

## *IT Security Standard:*

# **Security Program and Strategy**

### **Introduction**

In order to implement the requirements of Bellevue College policy # 5250: *Information Technology (IT) Security*, an IT security program has been created, supported by documented security standards as well as additional Bellevue College policies and procedures. This document describes the security strategy employed by the college and provides an overview to the set of policies, procedures and standards which are the Bellevue College IT Security Program.

This standard defines the specific conventions and procedures employed for the use and maintenance of Bellevue College IT security policies, procedures and standards, which are also guided by the Washington state Department of Information Services IT security policies, procedures and standards. This standard, and each standard created to support the IT Security Policy, will be reviewed on an annual basis or when changes are required and/or implemented.

### **Statutory Authority**

The collection of standards and policies developed to execute the IT Security Program and implement its controlling policy exercise the exemption granted in the Department of Information (DIS) IT Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200.

### **Scope**

This standard applies to all members of the Bellevue College community, with specific duties and responsibilities placed upon the Information Resources (IR) sub-departments. It applies to all campus facilities, IT equipment, and services, as well as off-site data storage, computing and telecommunications equipment.

### **Standard**

#### **A. Bellevue College Security Objectives**

1. Bellevue College recognizes that it operates within in a fairly open technology and networking environment that is typical of most academic institutions. This alters many of the more traditional approaches to securing assets.
2. Bellevue College will implement strong security measures/standards to protect the confidentiality and integrity of the college's data (the most important asset to be protected), to protect the college's computing resources, and to minimize any abusive network behavior originating from our sites.
3. During a security incident, Bellevue College will focus on continuance and restoration of services as opposed to prosecution. Bellevue College will, however, pursue a prosecution course when it is determined to be appropriate. This action will be consistent with Bellevue College's customer service mission.
4. When evaluating protective measures, Bellevue College will look for workable, cost effective solutions that are commensurate with the level of protection required by law.

## **B. Bellevue College Security Strategy**

1. The Bellevue College IT Security Program, through individual IT security standards and policies which address specific elements of the overall security procedures, has been crafted to address security practices for IT personnel, for the users of computer services, and for anyone else who has access to sensitive or confidential Bellevue College information through the technology provided on campus.
2. This section of this document does not replace any specific security standards; its purpose is to define the common assumptions and strategies used within those documents.
3. The policies, procedures and standards under the purview of the Bellevue College IT Security Program will address how Bellevue College ensures secure interactions take place within a technical working environment, consistent with the expectations articulated in the State of Washington Information Services Board (ISB) Information Technology Security Policy, Information Technology Security Guidelines, and Information Technology Security Standards.
4. Emphasized in the policies, procedures and standards which constitute Bellevue College's security program is the importance of preventing unauthorized access, misuse, modification, damage to or loss of IT hardware, software, data, and facilities.
5. The Bellevue College IT security program, in its policies, procedures and standards, has assigned responsibility for IT security and for the installation, monitoring, and enforcement of the security rules and procedures to individuals, groups, and units on campus with appropriate training and background to administer these vital technology functions.
6. Various policies, procedures and standards also address the actions that will be taken for failure to observe the established security rules and procedures.
7. Bellevue College has written standards specifying the physical security arrangements and controls for technology that are appropriate for an institution of its size and function.
8. In support of this security program, Bellevue College has identified a training program that will be used to ensure that all IT personnel, users of computer services, and others having access to sensitive or confidential information are aware of the security practices, policies and procedures at Bellevue College.

## **C. Audience for IT Security Policies, Procedures and Standards**

1. These policies, procedures and standards have a variety of audiences; some are very general and apply to all Bellevue College employees (e.g., *Password Management*); while others are very specific and pertain to a very small subset of the employees (e.g., *Network Device Management*). However, while these documents are organized topically, and may apply to different campus groups at different levels, there is no implied one-to-one relationship between a standard or policy and a specific campus work unit.
2. All Bellevue College employees are responsible for ensuring compliance with all aspects of IT security at Bellevue College with regard to any technology resources they use or manage. Therefore, all employees will be familiar with the full collection of security policies, procedures and standards.

## **D. Bellevue College Security Documentation Process**

1. Bellevue College has developed, and will maintain, standards covering security practices for such areas as: server facilities, computing and networking resources, data management, access controls, software development, incident handling, and personnel.
2. The Bellevue College IT Security Administrator and/or the Dean of Information Resources (IR) are responsible for establishing and maintaining this set of security standards.
3. Once established, each standard will be reviewed at least annually. Regular internal and external assessments will be performed to assure campus compliance with these standards.

4. A process for approval of Bellevue College IT Security policies, procedures and standards and for oversight of changes has been developed, and is illustrated in the flow chart at Appendix B (*IT Security Documentation Approval Process*) of this standard.
  - a. The IT Security Administrator will submit all policy or standards, original or updates, to the IR Review Team for feedback and suggestions.
    - i. The IR Review Team will consist of:
      1. The Dean of Information Resources
      2. The Director of Technology Development and Support
      3. The Director of Computing Services
      4. The Enterprise Support Lead
      5. The Network Support Lead
      6. The Support and Maintenance Lead
      7. Others as assigned by the Dean of IR
  - b. If required, campus units affected by specific policies, procedures and/or standards may be consulted with regard to the establishment and updating of those documents.
  - c. Additionally, the Bellevue College Technology Advisory Committee will participate in the development and updating of all IT security policies, procedures and standards:
    - i. Discussions between IR and the Technology Advisory Committee will be held to identify the need for changes, what the changes are and to provide the committee an opportunity for feedback regarding the changes.
    - ii. In some cases, committee members may take proposed changes to their appropriate campus constituencies for review and feedback.
  - d. Proposed policies or policy changes must also be reviewed by President's staff and in some cases, the All-College Council. The Dean of Information Resources or designee will be responsible for presenting the pending policy to these groups.
  - e. Proposed procedures and standards or changes in procedures and standards may be approved by the Dean of Information Resources or designee.
  - f. All Bellevue College employees will be notified via e-mail any time significant changes have been made to IT security policies, procedures and standards which affect the campus as a whole. At that time, employees will have two weeks to review and comment on a revised standard.
    - i. Comment may be provided directly to the Bellevue College IT Security Administrator and/or the Dean of Information Resources in an e-mail, in a one-on-one format, or in a large group discussion format. This assures that college employees are aware of proposed changes and will have an opportunity to influence the direction of changes to the standards.
    - ii. On rare occasions, mandates or extreme risk levels may dictate a shorter review period or even no review period. At those times, the process will be adjusted to best meet the stated principle.
  - g. After Bellevue College employees have provided their input on proposed IT policy, procedure and standard changes affecting the whole campus, the Bellevue College IT Security Administrator will finalize the new or revised policies, procedures and standards. Employees affected by the policy, procedure or standard will be notified via e-mail that it has been approved and how to access the finalized version.
  - h. A document change history will be maintained for each security standard any time it is in a revision process.

- i. Change notes will be kept at a summary level, but should be clear, concise and meaningful.
- ii. Once an updated version of the standard has been approved and made public, the change history will be removed in favor of an identification of the date last modified.
- iii. The effective date for the standard will continue to be the date the standard was initially approved.

## 5. Changes

- a. If changes to Bellevue College's computing environment or the more general state of computing (best practices, risk, vulnerability or threat) occur, appropriate standards will be modified.
- b. Changes to the security processes, procedures and practices established within the Bellevue College IT Security program will be made and approved by the Dean of Information Resources and/or the Bellevue College IT Security Administrator, or authorized designee.
- c. Review, evaluation, updates and/or changes to the Bellevue College IT Security program and its documents, policies and procedures will generally come as a result of:
  - i. Changes within the Bellevue College computing environment. This includes modifications to:
    1. the physical facilities,
    2. computer hardware/software,
    3. telecommunications networks,
    4. applications systems, or
    5. Internet-based information systems.
  - ii. Mandates from SBCTC-IT or DIS,
  - iii. Mandates from local, state or federal government, or
  - iv. Changes to the type or level of risk associated with the environment in which Bellevue College works. This includes any impact due to organizational and/or budget changes.

## E. Documentation Conventions

1. Each standard will contain, at least, the following sections:
  - a. A brief introduction.
  - b. A statement to define the scope of the standard.
  - c. A statement of whether, and how, exceptions to the standard will be managed.
  - d. A relatively concise description of the business impact as well as a risk, threat and vulnerability analysis.
  - e. The actual standard itself, which may contain subsections.
  - f. A document change log.
  - g. A list of any supporting references.
2. Additional sections may be added as necessary. Because technology exposure and acceptable levels of risk are constantly changing, these documents will also change to match the environment they are expected to address.

## F. Security and Bellevue College Staff

1. Bellevue College recognizes the critical role of all staff in maintaining the secure operation of the college. Employees will have opportunities to learn about the security risks facing the organization as well as the practices employed in mitigating that risk.

2. Bellevue College IR staff will assist in developing, reviewing, accepting, monitoring, and enforcing security standards and practices. These standards will be carefully and clearly written and available to all Bellevue College employees for review and reference.
3. Bellevue College recognizes the high degree of trust it places in its IT staff. This makes the hiring process and probationary period critical for assessing the trustworthiness and capabilities of all new IT employees. Careful employee screening and review practices, in accordance with the Bellevue College personnel policies and the Bellevue College IT Security Standard: "IT Support Personnel", will be followed.

## G. IT Security Administrator Position

1. Bellevue College will maintain an IT Security Administrator position responsible for maintenance and implementation of the Bellevue College IT Security Program and assigned primary oversight of IT security. The purposes, responsibilities and qualifications for an individual assigned to this position are articulated in the Bellevue College IT Security Standard: "Information Technology Security Administrator."

## H. Institutional Reporting

1. The President of Bellevue College, after consulting with the Dean of Information Resources and/or the Bellevue College IT Security Administrator, will provide annual certification to the Information Services Board that Bellevue College's IT Security Program has been developed, implemented, tested and its processes, procedures, policies, standards and practices updated as needed.

## Appendix A – References

1. SBCTC-IT IT Security Standard: Introduction
2. SBCTC-IT IT Security Standard: Security Strategy
3. DIS Information Technology Security Policy (<http://isb.wa.gov/policies/portfolio/400P.doc>)
4. SAO Information Technology Security Policy Audit Standards (<http://www.sao.wa.gov/StateGovernment/ITSecurity/ITStandards.htm>)
5. DIS Information Technology Security Standards (<http://isb.wa.gov/policies/portfolio/401S.doc>)
6. DIS Information Technology Security Guidelines (<http://isb.wa.gov/policies/portfolio/402G.doc>)
7. Appendix A as prepared by the State Auditor's Office, Revised August 20, 2002, Schedule of Compliance Area, Compliance Area for Information Technology Security Policy.
8. Bellevue College Policy # 1250: Formulation and Issuance of College Policies
9. Bellevue College Policy # 5250: Information Technology (IT) Security
10. Bellevue College IT Security Standard: Application Development
11. Bellevue College IT Security Standard: E-Commerce
12. Bellevue College IT Security Standard: Employee Security Training
13. Bellevue College IT Security Standard: Information Technology Security Administrator

Effective Date:	March 2008
Date Last Modified:	April 12, 2009

# Appendix B – IT Security Documentation Approval Process

## Approval Process

### IT Security Documentation

The team consists of the IR Dean, the Director of Technology Development and Support Services, the Director of Computing Services, the Enterprise Support Services Administrator, the Network Support Lead, the IT Security Administrator and others as assigned by the Dean.

