

## *IT Security Standard:*

# **E-Commerce**

### **Introduction**

This standard defines the steps needed to implement Bellevue College policy # 5250: *Information Technology (IT) Security* regarding the management and control of e-commerce at Bellevue College. The standard will be reviewed on an annual basis or when changes are implemented.

### **Scope**

This standard applies to all e-commerce activities at Bellevue College. This includes any campus entity that presents a Web-based presence providing services and collecting revenues. E-commerce will be assumed to be defined in its broadest terms with regard to 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, 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**

A significant amount of data and revenue transactions at Bellevue College are taking place through online interaction between campus units and the customers, clients and students served. As the technologies to securely perform this type of business operations continue to improve, the use of e-commerce at Bellevue College will become a larger part of all service and revenue transactions taking place on campus. Because the technologies involved with e-commerce are still developing, Bellevue College risks losing opportunities to provide services if the hardware, software, and business processes supporting e-commerce activities fail.

The dynamic nature of the Web also increases the chance that Bellevue College may not be able to provide access should systems break down. The web servers and applications that support e-commerce on campus are critical infrastructure to Bellevue College's daily business and operations. Bellevue College e-commerce business functions would be severely impacted by significant network or web server disruption.

Given the increasing level of dependence on web-based service for e-commerce transactions, the most significant threats are:

1. Malicious and/or unauthorized modification to web content.
2. Accidental, malicious and/or unauthorized disclosure, modification or loss of application, or e-commerce transaction data.
3. Malicious misuse or compromise of web servers, resulting in theft of goods or services.

4. Denial of service.

Given the nature of the asset and the nature of the threat, the main risks associated with e-commerce are malicious attacks to infrastructure or denial of services. All of these threats have additional associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and loss of reputation.

## Standard

- A. The various types of e-commerce that take place at Bellevue College make it imperative that the governing standards allow maximum flexibility for the business processes and dealings of the individual units engaged in such activities, while balancing the significant need for security consciousness within these transactions.
- B. Therefore, each individual Bellevue College unit wishing to provide services and collect revenue through e-commerce will be responsible for the development of its own e-commerce presence within the guidelines provided by the Bellevue College IT Security policies, Acceptable Use policies and the Bellevue College IT Security Standards addressing Database Management, Applications Development, Web Servers, and Web Space Usage.
- C. Units creating and maintaining an e-commerce website have the responsibility for ensuring that all transactions carried out within the site are secure transactions. Bellevue College e-commerce site providers will also develop a written plan outlining the security, guidelines, procedures, processes and expectations related to their e-commerce site to the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or authorized designee, who will document the details of the site for recordkeeping, and for maintaining as part of a centralized plan for e-commerce at Bellevue College. This documentation will include standardized records of all e-commerce site URLs, responsible units and website maintainers, as required under the applicable policies and standards, as well as any other information deemed appropriate.
- D. The Bellevue College IT Security Administrator and/or the Dean of Information Resources, or authorized designee, will also be responsible for ensuring adherence to any and all applicable Bellevue College policies and/or IT security standards and for enforcement of all matters related to investigations and sanctions in those policies and standards. Each individual unit's e-commerce plan will be reviewed at least annually.

## 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: Database Management

6. Bellevue College IT Security Standard: Applications Development
7. Bellevue College IT Security Standard: Web Servers
8. Bellevue College IT Security Standard: Web Space Usage

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