TechSture
Technologies

Anti Virus Policy

Document Number TT-ITP/03

Document Release Note

Document Version	1.0	**Release Date**	

Prepared By		**Approved By**
Pathik Patel		**Chetan Patel**

Document Revision History

Version	Date	Change Description	Modified By	Reviewed By	Approved By
1.0					

Purpose

This policy defines enforcement of an antivirus system to protect, clean and quarantine information systems and resources against virus threats. It defines how data entering in the local network (in form of email attachments, client data, internet downloads) to be examined for authenticity, classify its category and respond with necessary action to make sure no threats affect the defined functionality of the information systems of TechSture techno

Scope

This policy applies to all servers and workstations currently owned by TechSture

Policy

It is the company's responsibility to provide a framework for supporting appropriate induction.

	DOs & DON'Ts	Responsibility
✓	All workstations must have antivirus software installed and updated before they get used in Development & Operations	IT Department
✓	The Antivirus is configured to update automatically. Random checks of desktop are done on weekly basis for latest virus definition.	IT Department
✓	Always run the standard, supported anti-virus software available from the systems Manager/Lab Manager. Download and install anti-virus software updates as they become available.	IT Department
✓	Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.	IT Department
✓	Always scan USB from an unknown source for viruses before using it.	IT Department
✓	Back-up critical data and system configurations on a regular basis and store the data in a safe place.	IT Department

✓	If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.	IT Department
✓	New viruses are discovered almost every day. Periodically check the Anti-Virus Policy and update accordingly.	IT Department
✓	The updates of the authorized Anti-virus programs are run on all machines under a control of System Administrator	IT Department
✗	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.	User
✗	Don’t allow negligence, dilution of these procedures	User
✗	Never download files from unknown or suspicious sources	User

Records

Logs of Sequrite

Effective Measures

- No. of viruses prevented once per quarter.
- No. of times formatting done due to viruses.