

IT Security Standard:

Virus Protection

Introduction

This standard defines the steps needed to implement the Bellevue College IT Security Policy with regard to virus protection on Bellevue College computers and networks. 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 virus protection software for server and desktop computer systems in support of the Bellevue College IT Security Policy. This standard applies to all workstation class and server class computers. In addition, sections detail precautions and actions to be taken regarding e-mail servers and the handling of e-mail.

For the purpose of this document, “viruses” will be defined fairly broadly to include viruses, worms, Trojans, and any similar malicious programs or code.

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

Given the nature of viruses, the most significant threats are:

1. Malicious denial or disruption of service.
2. Malicious and/or accidental release of sensitive information.
3. Malicious and/or unauthorized access to computer systems.
4. Malicious destruction of data.

Vulnerability to infection and manipulation by malicious code creates an extremely high level of threat to Bellevue College business and educational operations, no matter the operating system being used.

To offset this threat, historically-proven techniques and tools are available. However, one complexity in risk assessment is the fact that virus protection is always a reactive activity -- there is little proven technology that prevents against a previously unknown attack.

With this as the context, it becomes clear that the day-to-day risk can be well-managed by good procedures and tools; the most significant risk is from the so-called zero-day (previously unknown) viruses that use a new attack vector that has been previously undefended.

Standard

A. General

1. Every network-enabled server and desktop will have antivirus (AV) software installed.
2. Real-time virus protection will be enabled for servers and desktops and will be set-up to perform a proactive scan each time a new file or message is introduced onto any of the systems. This real-time protection will be configured so that the user cannot tamper with or disable it.
 - a. Bellevue College network administrators and/or maintenance technicians are permitted to disable AV software in order to perform certain tasks when necessary, such as installing software.
3. Even with real-time protection, every Bellevue College server will be fully scanned at least once a week.
4. Scheduled scans on users' desktops will be performed no less than once a week and scheduled during business hours when the computer is expected to be on.
 - a. These scans can be run by users in the background to lessen disruption to their work.
5. Laptops that are not regularly powered up and connected to the network to receive updates will regularly be updated and scanned by Information Resources technical support personnel.

B. Microsoft Exchange Servers

1. Bellevue College's e-mail application, Microsoft Exchange, is also a significant component in controlling virus and worm outbreaks because e-mail is often used as a delivery method. In addition to the basic scanning described above, additional protection will be provided by having e-mail scanned as it is sent and received (prior to delivery into the Bellevue College recipient's mailbox).
 - a. All Bellevue College employees will show caution with regards to received e-mail. If a message looks suspicious, users will delete it from both the Inbox and the Deleted Items folders.
 - b. All incoming e-mail will be scanned by an appropriate AV solution and any files attached to an e-mail message that cannot be scanned will be quarantined and prevented from delivery to the e-mail client.
 - c. The AV software will also disable unsafe macros (specifically auto-start macros) in attachments.
 - d. Full scans of all e-mail mailboxes will be performed on no less than a weekly basis and a partial scan of all mailboxes will be performed at another time during that week.

C. Maintenance of the Antivirus System

1. The master AV servers will be configured to automatically update the virus pattern file on a daily basis. On a weekly basis, the pattern file on the master servers will be manually verified to assure they are current.
2. When new pattern files are received, they will be pushed to all other servers and desktops, if possible. All of this will be automated.
 - a. Macintosh AV software will be installed locally only, and will be configured to perform regular live updates from the Web, if the software has that capability.
 - i. If the AV software in use for Macintosh computers does not have the capability to be configured to automatically obtain regular live updates, it will be the responsibility of IR technical support personnel to manually update the virus signatures on all Macintosh computers at least once each quarter. This will be done remotely if possible.
 - b. The Windows client will be configured to check its master server at scheduled intervals to see if there is a new pattern file.
 - i. The Windows client will be configured to produce a pop-up message if the AV pattern file is older than 30 days.

3. Periodically, spot-checks of other servers and desktops will be performed by network administrators to verify that they have the most recent pattern files.

D. Response When a New Virus Is Spreading

1. IR support personnel will check the major vendors' web sites to confirm that there is indeed a new virus and will avoid false alarms due to hoaxes whenever possible.
2. If information regarding a new virus is verified, IR support personnel will determine whether Bellevue College systems are protected. Users will be informed in an appropriate manner, depending upon the specifics of the incident.
3. If the Bellevue College networks or workstations are not currently protected and the threat is significant, a member of the network administration staff will go into "monitoring mode," checking the pattern file site at least every half hour until it can be downloaded and deployed on the computers.
4. If the infection risk dictates, the Dean of Information Resources or authorized designee may choose to protect desktop or server systems by disconnecting them from the network.

E. Response to Infection

1. As a rule, infected servers and workstations will be rebuilt starting with a freshly formatted disk. Upon virus analysis and agreement among the designated IR Information Technology Management Team members that the virus is innocuous, the threat of spreading is minimal, and cleanup is easy, a cleanup may be performed instead of a rebuild.

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 Standard—*Microsoft Windows Virus Protection*, January 29, 2003.
2. Bellevue College Policy #5000: *Acceptable Use of Bellevue College Computers*
3. Bellevue College Policy #5150: *Acceptable Use of Bellevue College Networks and Systems*

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