



IT Security Standard:

Employee Security Training

Introduction

This standard defines the steps necessary to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding employee security awareness and training. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the security training and awareness programs implemented at Bellevue College for its staff.

For the purposes of this document Bellevue College staff members and non-Bellevue College staff (e.g., contractors) having access to Bellevue College network systems will be treated the same. All references to "staff" in this document will include both groups, unless specifically noted otherwise.

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, 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 (IR), 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

This standard does not address risk as much as it addresses improving the understanding of Bellevue College staff with regard to its responsibilities in mitigating the IT security risks faced. Increasing staff awareness of security, and encouraging participation in related training, will assist Bellevue College in maintaining a lower level of risk, vulnerability, and/or threat to Bellevue College computing resources.

Standard

A. Security Awareness Program

1. Each staff member will undergo an initial IT security awareness briefing within three months of being hired.
2. Sufficient time will be made available for staff to periodically participate in security awareness briefings.

3. The Bellevue College IT Security Administrator or an authorized designee will be responsible for administering the Bellevue College Security Awareness Program, for documenting employee participation in the program, and for maintaining records of training.

B. Policy and Standards Awareness

1. At least annually, Bellevue College staff will be required to review the Bellevue College IT security policies and standards. Sufficient time will be made available for staff to do this.
2. Bellevue College staff will be required to review some documents in their entirety; for other documents, a summary will be provided.
3. The Bellevue College IT Security Administrator, or an authorized designee, will determine when a summary is appropriate and will prepare those documents where needed.

C. Security Training

1. The Bellevue College IT Security Administrator or an authorized designee will maintain a resource list of security courses, programs, and conferences available to the staff since training will be part of the annual evaluation of all IT employees.

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 Policy, January 29, 2003
2. SBCTC-IT IT Security Standard – *Employee Training*, December 19, 2002
3. Bellevue College Policy #5250 – *Information Technology (IT) Security*
4. Rudolph, Warshawsky, Numkin, *Chapter 29 -- Security Awareness of Computer Security Handbook, 4th Edition*, (Bosworth, Kabay, Editors), 2001

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