



IT Security Standard:

Video and Television Services

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding the television and video services provided by the college. The necessity of this standard is to assure the integrity and reliability of the services provided, and of the Bellevue College internal networks and computers. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the security measures to be taken to protect the content, media, and delivery systems used by Bellevue College Television Services, both as an individual entity and in partnership with the City of Bellevue.

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

Generally, the contents of the electronic media covered under this standard are intended for dissemination to the public. This means that there is a significantly lessened security concern regarding this content when compared with other standards. However, there are related issues of physical security of the sophisticated equipment used by Bellevue College Television Services and the physical security of the various media used.

There are also related issues of security regarding access to the supporting computing equipment and its presence on Bellevue College networks. Additionally, a significant business partnership exists between Bellevue College and the City of Bellevue with regard to the shared operations and control of the two television channels cablecast from the campus. Any misuse of these resources could put these specific educational and business systems at risk.

Given all these factors, the most significant security threats are:

1. Malicious and/or unauthorized access to computing and cablecast systems.
2. Theft of computing, cablecast, or infrastructure components.
3. Accidental and/or malicious physical damage to computing, cablecast or infrastructure components.
4. Accidental and/or malicious destruction of cablecast storage media and/or data.

5. Interruptions to the operating environment.

Given the character of these specific assets and the nature of the threat, all risks associated with the management of the video and television facilities on campus are fairly nominal, and, at worst, would cause loss of these specific services provided by Bellevue College.

Standard

A. Introduction

1. The Bellevue College Television Services unit produces, for Bellevue College and the City of Bellevue, video content used for educational purposes, general programming, and for historical archival purposes. Two channels are cablecast from Bellevue College via cable only: *The College Channel* and the City of Bellevue channel.

B. Television Facilities Management Committee (TFMC)

2. Bellevue College has a joint ownership agreement with the City of Bellevue which created the Television Facilities Management Committee, comprised of members from both entities. The purpose of the committee is to set the administrative policies and make decisions regarding the management and use of the television production facilities and cablecast through the college and city channels.
 - a. The committee has the responsibility for establishing the schedule, training standards, work standards, and any other standards deemed necessary to carry out the agreement.
 - b. The TFMC will notify the Bellevue College IT Security Administrator and/or the Dean of Information Resources of any changes or updates to the current agreement. These Bellevue College administrators have the responsibility for determining the impact of the agreement as it relates to the Bellevue College IT Security Policy and for addressing with the committee any deviations or exceptions from this standard.
 - c. A copy of the current "*Interlocal Agreement for Co-Location of the City of Bellevue Cable Production Facilities at Bellevue Community College*" will be maintained in the files of the Bellevue College IT Security Administrator and/or Dean of Information Resources.

C. Ownership and Copyright

1. All programming cablecast by Bellevue College is intended for public consumption. Because of this, there are no special security issues regarding privacy and security of content aside from issues of Copyright and Ownership.
 - a. The Director of Television Services will put procedures into place to ensure that all copyrights regarding acquired content cablecast by Bellevue College are appropriately honored and in compliance with industry standards on copyright issues.
 - b. Original programs or works whose content and production are the sole result of the efforts of the City of Bellevue or Bellevue College remain the copyrighted property of that specific entity.
 - c. Copyright of original programming produced cooperatively between the City of Bellevue and Bellevue Community College will be jointly retained by Bellevue College and/or its employees, and the City of Bellevue.
 - d. In the event of a termination of the agreement between the City of Bellevue and Bellevue Community College, all ownership and copyrights jointly held will be transferred in accordance with the provisions of the current "*Interlocal Agreement for Co-location of the City of Bellevue Cable Production Facilities at Bellevue Community College.*"

D. Physical Security

1. All production, cablecast, and storage facilities on campus used by Bellevue College Television Services will be secured by doors which will remain locked at all times, unless attended by authorized Television Services personnel.

2. The primary means of access control is through the use of traditional metal keys that will be individually assigned to authorized Bellevue College employees. These facilities will be accessible to authorized staff via key twenty-four hours a day, 365 days a year.
3. Coded key-pads are also used to limit access to certain rooms and areas. Key code records are maintained by Campus Operations. All procedures and process described in the Bellevue College IT security standard addressing "Physical Security" related to distribution and control of key codes will be followed.
4. Any other access is granted under the provisions of the Bellevue College IT security standard addressing "Physical Security," except the following:
 - a. **City of Bellevue Employees**
 - i. City of Bellevue employees designated and authorized by the TFMC will be individually assigned metal keys and/or key codes, and have the same access privileges as authorized Bellevue College employees.
 - b. **Students**
 - i. Students may work at these facilities as a part of their normal coursework within the Advanced Track Video Production Training program, or in the capacity of part-time employees.
 - ii. Students working at the facilities will have their physical access to these facilities controlled by the Director of Television Services and Campus Operations, in accordance with the Bellevue College IT Security Standard addressing "Physical Security."

E. Computer and Networking Security

1. Access to the digital server, encoding computer, AVID editing systems, and digital archive computer systems will be limited to Bellevue College Television Services staff, authorized City of Bellevue employees, and authorized Bellevue College Information Resources technical and media support personnel.
2. All access to the production, editing and cablecast computing technology used by Bellevue College Television Services will be in accordance with Bellevue College Policies #5000, "Acceptable Use of Bellevue College Computers", and #5150, "Acceptable Use of Bellevue College Networks and Systems."
3. All accounts and passwords for City of Bellevue employees and students enrolled in the Advanced Track Video Production Training program will be requested and managed by the Director of Television Services in accordance with the Bellevue College IT Security Standard addressing "Password Management."

F. Security and Disposal of Output

1. All programming stored on tape will be protected from accidental or intentional erasure by breaking the protection tabs on the cassette.
2. All programming stored on tape will be locked in the secure Bellevue College Television Services facilities described above under: D. Physical Security.
3. All master programming stored digitally on computing systems will be adequately backed-up to prevent accidental or intentional deletion. These backups will include tape and/or digital formats.
4. If tape or digital media (CD, DVD) output is no longer needed for retention for archival or cablecast purposes, the Director of Television Services will order it destroyed. Such destruction will be of a method in compliance with the Bellevue College IT Security Standard addressing "Media Disposal."

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 IT Security Standard: *Physical Security*
5. Bellevue College IT Security Standard: *Media Disposal*
6. Interlocal Agreement for Co-Location of The City of Bellevue Cable Production Facilities at Bellevue Community College

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