

**Guidelines for effective implementation of
Anti-Virus and Anti-Spam in NICNET**

(February 2007)

**Government Of India
Ministry Of Communications and Information Technology
Department of Information Technology
National Informatics Centre**

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified Audience</i> <i>NICNET Administrators and Users</i>
Version <i>1.0</i> Date of last change <i>Feb 22, 2007</i>
Status <i>Accepted</i> Document No. <i>NIC-MAV(NICNET OPERATIONS)-001</i>

Table of contents:

- A) Introduction**
- B) Responsibilities of Network Team on site**
- C) Responsibilities of end user (to be circulated within Bhawan/Ministry)**
- D) Guidelines to be submitted to the IT Head of each Bhawan/Ministry**

(NOTE) A few points mentioned in the document might appear more than once under different heads, indicating responsibilities that need to be assigned to the Network Team, End User and IT Head.

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified</i> Audience <i>NICNET Administrators and Users</i>
Version <i>1.0</i> Date of last change <i>Feb 22, 2007</i>
Status <i>Accepted</i> Document No. <i>NIC-MAV(NICNET OPERATIONS)-001</i>

(A) 1. Introduction

1.1. Background

A set of technical and procedural controls are required to safeguard systems against viral and worm contamination. In addition to these, user awareness and good working practices are also essential to deliver the required degree of protection.

1.2. Applicability

These guidelines apply to the Network Administrators/End Users/IT Heads of all States/Bhawans/Ministries where the NICNET network is the backbone for Internet Access. It is the responsibility of the NICNET Network Administrator to adhere fully with its requirements and to bring relevant details to the notice of their users/IT Heads.

(B) Responsibilities of Network Team on-site:

3. Malicious Code strategy :

3.1 Malicious code Protection

Although NICNET's **malicious code** protection is very robust, there is always a delay between a new **virus** being released and anti-**virus** software producers updating their products:

- 1) Anti-Virus Group at NICHQ and its support staff who monitor and discover **virus** contamination on any of the clients/server will post the list of infected IP's on the antivirus website i.e. <http://antivirus.nic.in>. **No alerts will be sent over email.**
- 2) The primary responsibility of controlling and preventing malicious code lies with the respective state and bhawan administrator. The team in HQ is a support system and needs to be used as such. **They will provide technical telephonic/email support only.** Regular training sessions will be conducted at HQ for the support staff assigned at various sites.
- 3) Details of the current anti-**virus** software available within NICNET can be found at <http://antivirus.nic.in> and the Anti-Virus Policy is available on the NICNET Security site (<http://security.nic.in>)

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified Audience NICNET Administrators and Users</i>
Version <i>1.0 Date of last change Feb 22, 2007</i>
Status <i>Accepted Document No. NIC-MAV(NICNET OPERATIONS)-001</i>

- 4) Automatic anti-**virus** software updates will be provided centrally to all states and bhawans. It is the responsibility of the Network Team at each State and Bhawan to ensure constant connectivity between the Child server and Parent console in NICHQ
- 5) Users in each state/bhawan will be told to only let authorized personnel rectify the problems of their clients and a single point of contact would be made available to them. This would ensure continuity in terms of IP allocation , software loading and system naming.
- 6) In order to monitor NICNET mail traffic and application of uniform security policies, all incoming email must be routed through the NICNET core mail servers (mail gateways) .
- 7) Using security tools (IPS , Firewall) **Cyber Security Group** will monitor email traffic for signs of **virus/worm** contamination and mail servers/clients that are found to be passing infected emails (From and To) will be blocked from the network.
- 8) **Messaging Group** will block e-mail attachment types that could constitute a risk of **virus** introduction. The list of banned file attachment types will be reviewed periodically by the Messaging Group. A list of currently blocked e-mail attachment types include **scr,pif,exe,dat,bat,com,dll,vbs**.

3.2 Dealing with Contaminated E-mail

- 1) NICNET has implemented controls to block executable email attachment types that are known to have security weaknesses and which are used by attackers to carry **virus** payloads.
- 2) However, in order to facilitate legitimate transaction of executable files, files that are 'zipped' and sent as a .zip attachment to an email are not normally blocked.
- 3) Occasionally viruses are spread via any mode of attachment type . As soon as the Group becomes aware of a new **virus** spreading this way a temporary ban on attachments will be imposed pending receipt of updated anti-**virus** software.
- 4) During such periods, all emails containing the infected attachment type will not be accepted until the **virus** protection has been updated (generally between 4 and 24 hours) after which they will be allowed through. The Anti-Virus website will have all relevant alerts in this regard.

3.3 Technical and Procedural Controls

- 1) Day-to-day operations and monitoring including updation of patterns and patches of the AV server is the responsibility of the Local onsite Administrator.

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified Audience NICNET Administrators and Users</i>
Version <i>1.0 Date of last change Feb 22, 2007</i>
Status <i>Accepted Document No. NIC-MAV(NICNET OPERATIONS)-001</i>

- 2) The manpower made available (through Facility Management) to each state/bhawan will do the needful in terms of patching and cleaning . Subsequent to cleaning, the infected IP's listed on the Anti-Virus website should be deleted.
- 3) The onus of making the hardware available (**based on configuration indicated in Annexure A**) lies with the local administrator of each site/ IT Head of respective Bhawan/Ministry.
- 4) IP binding (to MAC address) is mandatory in order to ensure client identification and continuity.
- 5) The administrator of each site will ensure that each desktop and server is configured with anti-virus software products to protect desktop ,servers and laptop computers .
- 6) Latest Anti-Virus pattern cannot ensure an infection free client , unless the latest Operating system patches are also installed, the Network Team needs to ensure the same.
- 7) Sharing of hard disks across clients/systems is not allowed.
- 8) The administrators need to collect the CD's containing the Anti-Virus software for Dial-up Users (refer 4.2 below) from the NICNET Anti-Virus Help Desk in NICHQ.

(C) Responsibilities of End User (to be circulated to all users within the Bhawan/Ministry) :

4.1 Clients on local LAN

- 1) **In order to implement IB directives, servers/clients that are infected will be automatically taken off the network and reconnected only after cleaning.**
- 2) NICNET would NOT connect systems on the NICNET network loaded with Windows 95 and windows 98.This is being done as Microsoft has withdrawn support for these Operating systems, resulting in no patch updates (**refer Annexure B(a),B(b)**) . If required these systems can be used in a standalone mode, assuming that the system has the required hardware configuration and can be loaded with a standalone Anti-Virus software.
- 3) Clients without Anti-Virus software (as provided by NICNET) will not be allowed to connect to NICNET.
- 4) Single point of contact will be maintained across Bhawans/Ministries in case of any problem in the client. The problem can pertain to hardware/operating system/virus infection etc. **Users may not contact the vendor directly, the request may be routed/lodged through the on-site NIC Network team. In the**

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified Audience NICNET Administrators and Users</i>
Version <i>1.0 Date of last change Feb 22, 2007</i>
Status <i>Accepted Document No. NIC-MAV(NICNET OPERATIONS)-001</i>

eventuality of a team not being present, as per IB directives, in case a vendor needs to be called for troubleshooting, the presence of an authorized person is mandatory.

- 5) Sharing of hard disks across clients/systems is not allowed.
- 6) The end user has to ensure that his/her client has the latest Operating system, patches installed.
- 7) The clients and servers need to have legal copies of the Operating system so that updates of patches are not an issue. This can only be ensured with strict adherence to point no 4 above.
- 8) Clients spreading malicious traffic will be disconnected from the network without warning.
- 9) Users are advised not to open mails from unknown users.
- 10) Users are also advised not to open attachments which have no relation to their field of work as it could be malicious.
- 11) Users should check the status of their Anti-Virus software everyday. For details , indicating status go to <http://antivirus.nic.in/> → downloads => client icon status.
- 12) Users should immediately inform the Network control room if their software indicates a problem

4. 2Dial-Up users

If the users are connected through NICNET Dial-Up, the anti-virus software is mandatory , prior to connectivity.

- 1) The software will be made available through CD's for a one time installation. Subsequent updates can be done over internet.
- 2) Users can have the same collected from the NICNET Network control room in their respective bhawans/ministries.
- 3) Dial-up users choosing to use a software other than that provided by NICNET, need to ensure that the same is updated regularly.
- 4) The client needs to have the latest Operating system patches installed .

4.3 Servers configured on NICNET IP.

- 1) **In order to implement IB directives, servers/clients that are infected will be automatically taken off the network and reconnected only after cleaning.**
- 2) Servers without Anti-Virus software (as provided by NICNET) will not be allowed to connect to NICNET.

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified Audience NICNET Administrators and Users</i>
Version <i>1.0 Date of last change Feb 22, 2007</i>
Status <i>Accepted Document No. NIC-MAV(NICNET OPERATIONS)-001</i>

- 3) Single point of contact will be maintained across Bhawans/Ministries in case of any problem in the server. The problem can pertain to hardware/operating system/virus infection etc. **Users may not contact the vendor directly, the request may be routed/lodged through the on-site NIC Network team. In the eventuality of a team not being present, as per IB directives, in case a vendor needs to be called for troubleshooting, the presence of an authorized person is mandatory.**
- 4) The Server Administrator has to ensure that his/her server has the latest Operating system, patches installed.
- 5) The servers need to have legal copies of the Operating system so that updates of patches are not an issue. This can only be ensured with adherence to point no 3 above.
- 6) Servers spreading malicious traffic will be disconnected from the network without warning.
- 7) Server Administrators should check the status of their Anti-Virus software everyday. For details , indicating status go to <http://antivirus.nic.in/> → downloads => client icon status.
- 8) Servers should NOT be used for the purpose of Internet browsing. Only selected and trusted sites can be accessed for the purpose of updation of virus patterns/OS patches.
- 9) Servers configured as web servers, need to have in place a mechanism of scanning files that are being uploaded for site updation. Infected files should be dropped during the process of uploading.

(D) Guidelines to be submitted to the IT Head of each Bhawan/Ministry

- 1) **In order to implement IB directives, servers/clients that are infected will be automatically taken off the network and reconnected only after cleaning.**
- 2) No client/server can be connected to NICNET, without prior intimation to NIC Network Team . They will do the needful in terms of ensuring patches and anti-virus software before connecting it to NICNET.
- 3) NICNET would NOT connect systems on the NICNET network loaded with Windows 95 and windows 98.This is being done as Microsoft has withdrawn support for these Operating systems, resulting in no patch updates (**refer Annexure B(a),B(b)**) . If required, these systems can be used in a standalone mode, assuming that the system has the required hardware configuration and can be loaded with a standalone Anti-Virus software.

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Classification <i>Unclassified Audience NICNET Administrators and Users</i>
Version <i>1.0 Date of last change Feb 22, 2007</i>
Status <i>Accepted Document No. NIC-MAV(NICNET OPERATIONS)-001</i>

- 4) Clients/servers without Anti-Virus software (as provided by NICNET) will not be allowed to connect to NICNET.
- 5) The onus of making the hardware available (**based on configuration indicated in Annexure A**) lies with the local administrator/IT Head of respective Bhawan/Ministry.
- 6) Single point of contact will be maintained across Bhawans/Ministries in case of any problem with the client. The problem can pertain to hardware/operating system/virus infection etc . **Users may not contact the vendor directly, the request may be routed/lodged through the on-site NIC Network team. In the eventuality of a team not being present, as per IB directives, in case a vendor needs to be called for troubleshooting, the presence of an authorized person is mandatory.**
- 7) Sharing of hard disks across clients/systems is not allowed.
- 8) Users/Deptt who prefer to update anti-**virus** software under their own arrangements need to ensure that the client/server has the latest Operating system patches and Virus patterns.
- 9) In case any other Anti-Virus software is being used, the daily reports will be generated by the respective Administrators and made available to an authorized person , if required.
- 10) If the software, as provided by NICNET, is not installed on the clients, then NIC will not be responsible for maintaining the system and it would be disconnected in case it effects the NICNET Network.

Name of the Document <i>Guidelines for Effective Anti-Virus and Anti-Spam Implementation</i>
Document Maintained by: <i>Seema Khanna</i>
Version <i>1.0 Date of last change Feb 22, 2007</i>

Annexure A
System Requirements of Officescan/TMCM/IWSS

Officescan (7.3)	TMCM (3.5)	IWSS (2.5)
Officescan Server :-		
1. Windows 2000 or Windows Server 2003. 2. Microsoft™ Internet Explorer 5.5 or later. 3. Microsoft Internet Information Server (IIS) 4.0 or higher. 4. Minimum CPU Pentium-IV, 2 GB of RAM; 1GB of disk space or above. 5. Approx. no. of Clients:- 2500	1. Windows 2000 or Windows Server 2003. 2. Microsoft™ Internet Explorer 5.5 or later. 3. Microsoft Internet Information Server (IIS) 4.0 or higher. 4. Minimum CPU Pentium-IV, 2GB of RAM; 1GB of disk space or above. 5. Microsoft SQL Server 2000 (2000 + Service Pack 3 is recommended) 6. Approx. no of products managed:- 500	1. Windows 2000 or Windows Server 2003. 2. 1GB RAM without URL filtering; 2GB RAM with URL filtering. 3. PC with an Intel Pentium™ 4 2.4GHz processor or above. 4. 2GB disk space for program files with URL filtering installed. 5. Microsoft™ Internet Explorer 6.0. 6. Microsoft™ SQL Server 2000. 7. Approx. no of concurrent connections:- 500
Officescan Client :-		
1. Minimum 256 MB RAM or above. 2. Minimum 200 MB Hard Disk Space or above. 3. Minimum Pentium-III processor or above. 4. Windows XP/Windows Server 2000/ Windows 2000 Professional/ Windows Server 2003. 5. Microsoft Internet Explorer 6.0 or later.		

ANNEXURE B(a)

Quick Links

Home

Worldwide



Search
Microsoft.com for:

Windows Home

[Windows Home](#)

[End of support for Windows 98, Windows Me, and Windows XP Service Pack 1](#)

Products

Windows XP

Published: January 6, 2006 | Updated: May 22, 2006

On This Page

Windows Vista

[End of support for Windows 98 and Windows Me](#)

Plus!

Servers

[End of support for Windows XP Service Pack 1](#)

Windows Embedded

Windows Mobile

[Resources](#)

Microsoft Virtual PC

Other Versions

Technologies

Internet Explorer

Windows Media Player

DirectX

Windows Desktop Search

Resources

Downloads

Trial Software

Communities

Support

Training & Events

Windows History

Windows Security

Microsoft Worldwide

Microsoft At

End of support for Windows 98 and Windows Me

July 11, 2006 will bring a close to Extended Support for Windows 98, Windows 98 Second Edition, and Windows Me as part of the Microsoft Lifecycle Policy. Microsoft will retire public and technical support, including security updates, by this date.

Existing support documents and content, however, will continue to be available through the [Microsoft Support Product Solution Center Web site](#).

This Web site will continue to host a wealth of previous How-to, Troubleshooting, and Configuration content for anyone who may need self-service.

Microsoft is retiring support for these products because they are outdated and can expose customers to security risks. We recommend that customers who are still running Windows 98 or Windows Me upgrade to a newer, more secure Microsoft operating system, such as [Windows XP](#), as soon as possible.

Customers who upgrade to Windows XP report improved security, richer functionality, and increased productivity.

End of support for Windows XP Service Pack 1

On October 10, 2006, Microsoft will end all public assisted support for Windows XP Service Pack1 (SP1). After this date, Microsoft will no longer provide any incident support options or security updates for this retired service pack under the policies defined by the [Microsoft Support Lifecycle policy](#).

To enhance the security of your computer and to continue to receive updates for Windows XP, we recommend you [upgrade your computer](#), for free, to Windows XP Service Pack 2 (SP2).

Enterprise customers

Microsoft will, under qualified conditions, make Custom Support Agreements (CSA) available for eligible enterprise customers. CSA customers are also encouraged to consider migrating to Windows Vista as part of their migration plan. Customers may qualify for a CSA if they have a current Premier support agreement, and a detailed migration plan moving them from Windows XP SP1 to the latest operating system. To learn more about Custom Support Agreements, contact your Premier support Technical Account Manager (TAM).

[↕Top of page](#)

Resources

Need to upgrade your software?

If you don't yet have Windows XP: [Learn how to upgrade to Windows XP Professional](#)

If you already have Windows XP: [Learn how to upgrade to Windows XP SP2 for free](#)

Buying a new computer?

[Consider a Media Center PC with Windows XP Media Center Edition 2005](#)

[↕Top of page](#)

ANNEXURE B(b)

Quick Links

Home

Worldwide



Search
Microsoft.com for:

Windows Home

[Windows Home](#)

[Windows Life-Cycle Policy](#)

Products

Windows XP

Published: October 15, 2002 | Updated: July 7, 2006

Windows Vista

Plus!

Servers

Windows Embedded

Windows Mobile

Microsoft Virtual PC

Other Versions

Technologies

Internet Explorer

Windows Media Player

DirectX

Windows Desktop Search

Resources

Downloads

Trial

Software

Communities

Support

Training & Events

Windows History

Windows Security

Microsoft Worldwide

Microsoft At



On October 15, 2002 Microsoft announced a new support life-cycle policy. This consistent and predictable policy is designed to standardize support guidelines across product lines and will cover most products currently available via retail purchase or volume licensing and future release products.

Product life-cycle policies provide advanced notification of planned changes in product availability and support. This information helps customers and partners with product planning and information technology decisions.

The links on this page provide access to specific information about Windows products.

Product Life-Cycle Information for:

- [Windows 2000 Server](#)
- [Internet Explorer](#)
- [Windows Media Player 9 Series](#)
- [Windows Embedded](#)
- [Windows Lifecycle FAQ](#)

[Top of page](#)

Windows Desktop License Availability

Under the Support Lifecycle policy Windows desktop licenses are available for four years after general availability in all standard product distribution channels (e.g. direct OEM, System Builders, retail, and Volume Licensing programs via licenses or via downgrade rights). Licenses will continue to be available through downgrade rights available in Volume Licensing programs after end of general availability.

License Availability Roadmap

Desktop Operating Systems	Date of General Availability	Direct OEM and Retail License Availability (end date)	System Builder License Availability (end date)
MS DOS 6.xx	June 1, 1994	November 30, 2001	November 30, 2001
Windows 95	August 15, 1995	December 31, 2000	December 31, 2001
Windows NT Workstation 4.xx	July 29, 1996	June 30, 2002	June 30, 2003
Windows 98	June 30, 1998	June 30, 2002	November 30, 2003 ¹
Windows 98 SE	June 30, 1999	June 30, 2002	March 31, 2004 ¹
Windows Millennium Edition (Windows Me)	December 31, 2000	December 31, 2003	June 30, 2004
Windows 2000 Professional	March 31, 2000	March 31, 2004	March 31, 2005
Windows XP Professional	December 31, 2001	12 Months Following Windows Vista General Availability ²	24 Months Following Windows Vista General Availability ²
Windows XP Tablet PC Edition	February 11, 2003	12 Months Following Windows Vista General Availability ²	24 Months Following Windows Vista General Availability ²
Windows XP Professional x64 Edition	April 25, 2005	12 Months Following Windows Vista General Availability ²	24 Months Following Windows Vista General Availability ²

Windows XP Home Edition	December 31, 2001	12 Months Following Windows Vista General Availability ²	24 Months Following Windows Vista General Availability ²
Windows XP Media Center Edition³	October 28, 2002	12 Months Following Windows Vista General Availability ²	24 Months Following Windows Vista General Availability ²

¹ In the US and Canada only System Builder License Availability end dates are June 30th 2003 for Windows 98 and September 30th 2003 for Windows 98 SE.

² Precise dates to be finalized closer to the release of Windows Vista

³ Includes the 2002, 2004, and 2005 editions of Windows Media Center

[↩Top of page](#)

Windows Service Pack Roadmap

Microsoft continually works to improve its software. As part of this effort, we develop updates and fixes to recognized issues and release them for customers. On a regular basis, we combine many of these fixes into a single package and make the package available for installation. These packages are called Service Packs. Based on feedback from customers and partners Microsoft is committed to providing a 12 month roadmap of upcoming service packs and security rollup packages on the [Windows Service Pack Roadmap Web page](#). Visit the [Supported Service Pack list](#) to find the support timelines for a particular product's service pack.

[↩Top of page](#)