

IT Security Standard:

Login Banner

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding computer system login banners. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific procedural and configuration elements for the display of login warning banners on computers and networked devices managed by Bellevue College.

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

The purpose for the login banner is to give appropriate warning to those who would log into a device when legitimate access to the device is limited to explicitly preauthorized persons. It is also to give notice that activity associated with this device will be monitored. These are usually the two key criteria of interest to law enforcement in an investigation.

As such, this standard does not so much address risk as to improve the ability or likelihood that any evidence collected by Bellevue College staff in the course of an incident investigation (or other duties) could be used to take action against the wrongdoer.

Standard

1. A login warning banner will be displayed at the earliest possible point in the login process prior to entering an account name.
2. The banner will be selected from one of those listed below and implemented consistently across all devices of a particular class whenever possible; i.e., all desktop workstations will have the same banner, all production HP3000s will have the same banner, all configurable network devices will have the same banner, and so forth.

3. Some positive action by the person accessing the device is required to dismiss the banner from view. This action may be a mouse click of a button, a continuation of the login process, or other act that indicates the person consents to the statement.
 - a. Option 1

Only authorized users may connect to this controlled access system. This system is being monitored at all times; by connecting to it, you consent both to being monitored and to abiding by the governing policies of this processor.
 - b. Option 2

This system is for the use of authorized users only. All individuals using this computer system are subject to having their activities monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of inappropriate activity, system personnel will provide the evidence to agency management and law enforcement officials.
 - c. Option 3

You are logging onto a computer owned by the State of Washington and must follow all Bellevue College policies and procedures during all use of this computer. Bellevue Community College authorized employee use only.

Appendix A -- References

1. SBCTC-IT Security Standard—Login Banner, January 29, 2003.
2. Bellevue College Policy #5150, "Acceptable Use of Bellevue College Networks and Systems"
3. Bellevue College Policy #5000, "Acceptable Use of Bellevue College Computers"

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