Malicious Code, Spam and Spyware Protection Policy Sample

(Sample written policy to assist with compliance))

1.0 Purpose

To establish requirements which must be met by all computers connected to [*agency name]* networks, to ensure effective malicious code, spam and spyware protection.

2.0 Scope

This policy applies to all [*agency name]* systems with or without Internet access throughout the network and on all workstations, servers, and mobile computing devices on the network.

3.0 Policy

[Agency name] shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network.
[Agency name] shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

[Agency name] shall implement spam and spyware protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers). Spyware protection will be employed at workstations, servers, and/or mobile computing devices on the network.

[Agency name] will use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet access, and removable media.

4.0 Prevention of malicious code problems

- Always run the corporate standard.
- Run the current version and install anti-virus software updates as they become available.
- Anti-virus software is to be enabled on all workstations and servers at start-up and employ resident scanning.
- Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways.
- On servers, update virus signatures files immediately, or as soon as possible, with each new release.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk-sharing with read/write access unless there is absolutely an agency requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Always scan any media that is brought into the agency before introducing it to the network.

5.0 Detection

Any activities with the intention to create and/or distribute malicious programs into [a*gency name]*’s networks (e.g., viruses, worms, Trojan horses logic bombs, etc.) are prohibited. Virus-infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on your workstation and the anti-virus software can not eliminate the virus, please contact [a*gency Representative]*. **DO NOT TURN OFF** your computer, it will be quarantined and taken off of the network until it can be scanned and re-imaged with the operating system image.

6.0 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. *Refer to Acceptable Use Policy and Disciplinary Policy.*

Other Related Resources:

- Acceptable Use Policy (Not Required)
- Disciplinary Policy (Required)