एन एम डी सी
NMDC

VIRUS PROTECTION POLICY

Author		**Document name**		**Date of first issue**	
Owner	C & IT Department	**Document ref. no.**		**Date of latest re-issue**	
Version	1.1	**Page**	1 of 10	**Date of next review**	
Issue Status	Under Review/ Live	**Security classification**	Internal use only	**Reviewer**	

एन एम डी सी

NMDC

VIRUS PROTECTION POLICY

VERSION CONTROL

Revision no.	Date of issue	Prepared by	Reviewed by	Approved by	Issued by	Remarks

एन एम डी सी
NMDC

VIRUS PROTECTION POLICY

OBJECTIVE

The purpose of this policy is to ensure the protection of the NMDC`s computer systems against virus infection by providing the required technical support for timely distribution of antivirus software, its updates and upgrades as well as ensure prompt escalation of virus incident reporting and management. NMDC protects its IT resources from all possible computer virus and related threats by deploying the procedures and best practices.

SCOPE

This policy applies to all NMDC staff as well as to the third parties, and all NMDC information resources including corporate data, as well as the application and systems software.

RESPONSIBILITY

NMDC has an IT Support team staffed by third party IT Support Executives. The Security Officer IT in co-ordination with security executives will be responsible for the implementation of the policy and procedures for Virus protection.

The Security Manager, Security Officer, Security Executives along with all users (employees and external resources) at NMDC will be responsible for overall Virus Protection for NMDC.

POLICY RULES

C&IT Department's Responsibilities

The IT Support team will:

1. Provide total technical support for prevention, detection, reporting and eradication of computer viruses.
2. Provide training to the users on virus protection. Work with participating departments to install virus software on all computers.
3. Maintain and upgrade the antivirus solution deployed for the enterprise.
4. Assist individuals with recovery from infections by providing swift and accurate advice and assistance at the level the user and the situation require. This includes containment to stop the spread, disinfecting to clean the system, and the capture of incident information for future use.
5. Perform trend analysis to locate problem areas and identify high-risk areas where special actions may need to be taken. In cases of risk to other department/ location systems, take appropriate action to thwart the spread of the virus.
6. Configure computer systems to perform frequent auto-scans for viruses.

User's Responsibilities

1. It is the responsibility of all the IT users to protect their information systems from possible computer virus attacks.

एन एम डी सी
NMDC

VIRUS PROTECTION POLICY

2. For the systems not a part of the corporate network (which do not pick up the updates from the central server automatically) it will be the responsibility of the user of that system to update virus protection software frequently (weekly at a minimum).
3. Exercise extreme caution when opening attachments. Never open an attachment unless it is expected even if it is from a trusted user.
4. Report all virus incidents to the IT Helpdesk. Provide the following information if known: virus name or type, extent of infection (single PC, LAN, etc.), source of virus, and potential recipients of infected material.
5. Perform regular backups of the data on individual desktop system.

Updates of Virus 'DAT files'

These are the files, which contain the data on virus signatures. The updation of the virus signatures would be automated as much as possible. The updates would be performed at three levels

1. **Gate way:** The software would be configured such that it downloads the antivirus definitions automatically as and when required. It will scan all incoming and outgoing messages at the SMTP gateway.
2. **Mail & other servers:** The updates would be automated. The system administrators along with Security Executives may also perform virus definition updation for these servers manually. The Helpdesk will download the data from the Internet website of the respective antivirus vendor site.
3. **Client computers/network nodes:** Once the updates of virus DAT files are copied on the central host computers (servers), an operating system job will be scheduled in the network server for pushing these DAT file updates onto client computers/network nodes connected. This job will be scheduled every week immediately after copying the DAT files on the central host computers.

Antivirus software upgrades

The upgrades are the newer versions of the antivirus software. The antivirus software will automatically update its signatures from the internet and distribute to all its clients located in the network. For the machines / servers not a part of the network it is the responsibility of the concerned users and Security Executives to provide newer versions/engines of antivirus programs in regular and timely manner.

Specific virus protection procedures

1. It should be ensured that antivirus (AV) software is installed on all servers, gateway and client and would always be active.
2. Antivirus at the gateway would detect and remove viruses from inbound and outbound SMTP, FTP, and HTTP traffic in real time.
3. The Gateway should stop any message containing VBS scripts as attachments – this prevents viruses such as 'Melissa' and 'Loveletter' from spreading.
4. The Gateway antivirus system should stop any message containing any executable programs e.g. .EXE files, as attachments to prevent Trojans and viruses such as Navidad and MTX from spreading
5. Appropriate protection should be enforced so that the users cannot disable the antivirus check.
6. The scheduler should run the AV software at least once in a day and it should be properly scheduled, preferably during the lunch hours of the office. Users should not be able to stop the antivirus check.
7. Every diskette, CD and DAT tape should be scanned for virus before use.

VIRUS PROTECTION POLICY

8. Systems should be implemented to review the antivirus software activity/logs, especially to check whether the IT users are running the AV system regularly on their desktop computers. In case the user has the AV software and does not run it for stipulated number of times, his user id should be recorded and his network account should be disabled. This should immediately be informed to the Security Officer
9. Upon encountering the virus problem, the AV software should clean the infected files and send an alert to the user. Also the AV software must be configured to disconnect the user from network resources. The other options such as 'continue' and 'move to a directory' in AV check should not be enabled.
10. **Antivirus for messaging:** The messaging system is implemented for the messaging system. If the virus is found in mail attachment file, this file must be quarantined and the sender should be informed. The recipient would get the remaining message.
11. The DVD drives of all desktops/laptops must be disabled unless and until there exists a valid business justification.
12. The user desktops/laptops should not be configured for any shares. This will restrict the spread of virus to other systems to an extent. All the data that needs to be shared should be stored on a dedicated server from which users can retrieve/store their data.
13. **Checking the software downloaded from Internet:** Software/data downloaded from outside sources such as Internet may contain virus. In order to provide more security, the person downloading from external source, should log out of all files servers and terminate all other network connections. Before executing the software, it should be screened with the approved antivirus package. If a virus is detected, the Security Executive should be notified immediately and no further work should be carried on the affected machine until the virus has been shown to be eradicated.

Virus reporting (for cases which are not automatically cleaned or quarantined by the AV)

1. Upon encountering such virus attack, the users should immediately stop using the involved computer and report it to Security Executive and the IT Support team. The antivirus system should report / alert the security executive about the existence and eradicate the virus.
2. The eradication of virus problems by Security Executive alone would ensure that infections are centrally reported. The virus logs utility in AV check software must always be enabled and the logs will be reviewed by Security Executive and periodically by the Security Officer (IT). On encountering such virus, the detailed virus log should be printed and submitted to Head IT Systems. The log should also capture the virus itself so that the IT Support team can subsequently update its software to detect new viruses as well as mutated versions of old viruses.
3. All such virus incidents must be reported by users to the IT Support team immediately. The helpdesk in turn should take necessary action and report the incidents to the concerned Security Executive, on the similar lines of procedures given for Incident Management.
4. If such virus is reported in any of the sites, a notice to the other sites should be sent.

Virus Detection & Prevention Tips

1. Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.

एन एम डी सी

NMDC

VIRUS PROTECTION POLICY

2. Do not open any files attached to an email unless you know what it is, even if it appears to come from someone you know. Some viruses can replicate themselves and spread through email.
3. Do not open any files attached to an email if the subject line is questionable or unexpected. If the need to do so, always save the file to your hard drive before doing so.
4. Delete chain and junk emails. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
5. Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an antivirus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own antivirus software.
6. Update the antivirus software regularly as over 500 viruses are discovered each month. These updates should be at the least the products virus signature files.
7. Back up the files on a regular basis. If a virus destroys the data files, they can be replaced with the back-up copy. The backup files must be stored in an off-site location.
8. When in doubt, user should not open, download, or execute any files or email attachments.