

IT Security Standard:

Phone System Configuration

Introduction

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

Scope

This standard defines specific procedural and configuration elements for management of the Bellevue College-managed phone system, handsets, State Controlled Area Network (SCAN) codes, and phone mail accounts.

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 Bellevue College phone system is both a core and critical service that enables Bellevue College to communicate within the campus as well as with the outside world in a timely and efficient fashion.

Given the high level of dependence on the phone system, the most significant threats are:

1. Malicious and/or unauthorized access to the device
2. Malicious and/or accidental physical damage to the device
3. Theft of the device
4. Theft of a SCAN code
5. Interruption to electrical power

The primary risk associated with these threats is the potential for inappropriate use of the resource. This can include such things as uses inconsistent with Bellevue College's mission or uses that are in violation of Bellevue College policy #4400, Acceptable Use of State Resources and/or state and/or federal law. Additionally, theft of a SCAN code can result in substantial financial losses when large volumes of SCAN calls are placed via a compromised account.

Standard

A. System Configuration

1. Bellevue College's phone system is a Siemens HiCom 300E. The switching unit (SWU) executes and controls call processing functions and features with Intel-based microprocessors. Line/trunk interface boards provide interface to telephones and other telephony devices. Devices added to the system are:
 - a. Remote Communications Module (RCM)—We have 3 RCM's; one located on the Factoria campus and two at North Campus connecting the remote sites to our HiCom 300E by T1 lines.
 - b. Automatic Call Distribution Server (ACD)—The ACD server processes and distributes calls for our Call Centers.
 - c. APC Smart Uninterrupted Power Supply (UPS), with battery packs for battery backup.

B. Backups and System Recovery

1. The following procedures will be in compliance with the Bellevue College IT security standard addressing "Data and Program Backup":
 - a. System recovery media will be created and kept current by authorized Information Resources support personnel so the system can be recovered to a known good state in the event of a system failure or compromise.
 - b. The recovery media and documentation will be stored in a location providing restricted access control, known to all systems administration staff, and be reasonably accessible in the event it is required.
 - c. The system will be backed up weekly.
 - d. Restoring files from tape is an operation that will be performed by authorized Information Resources personnel or an authorized designee.
 - e. Tape backup media will be kept in a weekly rotation at an offsite data storage facility.

C. Phone Mail Account Management

1. Use of the telephone for accessing phone mail accounts will be in compliance with Bellevue College policies #4400, Acceptable Use of State Resources and #5150, Acceptable Use of Bellevue College Networks and Systems.
2. Phone mail is accessed via the Siemens telephone and secured by a five-digit numeric password. Use of this phone mail account will not be in compliance with the Bellevue College IT security standard addressing "Password Management." Given that the phone mail password is numeric only, an exception regarding its use is included in the Bellevue College IT security standard addressing "Password Management Exceptions."
3. Phone mail can also be accessed via Microsoft Outlook. Users will comply with the Bellevue College IT security standard addressing "Password Management", Bellevue College policy #4400, Acceptable Use of State Resources and policy #5150, Acceptable Use of Bellevue College Networks and Systems when accessing phone mail through Outlook.

D. SCAN Account Management

1. Use of SCAN accounts will be in compliance with Bellevue College policy #4400, Acceptable Use of State Resources and policy #5150, Acceptable Use of Bellevue College Networks and Systems." SCAN accounts are to be used for business purposes only.
2. SCAN user accounts are password secured by numeric-only passwords. Passwords will never be shared. Bellevue College employees will not ask for, accept, or use other user's passwords. Additionally, passwords will not be written down. A written password is more easily discovered than one committed to memory.

3. Use of SCAN accounts must be in compliance with the Bellevue College IT security standard addressing "Password Management." Given that SCAN passwords are numeric only, an exception allowing their use is included in the Bellevue College IT security standard addressing "Password Management Exceptions."
4. The Department of Information Services (DIS) manages the creation, modifications, and deletions of SCAN accounts and respective passwords for state agencies.
 - a. The Bellevue College Finance Office coordinates the acquisition and distribution of SCAN accounts and passwords for the college. This process is governed by the procedures identified in the Bellevue Community College "Finance Handbook."
 - b. The Finance Office makes such SCAN-related requests to DIS and then distributes the account information to campus users.
5. Unencrypted copies of records or documents containing scan codes may not be stored on any Bellevue College systems.
 - a. The network server controlling the phones is included in this encryption requirement.

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 Finance Handbook, as revised September, 2005
2. Bellevue College Policy #4400, Acceptable Use of State Resources
3. Bellevue College Policy #5000, Acceptable Use of Bellevue College Computers
4. Bellevue College Policy #5150, Acceptable Use of Bellevue College Networks and Systems
5. Bellevue College Policy # 5250: Information Technology (IT) Security
6. Bellevue College IT Security Standard: Password Management
7. Bellevue College IT Security Standard: Data and Program Backup
8. Bellevue College IT Security Standard: Database Management

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