Desktop Usage Policy

Document No – TT-ITP/09

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 the methodology for Desktop usage.

Scope

This policy is applicable to all desktop users. This policy applies to all equipment and data owned and operated by the organization.

Policy

	DOs & DON'Ts	Responsibility
✓	Use of desktop is permitted for official use only.	Users
✓	User should login on given desktop using domain id.	IT Department
✓	Avoid direct disk sharing with read/write access unless there is absolutely a work requirement to do so.	IT Department
✓	In case of any malfunctioning of programs/slow response/hang ups or virus activity please inform to IT Department.	Users
✓	Desktop should be set with password protected screensavers when there is no activity for five minutes.	Users
✓	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 IT Department	Users
✓	Label all the desktops with their unique ID, and maintain labelling system.	Users

✓	Maintain the record of desktop ID and allocated to which person, configuration and user rights.	Users
✓	Block access by changing password as soon as authorized person leaves the organization, and provide desktop back for use to another after verifying that any confidential information has not been passed. Maintain allocation list.	Users
✓	Lock your desktop by ALT+CTRL+Del+Enter orWin+L before leaving your place for any short or long break.	Users
✓	Switch off the monitor screen in breaks for saving energy.	IT Department
✓	Shutdown the PC at the end of the day when you leave.	IT Department
✓	Sign-out properly if you have taken remote access from another PC.	Users
✓	Run firewall policies (security policy) every week on maintenance day, for ensuring security.	IT Department
✘	Users should not be provided with Admin rights. The IT Director has to approve admin rights in case of special requirements related to production/testing.	IT Department
✘	Users should not change or delete the data which have been previously stored by other users in desktop without permission of IT Department.	Users
✘	Do not share any data or your login passwords of desktops with any one.	Users

Records

Users login log

Access rights records

Effective Measures

Number of deviations with respect to above acceptable usage per month.