

IT Security Standard:

Network Printer Configuration

Introduction

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

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 network printers within the scope of this standard are important infrastructure for the daily business and operations of Bellevue College. Loss of this service would have a significant impact on Bellevue College's ability to provide services.

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

1. Malicious denial of service
2. Malicious and/or unauthorized access

Given the nature of the asset and the nature of the threat, the primary risk associated with the network printers is loss of services. Printers, however, tend not to be prime targets of attackers. As such, the risk associated with printers is fairly low.

Standard

A. General

1. Network printers will be configured with the same care as any other network device. As such, only required services will be enabled, logins will be password-protected, and access methods will be limited to secure protocols.
 - a. All network-layer two protocols, except Ethernet, or Appletalk, will be disabled.
 - b. All network-layer three protocols, except Internet Protocol (IP), or Appletalk in the case of Macintosh computers, will be disabled.

- c. The only network - layer four protocols that will be allowed for remote management are: HTTP (80 and 280/tcp), Printer (515/tcp), Jet Direct (9100/tcp), and SNMP (161/udp). Other protocols, including Telnet, FTP, and WINS will be disabled. The firewall will be configured to block all outside access to the printers.
- d. SNMP will be allowed, even though it has very weak security, to manage the printers. The read and write community strings will meet the standards defined for printer passwords (# 7, below).
- e. If access to a printer can reasonably be restricted to one subnet, the devices gateway will be set to either 0.0.0.0 or its own IP Address. This is especially significant if the device cannot otherwise be configured in compliance with this document.
- f. The printer's firmware will be kept at the most current, safe, and functional version.
- g. Passwords that are in compliance with the Bellevue College IT security standard addressing "Password Management" will be used to protect administrative access to the printer. Password lifetime, however, can be extended to twelve months.

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. SBCTC-IT Security Policy
2. SBCTC-IT Security Standard—Network Printer Configuration
3. Bellevue College policy # 5250: Information Technology (IT) Security

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