THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY
NETWORK POLICY

1. Purpose

The Network Policy is implemented in order to facilitate a **Mal**icious Soft**ware** (Malware) free environment and smooth network functioning. The implementation of this would reduce the likelihood that any computer system connected to a network will be able to spread computer viruses, spyware, spam and other undesirable software from one computer to another and also reduce the chance of interference of network with external sources. The policy will help users to adhere to network ethics and take the use of the network to the maximum.

2. The Terminology

The term *Segregated Networks* describes extensions of the main campus network e.g. PCs at Residences and Wireless / Wired PCs at various Hostels.

3. The Policy

The University requires that all users exercise care in connecting devices to the computer network and that connected devices do not interfere with the operation of the network or the operations of others using it.

3.1 Applicable in all areas

3.1.1 Every computer on the network should have only licensed and/ or open source Operating System(s) and Application(s).

3.1.2 Due to the multiple vulnerabilities existing on the older versions of operating systems like Windows 95/98 and thereby chances of being getting such machines exploited are higher when online. Therefore use of machines having Windows 95 or Windows 98 on the University network for Internet and Intranet access is not allowed. (Upgrade to new versions before connection).

3.1.3 Every computer must have all (applicable) currently published security fixes\patches applied as soon as possible.

3.1.4 Every machine/network device on the network should be registered online by the owner/user with the centralized database.

3.1.5 All computers connected to the University network must have an anti-virus software package installed and enabled.

3.1.6 Anti-virus software pattern files (list of detectable viruses) must be updated at least weekly.

3.1.7 *No computer system shall be used to monitor network traffic, or conduct speed or bandwidth tests. Nor shall it be used to interact with any other computer unless said remote computer is offering a specific service, which the end user is authorised to use.

3.1.8 *No computer system shall be used to interfere with the operation of the network by acting as a network device (router, switch, hub, DNS server, DHCP server, etc). Connection of switches, routers, hubs or broadcast of any wireless signal from any such device is forbidden.

3.1.9 *No computer shall act as a gateway to the network by virtue of offering dial-in, wireless or direct access to third parties.

3.1.10 Any computing device that is found to be disrupting or degrading the operation of the network service intentionally or otherwise is subject to disconnection. In extreme cases this may be done without warning.

3.1.11 The downloading/ uploading/ sharing of illegal, pirated or unlicensed content (images, software, music etc) is forbidden.

3.1.12 The group mail accounts like heads@thapar.edu, faculty@thapar.edu etc. should be judiciously used. These accounts have been created to facilitate the distribution of official e-communications and should not be used to circulate personal messages.

3.1.13 Any creation of a personal World Wide Web page or a personal collection of electronic material that is accessible to others must include a disclaimer that reads as follows: "The material located at this site is not endorsed, sponsored or provided by or on behalf of Thapar University, Patiala."

3.1.14 Personal Web pages that are maintained by University's computer account holders must not contain paid advertising. This guideline is consistent with the University's policy against use of resources for private gain or commercial purposes.

3.1.15 Internet access accounts and Email accounts are for the exclusive use of the individual to whom they were assigned. Users must not allow or facilitate access to these accounts to others. Users may not set up a proxy or anonymous re-mailer for purposes of allowing access to others.

3.1.16 Any traffic on the University's network, stripped of information content, may be monitored for operational or research purposes by the Network Management Team.

3.1.17 Recreational use is prohibited: Do not play games, Minimize the use of chat programs such as IRC, ICQ, yahoo, MSN, rediff or AIM except to access technical services, Do not log into a remote access server and then log into other machines.

3.2 Applicable to Segregated Networks:

Apart from terms and conditions laid above following clause are applicable to segregated networks.

3.2.1 The University does not guarantee the privacy or security and accepts no responsibility for loss caused by use or failure of these networks. These networks should be regarded as insecure and users are advised not to transmit any vital information over these networks unless that communication is encrypted.

3.2.2 The University will not engage in the repair or configuration of any device that is not University's property.

3.2.3 Authorized users may access University's computing equipment, systems and networks for personal uses if the following conditions are met:

3.2.3.1 The use does not overload the University's computing equipment or systems, or otherwise negatively impact the system's performance.

3.2.3.2 The use does not result in commercial gain or private profit. In no case may University's computing resources be used for solicitation of external activity for pay.

3.2.3.3 The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.

3.2.3.4 The use does not involve sending or soliciting chain letters, nor does it involve sending unsolicited bulk mail messages (e.g., "junk mail," or "spam")

3.3 Individuals/ Owners in breach of this policy are subject to disciplinary procedures.

If an individual/ computer performs an activity that violates any clause of the policy, the University reserves the right to impose a financial penalty or terminate the access to the network for such individuals/ computers. The amount of the financial penalty and the period of deactivation will depend upon the severity of the damage done by the activity.

Important Note:

Every user on the network should read the network policy and abide by the same as an individual and as an owner of computer(s) in their respective domain(s); it is mandatory to accept the terms and conditions in the policy in order to gain access to the network.

- **IT technicians, with the explicit agreement of the network management team, may be exempted from clauses (3.1.7, 3.1.8, 3.1.9).**

Any amendments to these clauses will be circulated among all the users as and when applicable.