

IT Security Standard:

HP Administrative System Access

Introduction

This standard defines the steps needed to implement the Bellevue College policy # 5250: Information Technology (IT) Security for requests to access data stored in the Bellevue College HP Administrative System. This standard is needed to protect the data and records stored in all of these systems on campus. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to all users of the Bellevue College network, whether they are Bellevue College employees, students or non-employees, particularly those who may be authorized access to the Bellevue College HP Administrative System.

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

The use of computing technology to gather and store data is a ubiquitous tool used at Bellevue College. The federal Family Educational Rights and Privacy Act (FERPA) places significant restrictions on the dissemination of the data used at the College.

Given the variety of access available to Bellevue College data and the liability, a violation of the FERPA restrictions would place on the institution, the most significant threats are:

1. Malicious and/or accidental release of sensitive or protected information
2. Malicious and/or unauthorized access to data systems
3. Malicious and/or accidental destruction or disclosure of data
4. Malicious and/or fraudulent manipulation of data

The most significant of these are the destruction, disclosure or manipulation of data. Though historically-proven security processes and tools are in place which mediates this risk, the nature of the threat is high. This is because users can disregard the processes or maliciously access the information. Compliance with this procedure will assure the integrity and reliability of these resources.

Standard

A. General

1. Bellevue College implements policies in compliance with Public Law 93-380, the Family Educational Rights and Privacy Act of 1974 (FERPA). This law establishes that the education records of students attending or having attended the college are confidential and will be released only with written permission of the student. These policies include:
 - a. **Policy #2600: “Family Education Rights and Privacy Act: Disclosure of Student Information”** – Bellevue College has established this policy as the expectations on campus for the handling of education records. All definitions, expectations, and procedures outlined in this policy apply to the use of the campus HP Administrative System to handle those records.
 - b. **Policy #5150: “Acceptable Use of Bellevue College Network and Systems”** – Use of the Bellevue College HP Administrative System will be for the purpose of facilitating the exchange and storage of information, including information on students and/or employees, and is governed by this policy.
 - c. **Policy #4400: “Acceptable Use of State Resources”** – Requires that use of the system will also facilitate compliance with and furtherance of, the education, research, and administrative missions of the college. Utilizing the Bellevue College HP Administrative System for uses and/or communications that are specifically proscribed in this policy, or which violate any other Bellevue College policy and/or state and federal rule or law, is strictly prohibited.
 - d. **Policy #2500: “Access to Public Records”** – This standard also leverages the requirements detailed in this policy with regard to confidentiality, retention and access to public records.
2. When information must be shared outside Bellevue College, written Shared Expectations Agreements will be executed between the college and the information handling entity. Two such standing agreements are appended to this standard:
 - a. Information regarding the agreement with the State Board for Technical and Community Colleges – Information Technology unit (SBCTC-IT) (formally CIS) is at Appendix B.
 - b. Information regarding the agreement with CampusCE can be found at Appendix C.
3. Such agreements will also comply with the requirements of the Bellevue College IT security standard addressing “Non-Employee Access to Bellevue College Systems and Data”, if applicable.

B. Permission for HP Administrative System Use

1. Employees or authorized non-employees must formally request user log-on credentials before accessing a Bellevue College HP Administrative System. There are two steps in this request process, account creation and account configuration:
 - a. **Account Creation**

The administrator or supervisor to whom the individual reports will complete and submit a “Request for Access to HP Administrative System Data” form to Enterprise Support Services (ESS).

 - i. ESS personnel are the Information Resources (IR) staff authorized to create and maintain accounts on the HP Administrative System.
 - ii. No access can be configured until ESS has the completed, authorized form in hand. Once the form has arrived, ESS personnel will create the username and set up a password for the account.

b. Account Configuration

In addition, the requesting administrator or supervisor will contact by e-mail the appropriate authorizing authority, or their designee, for approval regarding the HP screens and fields for which access is to be configured:

- i. For access to student (SMS) information, the e-mail will be sent to the FERPA Officer, or an authorized designee. The Bellevue College FERPA Officer is the Associate Dean of Enrollment Services.
 - ii. For access to financial or facilities information, the e-mail must be sent to the FMS/FAE authorizing authority, or an authorized designee. The authorizing authority for FMS/FAE systems is the Executive Director of Finance.
 - iii. For access to personnel information, the e-mail will be sent to the PPMS authorizing authority, or an authorized designee. The authorizing authority for the PPMS system is the Vice President of Human Resources.
 - iv. **Note:** If the administrator or supervisor is submitting a request to change or update an existing account, the individual's current userid and a list of the changes/additions requested will be included in the e-mail to the appropriate authorizing authority.
2. The authorizing authority or designee will contact ESS staff, identifying the screens authorized for the requesting school official.
 - a. ESS staff will configure the specific authorized access for the user account.
 - i. Once ESS has processed the request, the requesting individual will be e-mailed login instructions, and a userid and password.
 - ii. The approving administrator or supervisor will also be notified that the account has been created and configured.
 - b. The completed form will be maintained on file in a secure location in ESS.

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 #2500: [Access to Public Records](#)
2. Bellevue College Policy #2600: [Family Education Rights And Privacy Act: Disclosure Of Student Information](#)
3. Bellevue College Policy #4400: [Acceptable Use of State Resources](#)
4. Bellevue College Policy #5000: [Acceptable Use of Bellevue College Computers](#)
5. Bellevue College Policy #5150: [Acceptable Use of Bellevue College Networks and Systems](#)

6. Public Law 93-380, the Family Educational Rights and Privacy Act of 1974 (FERPA)
7. Bellevue College IT Security Standard: *Non-Employee Access to Bellevue College Systems*

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

APPENDIX B –

BCC-CIS SHARED EXPECTATIONS FOR OPERATIONAL SECURITY



3000 Landerholm Circle SE, Bellevue WA 98007-6484
Telephone: (425) 564-2301 Fax: (425) 564-2261

Shared Expectations for Operational Security

The Center for Information Services (CIS) and the Washington Community and Technical Colleges (WCTC) share many things in common including networks, applications, reporting responsibilities, and methodologies. This allows for many efficiencies and benefits, but it also increases the level of vulnerability. As provider of computing services for WACTCs, the CIS agrees to protect its operating environment by providing a safe and secure data center for colleges that locate their administrative (Student Management Systems [SMS], Financial Management Systems [FMS], Payroll/Personnel Management Systems [PPMS] and Financial Aid Management System [FAID]) processors at the CIS; and/or that engage the CIS for administrative applications, data support, and technical services. This includes following industry standard best practices for environmental control, backup and recovery, disaster recovery, network access, and security. This document defines, at a high level, the shared expectations between Bellevue Community College (BCC) and the CIS to manage shared operational security risks.

CIS Responsibilities: Bellevue Community College's (BCC) Expectations of the CIS

- The CIS will provide BCC with core business application software applications. To assure the integrity and confidentiality of the data, as well as reliable, correct, and timely processing of that data, the CIS will follow safe and auditable practices throughout its software development, deployment, and maintenance cycle.
- The CIS will provide business applications and technical support to BCC. The CIS recognizes this as a high-risk security area and will work to assure that only trusted staff members are in these roles. These staff members are aware of the importance and sensitivity of the information and safeguard it appropriately.
- In addition, the CIS will provide limited security assistance to BCC in the form of documentation, consultation, incident response and information sharing.

BCC Responsibilities: CIS's Expectations of BCC

- BCC will ensure that the application security provided within the CIS business applications is configured and maintained to provide appropriate access to the data. Further, BCC assures that the various control features and reports within the applications are configured and monitored.
- BCC will respect the partnership between itself and the CIS in assuring the integrity and confidentiality of the data and does not attempt to circumvent security devices or procedures put in place by the CIS.
- BCC recognizes that the WCTC's K20 connection, as well as the connection to the larger Internet, as shared connections pose a security threat to the consortium, and must be protected by member organizations. As a participating member, BCC will take measures to ensure that its network perimeters are adequately protected and that the servers and workstations within its local area networks are secured.
- BCC recognizes that the CIS and the K20 Network Operations Center (NOC) have a responsibility to protect the larger WAN. If necessary to protect the Internet, the WAN, or other WCTC colleges from an incident at one college, the CIS will disable K20 connectivity for the affected college.
- BCC will share appropriate information regarding security issues and incidents with the CIS for the purposes of tracking trends, resolving incidents, and improving the security of the WCTC as a whole.

B. Jean Floten
B. Jean Floten, President, BCC

15 July 2003
Date

Corey Knutsen
Corey Knutsen, Executive Director, CIS

16 July 2003
Date

APPENDIX C –

BCC-CAMPUSCE SHARED EXPECTATIONS FOR OPERATIONAL SECURITY



3000 Landerholm Circle SE, Bellevue WA 98007-6484
Telephone: (425) 564-2301 Fax: (425) 564-2261

Shared Expectations for Operational Security

Bellevue Community College (BCC) and CampusCE share continuing education student registration data. This allows for many efficiencies and benefits that are presently not possible through the Center for Information Services (CIS). However, this also increases the level of vulnerability of our student data. As a provider of continuing education student data to CampusCE, BCC agrees to protect its operating environment by providing a safe and secure data center for transferring data to CampusCE. This includes following industry standard best practices for environment control, backup, and security. This document defines, at a high level, the shared expectation between BCC and CampusCE to manage shared operational security risks.

BCC Responsibilities: CampusCE Expectations of BCC

- BCC will provide CampusCE with core continuing education student registration data. To assure the integrity and confidentiality of the data, as well as reliable, correct, and timely processing of that data, BCC will follow safe and auditable practices throughout its continuing education registration process.
- BCC will provide business applications and technical support to CampusCE. BCC recognizes this as a high-risk security area and will work to assure that only trusted staff members are in these roles. These staff members are aware of the importance and sensitivity of the information and safeguard it appropriately.
- In addition, BCC will provide limited security assistance to CampusCE in the form of documentation, consultation, incident response and information sharing.

CampusCE Responsibilities: BCC's Expectations of CampusCE

- CampusCE will ensure that the application security provided to their server is configured and maintained to provide appropriate access to the data. Further, CampusCE assures that the various control features and reports within the applications are configured and monitored.
- CampusCE will respect the partnership between itself and the BCC in assuring the integrity and confidentiality of the data and will not attempt to circumvent security devices or procedures put in place by BCC or CampusCE.
- CampusCE recognizes that the larger Internet, as shared connections pose a security threat to BCC, and must protect the continuing education student data. CampusCE will take measures to ensure that its network perimeters are adequately protected and that the servers and workstations within its local area networks are secured.
- CampusCE recognizes the responsibility to protect their Internet connection. If necessary to protect BCC student data, CampusCE will disable the connection to their server if their security is breached.
- CampusCE will share appropriate information regarding security issues and incidents with BCC for the purposes of tracking trends, resolving incidents, and improving the security as a whole.

B. Jean Floten, President, BCC

Date

Loren Pace, Chief Operations Officer,
CampusCE

Date