

IT Security Standard:

IT Support Personnel

Introduction

This standard defines the specific steps necessary to implement Bellevue College policy # 5250: Information Technology (IT) Security and other policies and standards as they relate to Information Technology (IT) support personnel issues. This in no way is meant to supersede Bellevue College's personnel policies, but rather assembles into one document the security requirements related to support personnel assigned to IT positions at Bellevue College. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This document is intended to augment, not supersede, other Bellevue College personnel policies. This standard applies to the hiring of personnel in IT support positions only and how they are informed of the additional requirements they have to understand and abide by Bellevue College IT Security policies and standards.

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 places a tremendous amount of trust in the honesty and integrity of its IT staff as well as in their technical competence. Bellevue College IT staff design, manage, and support the core services and business applications of the college. If this trust is compromised, either through malicious acts or carelessness, severe damage will be done to all Bellevue College technology resources and systems.

Given the high level of dependence on the IT staff, the most significant threats are:

1. Malicious and/or unauthorized access to data
2. Malicious and/or unauthorized modification of data
3. Accidental modification of data (e.g., while performing support)
4. Theft of equipment or resources
5. Malicious and/or accidental damage to equipment or resources
6. Malicious and/or accidental denial/loss of service

Given the nature of the asset, the nature of the threat and the history of the organization, the primary risk associated with Bellevue College IT staff is loss of service by accident. This loss of service includes the additional risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work and, to some degree, a loss of reputation. Secondary to this threat is the unintentional or incorrect modification of data. This can include such things as severe program bugs or failures and incorrect procedures during recovery or support operations.

Standard

A. Hiring

1. Standard fair hiring practices, as defined by Bellevue College policies, will be followed.
2. Three references will be requested and all three will be contacted. An effort will be made to gain a clear sense of the applicant's competence, levels of prior performance, and personal integrity. These references will be asked to supply additional references who could be contacted for further information relevant to the applicant. Former peers and/or supervisors at places of prior employment will also be contacted.
3. For sensitive positions, such as systems or network administrators or technical supervisors, more complete background checks may be conducted by the Bellevue College Public Safety Office at the request of the Dean of Information Resources. These background checks will include questions concerning the applicant's education, previous employment, and any criminal history.
4. Bellevue College recognizes the high degree of trust it places in its IT staff. This makes the hiring process and probationary period of a new employee critical for assessing the trustworthiness and capabilities of all new IT employees. Careful IT employee screening and review practices per Bellevue College Human Resources procedures and Bellevue College IT security standards will be followed.

B. Contract or Consultant Staff

1. Contract or consultant staff expected to be on-site for any extended period of time will be made aware of, and expected to comply with, the policies and procedures of Bellevue College.
2. If they are granted keys, key cards, or accounts to computer systems, the end of their contract will be treated as an employee separation as defined below.
3. If they are granted an account, it will be configured to expire after 60 days or at the end of the contract whichever comes first. The account may be extended for additional 60-day periods if they are still employed by Bellevue College. Requests for extensions will be made in writing by the Bellevue College administrator who signed the individual's initial Bellevue College Network Account and E-mail Request Form to Information Resources.

C. New Employee Orientation

1. A new hire will be given a basic orientation covering the following procedures, policies, and standards as well as the location of the full collection of documents for future review and reference:
 - a. **Bellevue College Policies**
 - i. #1500– Access to Public Records
 - ii. #2600– Family Education Rights and Privacy Act: Disclosure Of Student Information
 - iii. #3600– Copyright and the Right of Fair Use
 - iv. #4200– Prevention of Discrimination, Harassment and Retaliation
 - v. #4250– Standard of Ethical Conduct
 - vi. #4500– Drug-Free Environment
 - vii. #6900– Records Storage and Disposal
 - b. **Bellevue College IT Security Policies**
 - i. #4400– Acceptable Use of State Resources

- ii. #5000– Acceptable Use of Bellevue College Computers
- iii. #5050– E-mail Usage
- iv. #5100– Software Licensing Compliance
- v. #5150– Acceptable Use of Bellevue College Networks and Systems
- vi. #5200– Student Network Web Space Usage
- vii. #5250– Information Technology (IT) Security
- viii. #5260– Security Breach Notification
- ix. #5300– Computer Labs
- x. #5350– Use of Bellevue College Computer Facilities by Outside Groups

c. Bellevue College Emergency and Public Safety Procedures

- i. Bellevue College Emergency Preparedness Plan
- ii. Policy #6000– Emergency Procedures
- iii. Policy #6250– College Keys
- iv. Policy #6280– Employee Identification

d. Bellevue College IT Security Standards

- i. Security Program and Strategy
- ii. Physical Security
- iii. Security Strategy
- iv. Password Management
- v. Virus Protection
- vi. All Other Bellevue College IT Security standards

e. State Policies

- vii. Whistleblower Program
2. The employee will also receive training regarding the sensitivity to privacy of personal and sensitive data which may be stored on Bellevue College computers.
 3. Copies of these procedures, policies and standards will be provided to new employees in IT classifications. After their review of the documents, new employees will be presented a statement for signature acknowledging that they have read and understand their responsibility for compliance with these policies (See – Information Resource IT Personnel Form). At the discretion of the Dean of Information Resources and/or the individual's immediate supervisor, additional policies may also be included in the initial orientation.

D. Ongoing Training

1. It is the responsibility of each employee to review annually the various procedures, policies, and standards that pertain to ongoing employment with Bellevue College, including those listed in the New Employee Orientation section above. (Also, see the Bellevue College IT security standard addressing "Employee Security Training"). These documents will be provided by the immediate supervisor as needed.
2. Annual evaluations for IT support personnel will identify technical training goals appropriate for their position and responsibilities. Personnel will be encouraged to participate in appropriate technical and security organizations and working groups which will support their individual professional development. In addition, pursuit of professional certifications in technical and security fields are encouraged.

E. Employee Performance Requirements

1. Directors and managers will provide supervision for new employees working in sensitive areas or on sensitive processes.
2. Each employee has the responsibility to ensure appropriate separation of responsibility and adequate audit trails in sensitive areas of work.
3. When reassignment of duties takes place, the manager or director will arrange for any needed security updates.

4. Each employee will be evaluated annually.

F. Separation

1. As noted in other standards, upon separation or being relieved of duties:
 - a. An employee will be required to surrender all keys, key cards, and proximity readers, and
 - b. All account access will be disabled and any shared passwords known by the employee will be changed.
2. All IR directors/supervisors are responsible for notifying the appropriate IT support personnel of their subordinate's separation no later than the day the separation or relief of duties occurs.
3. IR directors/supervisors must follow institutional guidelines regarding retention of any employee data or e-mail. A director/supervisor may access an employee's e-mail or data saved on the individual's hard drive only:
 - a. If voluntarily transferred to them directly by the individual, or
 - b. As authorized by the Human Resources office.
4. It is recommended that mission-critical data and communications generated by IR support personnel be stored and available to supervisors in a shared data-storage location to ensure a smooth transition of responsibilities in the event of an individual's separation.

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. CIS (SBCTC-IT) Personnel Security Standard, December 2002
2. Bellevue College Policies and Procedures Manual
3. Bellevue College Policy #5250: Information Technology (IT) Security
4. Bellevue College IT Security Standard: Employee Security Training
5. Public Law 93-380, The Family Educational Rights and Privacy Act of 1974 (FERPA)

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