

IT Security Standard:

Network Time Protocol Configuration

Introduction

This standard defines the specific steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding network time protocol 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 network time servers.

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

Time synchronization is important for event correlation across devices for a wide variety of reasons, including troubleshooting network problems and collecting evidence for prosecution of a crime. Also, time synchronization can be critical in managing distributed systems and such things as recovering databases after a failure.

In Bellevue College's current environment there is no direct risk associated with incorrect system time. However, accurate time is often taken for granted when analyzing problems. Currently, the risk is mainly associated with working on an assumption of precise and accurate time when it does not exist.

Standard

- A. All Bellevue College domain controllers will synchronize their time with the domain naming master at the forest root. Time updates from other sources will be ignored.
- B. All Bellevue College Windows workstations will synchronize to the domain controller from which they are authenticated. This process of time synchronization occurs automatically when a Windows computer logs into the Campus domain
- C. Network devices (routers, switches, firewalls), that support time synchronization will use either an SBCTC-IT time server or the current domain naming master server.
- D. The two primary time-servers will be configured to request time only from well-known and trusted sources using Network Time Protocol (NTP). Bellevue College currently uses time-nw.nist.gov as its time source. All other updates will be ignored.

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. University of Delaware, Network Time Protocol project, <http://www.ntp.org/>
2. SBCTC-IT Security Standard— *SBCTC-IT Security Policy for Network Time Synchronization*

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