

IT Security Standard:

Technology Partnerships

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding necessary partnerships in technology that the college engages in with outside agencies in order to accomplish its diverse and multifaceted technology mission. This standard is necessary to help assure the integrity and reliability of the Bellevue College internal networks, servers and computers. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the authority for entering into and monitoring those necessary agreements with non-Bellevue College entities that provide technical services or infrastructure supporting the college. It also provides for maintaining the documentation of those technology partnerships. It applies to any Bellevue College employee authorized to represent the college in entering into agreements which affect Bellevue College networks, servers, computing systems, and/or any technical resource on campus.

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

Bellevue College will frequently rely on outside agencies to provide some of the diverse technical services upon which the college relies, such as phone access or access to the Internet. These partnerships are a vital part of the overall technology services used to fulfill the educational, service and administrative missions of the college. Generally, authorized Bellevue College support personnel have total control over the internal networks and computing systems used at the college.

However, outside agencies providing technical services, both externally and/or internally, may need to access these facilities and infrastructure, and may, in fact, have full control over the installation and operation of certain vital components.

Furthermore, persons representing these agencies may have neither the training, nor the understanding of security issues or network integrity that is expected of internal personnel.

Therefore, carefully articulating to outside agencies the Bellevue College IT security policies, standard, and expectations becomes a critical factor in assuring the security of the computing and communications resources under Bellevue College's responsibility. Any misuse of these resources could put college instructional and business systems at great risk.

Given the high level of access and significant responsibilities inherent in these types of partnerships, the most significant threats include:

1. Outside personnel maliciously increasing privileges to include unauthorized systems
2. Malicious and/or unauthorized access to controlling components (e.g., routers, DNS, domain controllers)
3. Malicious and/or unauthorized access to data and or processes for purposes of theft, fraud, and/or misinformation
4. Accidental and/or malicious destruction or disclosure of critical data
5. Accidental and/or malicious loss or denial of vital services
6. Accidental and/or malicious creation of civil liability for damage caused by Bellevue College personnel

Given the nature of the assets affected by these partnerships and the nature of the threat, all risks associated with technology partnerships with outside agencies are very significant, and could cause considerable loss to Bellevue College.

Standard

A. Introduction

1. The Dean of Information Resources, and/or authorized designees, has the authority to enter into any technology partnerships with outside agencies that are necessary to provide the technical services required to allow Bellevue College to fulfill its educational, research, and administrative missions. These partnerships may also be used to facilitate the active exchange of information between Bellevue College and any outside entity.

B. Partnerships

2. All such partnerships will be recorded in a signed document articulating the responsibilities and rights of each party to the agreement.
3. Any shared expectations and individual responsibilities agreed to between the parties involved in the partnership will be clearly identified in the agreement.
4. Technology partnership agreements will inform the non-Bellevue College agency of the expectations and requirements of all Bellevue College IT security policies and standards which specifically relate to the services covered under the partnership.
5. All such partnerships will be in accordance with Bellevue College Policy #4400, Acceptable Use of State Resources, and will not violate any other Bellevue College policy.
6. All technology partnerships will be lawful under any local, state and/or federal law.

C. Documentation

7. If necessary, a letter of understanding defining the security relationship between Bellevue College and the outside agency will be used to supplement any technology partnership agreement.
8. The Bellevue College IT Security Administrator, or an authorized designee, will ensure that copies of all technology partnerships and all supporting documentation are centrally stored and accessible for administrative review.
9. The Bellevue College IT Security Administrator is responsible for maintaining and updating technology partnership agreements, as necessary.

10. All technology partnership agreements and supporting documentation will be reviewed annually by the Bellevue College IT Security Administrator and/or the Dean of Information Resources.

D. Additional Agreements

1. Other administrative representatives of Bellevue College may also be authorized by the President of the college to enter into various kinds of partnership agreements with outside agencies.
2. If any of these agreements have a technical or technology component, or create a responsibility for Bellevue College technical support personnel to provide services, the agreement will be made in consultation with the Bellevue College IT Security Administrator and/or the Dean of Information Resources.
3. Such agreements will be documented as described in this standard.
4. Copies of these agreements will be retained by the office of the Bellevue College IT Security Administrator and/or the Dean of Information Resources even though the agreement may not have been initiated there.

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*

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