

IT Security Standard:

Disaster Recovery

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding institutional recovery from various kinds of disasters. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to all disaster recovery operations at Bellevue College. This includes recovery from physical damage or destruction of property, personnel actions, restoration of physical facilities, restoration of business data and information, and salvage operations.

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

A catastrophic disaster at Bellevue College, whether it involves facilities, infrastructure, or any component parts of those systems, has the ultimate business impact on the campus that is possible. Until recovery operations are engaged, any systems or services impacted by any type of disaster will be unavailable. Though the threat of some disasters is minimal, the impact of any disaster is so significant that a valid, cohesive and effective plan for recovery is imperative.

Given the nature of the disasters which could impact Bellevue College, the most significant threat is total loss of services and ability to manage business operations

Standard

- A. The Bellevue College IT Security Administrator and/or the Dean of Information Resources, or an authorized designee, will be responsible for developing and maintaining a Disaster Recovery and Business Resumption Plan, defining the organizational and procedural requirements for guiding Bellevue College through a recovery period following a disaster. All guidelines, procedures, processes and expectations related to disaster recovery will be articulated within the plan.
- B. This plan will be made and carried out in conjunction with all Bellevue College administrative units. The Bellevue College IT Security Administrator and/or the Dean of Information Resources,

or an authorized designee, will be responsible for documenting the plan, for maintaining formal copies of the plan, and for disseminating any information required under the plan. The plan will be reviewed at least annually.

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. SBCTC-IT Disaster Recovery and Business Resumption Plan

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