

IT Security Standard:

Data Recovery

Introduction

Bellevue College IT support personnel are often called upon to perform technical work to recover Bellevue College data stored on damaged storage media. This standard describes the processes needed to implement Bellevue College policy # 5250: *Information Technology (IT) Security* regarding the management of that work and defines the expectations and safeguards in place to ensure that any outside contractors engaged to assist in this work perform in compliance with that policy. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard will be applied in all cases where any damaged or malfunctioning Bellevue College storage medium is manipulated in an attempt to restore or recover Bellevue College data. It applies specifically to non-Bellevue College personnel who are not already under contract with Bellevue College as a vendor performing technical services. However, this standard can also be used as a guide when contracting with any vendors who may be granted access to Bellevue College data. Unlike other standards which create an extraordinary responsibility for protecting data that is defined as protected by the Bellevue College IT security standard addressing "*Data and Information Security*," this standard applies to all Bellevue College data that may potentially be exposed to an outside contractor performing this specific service.

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 outside vendors to recover important deleted Bellevue College business data from Bellevue College storage devices which cannot be reinstated by Bellevue College IT support personnel is an important tool in keeping the information and data used at the college accessible, even in times of technology or procedural failures. It is a common business practice to utilize technical specialists and companies that have developed great expertise to handle these types of disaster recovery efforts. However, because Bellevue College has policies in place that limit access to information that is protected, careful steps must be taken to ensure Bellevue College remains compliant with federal and state privacy laws even in exigent circumstances.

The most significant security threats related to using outside vendors to assist in data recovery are:

1. Public disclosure of protected Bellevue College data
2. Loss of Bellevue College resources (the media, itself)

Given the nature of the asset and the nature of the threat, the main risk associated with use of vendors to recover data stored on Bellevue College storage media is the disclosure of the data to the vendor, the vendor's employees or any other entity not normally authorized to have access to the data. All of these threats have associated risks of: inadvertent violation of privacy laws, dissatisfaction of those to whom Bellevue College provides services, vulnerability of the institution to civil sanctions, and a loss of reputation.

Standard

A. Introduction

1. With the ubiquitous nature of computing technology in Bellevue College's business environment it is inevitable that at times the technology will not properly function. When this failure of technology includes storage media, such as hard drives or portable storage media, such failure can mean important Bellevue College business data is not accessible for a period of time and potentially lost completely.
2. While Bellevue College IT support personnel are skilled in all aspects of supporting computer technology, at times it is required that Information Resources delegate a support task to outside companies who specialize in a particular field and who have access to adequate technological support resources to accomplish that which cannot be done at Bellevue College. However, in performing this technical service, the outside vendor may obtain protected college data, a technical violation of Bellevue College policy.
3. When data has been deleted from any Bellevue College storage media, or the storage device has been damaged, making the data inaccessible, and a campus user or unit responsible for the media and the data it contains needs to recover that information, the below procedures will be followed, whether or not the user states there is or is not protected data potentially on the media.

B. Procedures

1. Information Resources IT support personnel will determine if any adequate backup of the data exists either at the unit or within IR's networking and computing resources.
2. If an adequate backup does not exist, IT support personnel will attempt to recover the needed data using standard Bellevue College equipment and practices.
 - a. If recovered, this data will be moved to a different storage medium and any failed storage media will be disposed of in accordance with the Bellevue College IT security standard addressing "Media Disposal."
3. If the data cannot be satisfactorily recovered by IR, the requesting unit will be notified and will have the option of asking that IR send the storage media to an outside vendor for further data recovery attempts at the unit's expense.
 - a. IR will maintain a list of area vendors that specialize in data recovery tasks approved by the Dean of Information Resources or appropriate designee, in accordance with Bellevue College policy.
 - b. An estimate of the cost of the data recovery will be obtained from the vendor and approved by the requesting unit before any work to recover the data will be undertaken.
4. If the requesting unit chooses to engage a company to attempt data recovery, the following steps will be followed prior to releasing the storage medium to the vendor. **NOTICE**: Bellevue College users or units will not engage a data recovery vendor without IR's knowledge and approval.
 - a. IR will obtain a copy of the "Bellevue College Information Release Authorization" form approved by the unit administrator.
 - b. The form will be copied and the original forwarded to the company being contracted to perform the attempted data recovery for acknowledgment of the vendor's responsibility to protect the Bellevue College data.

- c. Upon receipt of the completed form, IR will file the form and will provide a copy to the vendor and the requesting unit, if desired.
5. The storage media will be delivered by IR to the vendor for the recovery attempt. Written receipt acknowledgement will be obtained.
 - a. IR will request that the vendor keep IR apprised of the status of the recovery.
 - b. If the data is recovered, the vendor will provide the recovered data to IR, who will make and secure any copies needed for later recovery purposes, if any, and will then pass the data along to the requesting unit.
 - c. If the data is unrecoverable IR will request the vendor return the storage media, which will be properly disposed of.
6. In all cases, the vendor will be expected to return the original media to IR and will destroy all copies of any data in their possession in accordance with the contract.
7. Vendors may not keep copies of any data recovered or disclose such data to any party except authorized Bellevue College representatives.
8. All records and forms pertaining to data recovery attempts by vendors will be maintained on file by the IT Security Administrator.

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 #5150, "*Acceptable Use of Bellevue College Networks and Systems*"
2. Bellevue College Policy #5000, "*Acceptable Use of Bellevue College Computers*"
3. Bellevue College IT Security Standard: *Data and Information Security*
4. Bellevue College IT Security Standard: *Non-Employee Access to Bellevue College Systems and Data*
5. Bellevue College IT Security Standard: *Media Disposal*

Effective Date: July 2006
Date Last Modified: April 12, 2009