Policy-Computer Maintenance & Best Practices

The following are recommended best practices for keeping the staff and public computers within the company secure and functioning properly. Most of the information provided here are guidelines and do not deal with specific procedures. Please contact the IT Department for more details.

# Scope

This policy focuses on how a computer should be used and satisfy necessary precautions and also to maintenance personnel to keep equipment operating at peak reliability and companies functioning more profitably through reduced maintenance costs and increased productivity and capacity.

# Firewalls

1. Separation of internal staff access network and distribution network (Corporate, SOHO, Retail) is a mandatory requirement and is customary to all enterprise network design. Provision for a DMZ (internal access servers: MIS, HR, Finance) space must be separated and inaccessible to client network. Following ABB Inc, AT&T, Cisco Systems Inc., F5, Palo Alto, FireEye, Juniper, Huawei, EnterpriseWeb LLC, Fujitsu Limited, General Electric, IBM Corporation, SAP, RSA, Intel, Symantec, MITRE, TOGAF, Wind River’s Reference Architecture should be followed and be mapped to Link3’s requirements.
2. The central firewall, which provides intrusion protection, network address translation for the Internet connection and other security features; is maintained by NOC (Network Operation Center), in conjunction with the IT for IT Resources Access to internal office staff.
3. IT department only deals with internal network and provides productivity options towards the staff. However, it is still recommended that the laptops OS Firewall be turned on for all staff computers for computer level security. The main reason why the OS Firewall is recommended over other software firewalls is the ease of administration.

# Standard Software (Pre-Approved)

 The following applications are recommended for staff computers:

1. Adobe Reader
2. Foxit Reader
3. Adobe Flash Player
4. Mozilla Firefox or Chrome Browser
5. Microsoft Office Professional
6. System Center Endpoint Protection (Antivirus)
7. For eAudiobook use: iTunes, Windows Media Player 11 and Standard Download Manager that’s built into windows. If you are in need of a download accelerator, send the request to IT or Software request portal.
8. For eBook use: See above.
9. SNMPc for collecting valid network insights by Technical/IT team
10. EyeBeam Software for HelpDesk seats

Employees may request software such as Google Earth or Windows Live Messenger, Microsoft OneDrive, BropBox. It is up to the computer administrator or IT department to determine if these applications pose any security threats or have any other impacts on the computers, such as performance impacts, transmission of official documents over the internet etc or poses data breach possibility for organizational documents. As a general practice, other than the assigned or pre-approved software’s, you cannot install any software, as policy applies to all organizational computers. Moreover, complete pre-approved software list can be found under Annexure-A of the “Software Installation Policy.”

Furthermore, GNU open license (open source) & sharewares which are of no "threat" to network infrastructure, which should be free from malware (which will not destroy legitimate software licenses), at least digitally signed by the publisher, would be labeled "Legitimate Requirement" and users will be able to use them, and will be periodically uploaded to the "Software Center" provided in the Active Directory Computers. But cracked/patched/pirated software(s) should not be used across the system.

# Software Licensing

1. The software licensing terms will value of using licensed software across the organization, while minimizing risks/threats to the central network, compliance & penetration tasks etc. and also respecting government initiated IPR law.
2. Compromised software’s poses a direct threat to the central network, where a network crawler can disrupt access to the network resources; effect may cause network to shut down. However, if your requirement for using a software is justified, the organization will purchase licensed software and provide you the software and activate it for you. IT department will get involved into it and see through the complete installation either remotely or on site.

# Computer Maintenance

1. Activities such as performing a disk defragment and disk cleanup should not be ignored. However, on public computers with genuine OS installed, very few permanent changes are being made to the hard drive; therefore defragmenting the hard drive and performing a disk cleanup probably only need to be done once or twice in every three months.
2. On staff computers where changes are constantly being made to the hard drive, these activities may need to be performed more frequently and will be automated throughout the organization, by managed IT services.
3. Company provided devices should be kept out of reach of children; devices of such sort are not provided for personal entertainment as well.

# Privacy

1. Personally identifiable information (PII) cannot be saved or transmitted to/from your computers.
2. It is recommended that your computers need to boot up using the network hard lines and restarting at least twice a day. By doing so, IT will clear and update any changes made to the computer during the last session. This includes changes such as documents that may have been saved onto the hard drive or to the company provided secured & remote location, Internet browser history, and any other changes that a staff might have made on the computer.
3. By all means your laptop should not be unattended for longer period of time. If you leave your computer on your desk or soft desk; do always lock your computer by using the “Windows Key + L” combination, this will soft lock your computer until your return. IT will also manage your computers inactivity timeout period.

# Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# Distribution

This policy is to be distributed to all Staff members with access to Company’s Information Resources.