

## *IT Security Standard:*

# **Firewall Configuration and Change Management**

### **Introduction**

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

### **Scope**

This standard defines specific procedural elements for management of the Bellevue College firewall and its associated components in support of the Bellevue College IT Security Policy. This standard will limit itself to addressing the configuration and change management processes of these devices as opposed to the detailed configuration of them. It is assumed in this document that the specific configuration of those devices will be done in a manner consistent with the overall Bellevue College IT Security policies and standards as well as current industry best practices.

### **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**

An organization's firewall serves as a choke point in the network topology; and as such it is a significant component in the overall defense protecting an entity's computing resources from attack or misuse. Adequate measures must be taken to carefully configure and maintain the firewall and to protect the information regarding that configuration from unauthorized persons.

In this light, the most significant threats are:

1. Malicious denial of service or destruction/disclosure of protected data
2. Malicious and/or unauthorized access to controlling components (i.e.; routers, etc.)
3. Malicious and/or unauthorized access to systems, data, and/or processes
4. Theft or malicious manipulation of data and/or services
5. Theft or physical damage to the network hardware components

Given the nature of the asset and the nature of the threat, the primary risk associated with the networking infrastructure is loss of service. This loss of service has associated risks including: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and to some degree a loss of reputation. Secondary to these threats is the potential for inappropriate use of

the resource. This can include such things as: excessive bandwidth use, uses inconsistent with the Bellevue College organizational mission, uses that are in violation of the Acceptable Use of Bellevue College Networks and Systems policy or federal and/or state law, or theft and fraudulent use of data.

This standard attempts to provide a process by which reliable and appropriate configuration can be maintained on the firewall, thereby minimizing malicious or otherwise inappropriate traffic and maximizing availability of the resources for appropriate use.

## Standard

### A. Firewall Configuration

1. Publishing the details of the firewall configuration in a public forum is a significant breach of confidentiality. A knowledgeable user with the details of the firewall configuration would have the tools to defeat any and all IT security in place at Bellevue College. Therefore, separate documents identifying the details needed for Information Resources personnel to be able to set up and support the firewall will be held in a secure location designated by the Bellevue College IT Security Administrator and will not be among these public standards.
  - a. These documents will be created and approved by the Bellevue College Network Server Group as well as any other support staff designated by the Dean of Information Resources and the IT Security Administrator.
  - b. Documents created in support of this standard will be disseminated only to appropriate support staff. Printed copies will be limited and distributed only by permission of the IT Security Administrator or designee, and will require secure disposal after use or review.
  - c. These documents should be stored digitally in a secure location designated by the IT Security Administrator and/or the Dean of Information Resources.

### B. Standard Process for Making a Firewall Change

1. Firewall change requests will be made to the Bellevue College IT Security Administrator, who will review them for consistency with policy and best practices as well as assess any increased level of risk. Additional information may be requested to support the need for the change.
2. Once a week, the Bellevue College IT Security Administrator and/or the Dean of Information Resources will forward all approved change requests to the Bellevue College Firewall Administrative Team for implementation during off peak hours later in the week.
3. Changes requested outside the normal weekly schedule will be evaluated for criticality and emergency updates will be processed in a timely manner.
4. In the absence of the Bellevue College IT Security Administrator and/or the Dean of Information Resources, changes will be submitted to the Director of Computing Services (CS).

### C. Documentation of Firewall Rules

1. The Bellevue College IT Security Administrator will maintain documentation of the firewall rule-set. This documentation entitled "**Firewall Logical Specifications (Confidential)**" will include:
  - a. The characteristics and expected usage of each firewall interface.
  - b. The design goals for each interface's rule set (i.e., a logical design).
  - c. The specific rules to implement that design, by interface.
  - d. Explanation and documentation on each exception to that design.
2. Change control logs will be maintained with the **Firewall Logical Specifications (Confidential)** documentation defining who made a change request, when it was made, when it was implemented, and the rationale for that change.

#### **D. Backup and Version Control of the Firewall Configuration**

1. The firewall's configuration (access control list, or ACL) and rules will be backed up onto a secure server in the demilitarized zone (DMZ) or Administrative Network, not on the firewall itself, where they will be maintained as text files. In addition, a copy of the configuration will be maintained on CD-ROM.
2. Processor and file system security will be configured such that these files will have restricted access.
3. On that server, these configuration file(s) will be backed up to the system backup tape on the processor's regular backup cycle.
4. The ACL and other configuration file(s) will be maintained using a method of version control, such as Revision Control system (RCS).

#### **E. Audit/Assessment of Firewall**

1. At least annually, the Bellevue College IT Security Administrator and/or the Dean of Information Resources will review the implemented firewall configuration and ACL files against the firewall rule-set documentation. The administrator will verify:
  - a. The ACL matches the documented rules.
  - b. The rules and exceptions are still valid and consistent with best practices, policy, and business needs.
  - c. The change control processes are being followed.
  - d. The development of a plan to address any discrepancies and recommend any improvements to the configuration or rules that seem appropriate.
2. An external audit of the firewall implementation and management procedures will be performed every three years, in addition to this internal assessment.

### **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 Standard –Firewall Management, November 2, 2002
2. Bellevue College Policy #5150, *Acceptable Use of Bellevue College Networks and Systems*
3. Bellevue College Policy #5250 – *Information Technology (IT) Security*
4. Bellevue College IT Security Document: Firewall Logical Specifications (Confidential)

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