अमर उजाला
हर सवेरे नया जोश
नया उजाला

Antivirus Policy

Ver 1.0

Table of Contents

1. Overview

This defines anti-virus policy on all machines including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It also defines the best practices to prevent virus definitions.

2. Purpose

This policy is designed to protect the organization's resources against intrusion by viruses and other malware.

3. Scope

The organization will use a single product for anti-virus protection which is McAfee. This product will be reviewed periodically and IT reserves the right to change the product in order to meet the future needs. The following minimum requirements shall remain in force:

- The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
- The anti-virus library definitions shall be updated at least once in a day.
- Anti-virus full scans shall be done a minimum of once per week on all user controlled workstations and servers.
- No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.
- All Amar Ujala owned machines will be covered in this policy.

4. Policy

4.1 System Scan

- IT will ensure to install antivirus in all the machines issues to end users.
- IT will install anti-virus software on all desktop workstations, laptops, and servers.
- A scheduled virus scan will happen every Wednesday of the week between 12:00PM to 4:00PM to scan the active machines for virus/malware. During this scan you might experience slowness in your machines performance.
- The updation of signatures will be real-time as per the schedule of McAfee server.
- The anti-virus will attempt to clean the infected files and if it fails to clean, the respective files will get quarantined or deleted.
- Once the files are quarantined/deleted by the anti-virus, IT will not be responsible to recover such Files.
- It will be user's responsibility to scan the additional storage devices like DVD, USB drives before use.
- Any activity intended to create and/or distribute malicious programs onto the Amar Ujala network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.

- If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the IT immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

- No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from IT.

- Any virus-infected computer will be immediately removed from the network until it is verified as virus-free.

- It will be user's sole responsibility to ensure that their machine is running with latest antivirus updates.

4.2 Email Malware Scanning

McAfee has the capability to scan the emails for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored emails in the machine once in a week for viruses or malware.

When a virus or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true.

5. Guidelines: Best Practices for Virus Prevention

5.1 Always run the standard Anti-virus software provided by the organization

5.2 Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

5.3 Never open files or macros attached to an e-mail from an unknown source (even a coworker) if you were not expecting a specific attachment from that source.

5.4 Be suspicious of e-mail messages containing links to unknown web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link. Report such links to IT immediately.

5.5 Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

5.6 Avoid direct disk sharing with read/write access. Always scan any removable media for viruses before using it.

5.7. If instructed by IT to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

5.8. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

6. Policy Compliance

6.1 Compliance Measurement

The Infosec team of IT will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, remote monitoring, business tool reports, internal and external audits, and provide feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved by the Infosec team of IT in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action as per Amar Ujala's policy

7. Definitions and Terms

Organization mentioned in the document means Amar Ujala.

Machines mentioned in the document means Desktops, Laptops, Workstations and Servers

8. Revision History

Date of Change	Responsible	Summary of Change
Nov 2014	IT Helpdesk Team	