

Government
Information
Technology
Agency

Statewide
STANDARD
P800-S860 V1.0

**TITLE: Virus and Malicious
Code Protection**
Effective Date: DRAFT

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

To establish a statewide Virus and Malicious Code Protection standard for the State of Arizona.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology PSPs within each Agency.

4. STANDARD

In an effort to safeguard networks and critically sensitive information from software contaminants, each Agency shall:

4.1. Implement an architecture that protects against the following:

4.1.1. Newly Identified Virus and Malicious Code

- Boot Sector - These viruses infect the first sector of a diskette or hard disk, which contains the master boot record, and are launched when a computer initializes with an infected disk. If a computer is booted with an infected diskette, the infected sector is loaded into memory and writes itself to the master boot sector on the hard drive. The virus stays in memory and infects new diskettes when the operating system accesses a new diskette and infects the boot

sector of that disk. A boot sector virus, unlike other forms of viruses, does not travel across a network.

- **File Infectors** - File infectors, a second type of virus, can attach themselves to executable files, such as files with the extension .COM, .EXE, .DLL, .OVR, or .OVL. When the file is run, the virus, which operates in memory, spreads by attaching itself to other executable files. These types of viruses usually cause problems on LAN servers that run local applications shared by multiple systems. Unlike boot sector viruses, they can travel via a network as e-mail attachments or via file transfers. Gateway-based antivirus products stop the spread of these network-transported viruses by intercepting them at the network perimeter.
- **Macro Viruses** - The macro virus represents the second generation of virus threat and spreads by means of macro instructions that are found in office applications such as Microsoft Word or Excel spreadsheets. The macros are typically stored as part of a document and can be transported as attachments to e-mail messages. Any application that supports automatically executable macros is a potential carrier for macro viruses, and because of the increasing use of the Internet, macro viruses are becoming more and more problematic. When a file containing an infected macro is used, the infected file reproduces the virus into an application from which it will infect other Word or Excel files. These type of viruses are not detected by traditional scanning engines, but can be detected using a heuristics approach.
- **Stealth Viruses** - Stealth viruses hide from both the operating system and antivirus software by residing in memory and intercepting attempts to use the operating system via system calls. The virus hides, from both users and the antivirus software, the changes it makes to file size, directory structure, and/or other operating system aspects. Stealth viruses must be detected while they are in memory. Once found, they must be disabled in memory before the disk-based components can be corrected.
- **Polymorphic Viruses** - Polymorphic viruses are encrypted viruses that change their appearance with each infection. They are difficult to detect because they hide from the antivirus software. In addition, these types of viruses complicate the AV software procedure because they alter the encryption algorithm with each infection.

- Multipartite Viruses- Multipartite viruses infect both boot sectors and executable files. They can combine some or all of the stealth techniques, along with polymorphism to prevent detection.
- 4.1.2. Other Types of Malicious Code - In addition to the above types of viruses, there are other types of malicious code that have become more serious recently because of the ease with which they are distributed.

- Worms, for example, reside in memory and duplicate themselves throughout the network without user intervention. A worm spreads from one machine to another and can take advantage of the Internet to spread. Some of the most pernicious outbreaks recently, such as Melissa, have been worms.
- Trojan Horses - Although Trojan horses are an elementary form of malicious code, they are still very problematic, particularly with the growth in use of Microsoft ActiveX and Sun Java applets. Trojan horses are not really viruses because they do not propagate themselves. Rather, they attack specific computers by enticing unsuspecting users into executing a command that appears benign. These commands can include seemingly innocent activities, such as initiating a screen saver, accessing an e-mail attachment, or downloading executable files from an untrusted Web site, which can then execute commands to destroy files or to give a hacker access to system files. When a file containing an infected macro is used, the infected file reproduces the virus into files or to give a hacker access to important system files. Although the Trojan horse does not inherently self-replicate, the introduction of and increase in use of Microsoft ActiveX control and Sun Java applet technology has increased the opportunity for Trojan horses to spread dramatically. Trojan horses can be used by hackers to enter the network, where upon they utilize Hypertext Transfer Protocol (HTTP) to establish communications.

Other types of Trojan horses can turn on a user's camera or microphone and record conversations and retransmit them. Others are programs, such as Back Orifice, NetBus, or PrettyPark, which are marketed as legitimate software products with legitimate functions, but which can be used by hackers to penetrate a network. BackOrifice and NetBus are essentially remote administration tools that are installed as a server. A hacker with the corresponding client software can gain control of the system and eavesdrop, download files, or shut down the system. PrettyPark is spread as an e-mail attachment that logs users onto an Internet Relay Chat channel that can download passwords or credit card numbers.

- 4.2. Implement a protection architecture that guards against intrusion via the use of Instant Messaging. Instant messaging is essentially realtime online e-mail that is provided by services such as AOL's ICQ and Instant Message, Yahoo Chat, Microsoft's MSN Messenger, and Tribal Voice's PowWow. The Instant Messenger attachments typically bypass firewalls or gateways that scan for malicious content; if the content is encrypted either through the use of secure socket layer (SSL) or VPN services, detection is more difficult.
 - 4.3. Report each virus or malicious code infection to the Statewide Infrastructure Protection Center (SIPC), within one hour of the occurrence, utilizing the SIPC incident reporting form and process.
 - 4.4. Scan all incoming e-mail for the existence of malicious code.
 - 4.5. Protect all workstations and servers with virus-scanning software that has "notify and clean" enabled by default and that prevents users from disabling it. Agency policy shall expressly prohibit disabling of virus-scanning software.
 - 4.6. Apply appropriate inoculants and patches for each virus or malicious code infection.
- 5. DEFINITIONS AND ABBREVIATIONS**
Refer to ~~both~~, the PSP Glossary of Terms ~~and the PSP Glossary of Abbreviations~~, for definitions and abbreviations.

6. REFERENCES

6.1. Developmental

- 6.1.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.1.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.1.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.1.4. A. R. S. § 41-1461, “Definitions.”
- 6.1.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 6.1.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.1.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.1.8. A. R. S. § 41-3501, “Definitions.”
- 6.1.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.1.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.1.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.1.12. Arizona Administrative Code, Title 2, Chapter 7.
- 6.1.13. Arizona Administrative Code, Title 2, Chapter 10.
- 6.1.14. Arizona Administrative Code, Title 2, Chapter 18.
- 6.1.15. Statewide Information Technology Policy P100.
- 6.1.16. Statewide IT Security Policy P800.

7. ATTACHMENTS

None