

IT Security Standard:

DNS Configuration

Introduction

This standard defines the steps and guidelines needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding Domain Name Systems (DNS). The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific procedural and configuration elements for the management of Domain Name Systems (DNS) in support of the Bellevue College IT Security Policy. This service is principally responsible for mapping Internet Protocol (IP) addresses to human-friendly computer names; in addition, it also provides the ability to alias names and map services. Bellevue College Information Resources (IR) manages DNS for the college's internal networks and sub-networks.

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

DNS is a component of the critical infrastructure supporting the daily business and operations of Bellevue College. While not true across the board, some of the college's business (administrative, instructional, and public service) functions nearly halt with any significant disruption to DNS.

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

1. Denial of service.
2. Malicious and/or unauthorized disclosure of sensitive security information.
3. Malicious and/or accidental misdirection of traffic (spoofing).

Given the nature of the asset and the nature of the threat, the primary risk associated with DNS is loss of service. This loss of service does have associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and loss of reputation. Secondly, the information contained in the DNS database effectively maps Bellevue College and critical components of many of the college networks. Disclosure of this information could give attackers key information regarding where to direct their efforts. Because DNS provides address-to-name resolution, accidental or intentional misinformation contained in its database can lead to traffic being misdirected away from where the services are provided -- in effect, another form of denial of service.

Standard

A. General Architecture

1. Bellevue College will use a split DNS structure that exposes only selected records to the "outside world," keeping the remainder of the internal domain structure hidden. The external name servers will be supported by a current version of Berkley Internet Name Domain (BIND), while internal name servers may be either BIND or Microsoft DNS.
 - a. DNS records that are intended to be externally visible will be maintained on primary name servers on the demilitarized zone (DMZ). In computer networks, a DMZ is a computer host or network segment inserted as a "neutral zone" between a college's private network and the outside public network.
 - b. The internal DNS servers will be configured to forward all unresolved queries only to another internal name server or the two primary name servers on the DMZ.
 - c. Dynamic Updates of DNS information will be disabled for servers in the DMZ or external to the firewall.

B. Server Requirements

1. All unnecessary services on the processor will be disabled (and preferably removed). *Note:* While it is ideal to isolate services on computer systems that serve only a single purpose, it must be recognized that historical, practical, architectural, and financial considerations often dictate the sharing of services across computer systems. When this occurs, the fallback position should be to cluster "compatible uses" onto a computer system. It is at this point that stating "all unnecessary services ... will be disabled" becomes a reasonable security stance.
2. The system clocks of the servers will be synchronized to one of Bellevue College's standard time servers.

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 Policy #5250 – *Information Technology (IT) Security*
2. *Guide to Securing Microsoft Windows 2000 DNS*, National Security Agency, April 2001 (Ver.1)
3. Fossen, *Windows 2000: Active Directory and Group Policy*, SANS 2001, May 2001
Thomas, Rob, *Secure BIND Template Version 3.2*,
<http://www.cymru.com/Documents/secure-bind-template.html>, updated Jan 2006
4. Householder, King, and Silva, *Securing and Internet Name Server*,
<http://www.cert.org/archive/pdf/dns.pdf>, CERT, Aug. 2002
5. SBCTC-IT IT Security Standard—*DNS Configuration Standard*, January 29, 2003.

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