

Best Security Practice for
**VIRUS, TROJAN, SPYWARE and OTHER MALICIOUS CODE
PREVENTION**

PUBLISHED BY THE OFFICE OF INFORMATION TECHNOLOGY – MARCH 2008
"BEST PRACTICES ARE THE PROCESSES AND ACTIVITIES THAT HAVE BEEN SHOWN TO BE THE MOST EFFECTIVE"

BEST SECURITY PRACTICE (BSP) No. 4: ALL UNLV NON-MAINFRAME COMPUTERS, NETWORK-CONNECTED OR NON-NETWORKED, SHOULD EMPLOY A STRONG ANTI-VIRUS/ANTI-MALWARE APPLICATION(S). ADDITIONALLY, IT IS STRONGLY RECOMMENDED THAT ALL UNLV NETWORK-CONNECTED COMPUTERS SHOULD ALSO EMPLOY AN ANTI-SPYWARE APPLICATION(S). THIS PRACTICE ESTABLISHES A MINIMUM STANDARD WHICH SHOULD BE MET BY ALL SMALL UNLV COMPUTERS TO ENSURE EFFECTIVE VIRUS, MALICIOUS, AND OTHER MALWARE PREVENTION OR DETECTION AND REMOVAL.

OBJECTIVES: To provide direction and support for information security in accordance with internationally accepted standards (ISO 17799/27001), business requirements and relevant State and Federal laws and regulations. This technical Best Practice directly supports the UNLV Capstone Policy IS01 - Information Security for Information Resources and Asset, and defines the acceptable use of UNLV information technology services and accounts. **This BSP is the foundation for the forthcoming UNLV Virus, Trojan, Spware and Other Malicious Code Prevention Policy (IST103).**

BACKGROUND: virus, spyware, and other malicious threats, collectively referred to as "malware" in BSP series of documents, have the potential of causing significant business and academic disruption and significant cost in terms of failed services, service recovery, loss of productivity, and costs associated with the potential loss of protected or sensitive information.

The purpose of this Practice is to:

- Establish the use of anti-malware applications.
- Ensure as much as possible that your computer remains free of digital malware infections.
- Ensure that access to UNLV electronic resources are reasonably secure.

In order to manage information security comprehensively, this Best Practice serves the to:

- Ensure that use of IT systems is consistent with sound security principles;
- Ensure that IT systems are used for their intended purposes and meet any compliance requirements;
- Ensure the integrity, reliability, availability, and superior performance of IT systems;
- Assure that the core IT network and systems is available to support emergency services in the event of community disaster response needs; and
- Establish standards for addressing security consistency.

AUDIT CONTROL: Security audits will inspect the in-use security applications, procedures, and processes of anti-malware applications by using this Best Practice, including timeliness of updates, for compliance to security best practice standards. This Best Practice will be audited using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and through a complete review of all related complaints (security incidents) that occurred after the previous audit.

BEST SECURITY PRACTICE STANDARDS

INFORMATION SECURITY STANDARDS AND CONTROLS. The following are the anti-malware Best Practice Standards that should be applied to each IT system, as appropriate, to be in minimum compliance with UNLV standards.

STUDENT RESPONSIBILITIES:

BSP: 5-1 Anti-Malware for Personal-type Computers. All laptops & desktops computers should have UNLV's standard, supported anti-malware software, or approved alternate(s), installed and actively running when connected to UNLV networks. In addition, the anti-malware software and the malware signature/pattern files must be kept up-to-date. Malware infected computers must be removed from the network or quarantined until they are verified as updated and virus-free. System administrators are responsible for creating and enforcing procedures that ensure anti-malware software is running on network connected computers, and the computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into UNLV's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy* and the *Acceptable Email Usage Policy*.

BSP: 5-2 Anti-Spyware for Personal Computers. All personal-style (laptops & desktops) computers are strongly recommended to have a UNLV recommended standard anti-spyware application, or approved alternate, installed and actively running when connected to UNLV networks. In addition, the anti-spyware software and the spyware pattern files should be kept up-to-date. Spyware-infected computers should be removed from the network or quarantined until they are verified as updated and clean. System administrators are granted permission to create and enforce anti-spyware procedures where needed and that the computers are verified as clean.

BSP: 5-3 Anti-Malware for Small Computing Devices. Computer devices such as PDA's with operating systems that do not have commercial anti-malware software available for use are exempt from this policy until the software becomes available. Refer to the *Anti-malware Guidelines* below to help prevent infection problems.

ACADEMIC AND GENERAL STAFF RESPONSIBILITIES:

BSP: 5-4 Anti-Malware for Business/Application Servers. All departmental servers and other departmental-style small computers should have UNLV's standard, supported anti-malware software, or approved alternate(s), installed and actively running when connected to UNLV networks. In addition, the anti-malware software and the virus signature/pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. System administrators are responsible for creating and enforcing procedures that ensure anti-malware software is running on network connected computers, and the computers are verified as malware free.

BSP: 5-5 Anti-Malware for Email Servers. All email servers and other departmental-style small computers operating an email service should have UNLV's standard, supported anti-malware software, or approved alternate(s), installed and actively running when connected to UNLV networks. In addition, the anti-malware software and the virus signature/pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. System administrators are responsible for creating and enforcing procedures that ensure anti-malware software is running on network connected computers, and the computers are verified as malware free.

BSP: 5-6 Any Network Connected Business/Application Computer. Network connected departmental/small computers that do NOT have UNLV's standard, supported anti-malware software, or approved alternate(s), installed and actively running when connected to UNLV networks should be quarantined or removed from the network until they are updated and verified as malware free before allowing further access.

ANTI-MALWARE GUIDELINES

General Prevention Guidelines

Recommended processes to prevent virus problems:

1. Always run the UNLV standard, supported anti-malware software available from the University download site. Alternate anti-malware applications may be used if approved. Download and run the current version and/or download and install anti-malware software updates as they become available.
2. NEVER open any attachments to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "purge" the deleted attachments by emptying your Trash.

3. Delete spam, chain, and other junk email without forwarding, in concert with UNLV's *Acceptable Use Policy* and the *Email Usage Policy*.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
6. Always scan a floppy diskette or USB drive from an unknown source for viruses before using it.
7. Always back-up critical data and system configurations on a regular basis and store the data in a safe place.
8. If lab testing conflicts with anti-malware software, run the anti-malware utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-malware software. When the anti-malware software is disabled, do not run any applications or any media that could transfer a virus, e.g., email or file sharing.
9. Multiple new viruses or variants of old viruses are discovered on most days. It is a very good practice to manually check for updates.