitive to the computer user* -- they will notify the user and immediately quit the session upon request. A later time to assist will be arranged.

2. Without the specific permission of the file owner, IR technical support personnel will not perform activities that may result in the loss or destruction of information.
 - a. If it is necessary to make changes to user files, it should be done so in a way that preserves the information within the files.
 - b. If a change is necessary to user files, the affected user will be informed of the change and the reason for it as soon as possible.
 - c. Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, IR technical support personnel must not attempt to make the content readable without specific authorization from the owner of the file.
3. Remote control of a computer that has been locked by the user must be authorized by the Director of Computing Services or designee.

G. Remedies

1. Any user whose assigned computer is remotely accessed, who believes that the participating IR technical support personnel have failed to abide by any aspect of this standard may report the matter to the Director of Computing Services and/or the IT Security Administrator for follow-up.
2. Any user who, having reported a failure of IR technical support personnel to abide by this standard, who feels their complaint has not been satisfactorily addressed, may escalate the problem to the Dean of Information Resources.

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. Bellevue College Policy # 4400: *Acceptable Use of State Resources*
2. Bellevue College Policy # 5000: *Acceptable Use of Bellevue College Computers*
3. Bellevue College Policy # 5150: *Acceptable Use of Bellevue College Networks and Systems*
4. Bellevue College Policy # 5250: *Information Technology (IT) Security*
5. Bellevue College IT Security Standard: *Remote Access to Bellevue College Systems*
6. Bellevue College IT Security Standard: *Intrusion Detection and Incident Response*

Effective Date:	June 2009
Date Last Modified:	June 1, 2009