St.Francis Institute of Management & Research (SFIMAR)

I.T ACCESS/USAGE POLICY- GENERAL

Whom this Document Concerns

All Users of IT infrastructure (Computers and the Network) at SFIMAR. (Inclusive of All the Employees, Students of MMS, PGDM & Part-time Programmes & any other person to whom SFIMAR IT services are extended on authorized request)

Reason for Policy

This policy outlines the responsible use of the Information Technology Infrastructure at SFIMAR (Inclusive of Hardware, Software & Network Resources)

Statement of Policy

All users of SFIMAR will be subject to the following **Acceptable Use Policy**

1. [CONTENT] User will be responsible for all use of this network. In case user owns a computer and is connected to SFIMAR network, he/she will be responsible for all the content on it especially that which he /she makes available to other users. (This provision will also apply to any computer or device owned by User, and is included in the meaning of "my computer".). In case the user does not own a computer but is provided with some IT resources by SFIMAR, He/She will be held responsible for the content stored in the designated workspace allotted to him/her.(examples: file storage area, web pages, stored/archived emails, on Computer Centre or any other department machines).

2. [NETWORK] User will be held responsible for all the network traffic generated by "my computer". He/ She shall understand that network capacity is a limited, shared resource & agree that physically tampering with network connections/ equipment's, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Offenses of this type could result in suspension/permanent disconnection of network services. User shall not share the network connection beyond his/her own use and will not act as a forwarder/ masquerader for anyone else.

3. [ACADEMIC USE] User shall understand that the IT infrastructure at SFIMAR is for academic use and he/she shall not use it for any commercial purpose or to host data services for other people or groups. Also, User shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per IT Act.

4. [IDENTITY] User shall not attempt to deceive others about my identity in electronic communications or network traffic. User will also not use SFIMAR IT resources to threaten, intimidate, or harass others.

5. [PRIVACY] User will not intrude on privacy of anyone. In particular User will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

6. [MONITORING] User needs to understand that the IT resources provided to him/her are subject to continuous monitoring, with cause, as determined through consultation with the SFIMAR Computer Centre administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. SFIMAR Computer Centre Personnel's are authorized to perform network vulnerability and port scans on user systems, as needed, for protecting the overall integrity and efficiency of SFIMAR network.

7. [VIRUSES] User shall maintain "my computer" on this network with current virus detection software and current updates of his/her operating system, and also shall attempt to keep "my computer" free from viruses, worms, trojans, and other similar programs.

8. [FILE SHARING] User will not use the IT infrastructure to engage in any form of illegal file sharing (examples: copyrighted material, obscene material).

In particular User needs to have noted the following:-

- Electronic resources such as e-journals, e-books, databases, etc. made available by the LIRC- SFIMAR are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited.

- Use of robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute. User shall be aware that Systematic downloading will result in the publisher blocking the entire community of users at SFIMAR from accessing these resources.

9. [SECURITY] User shall understand that he/she will not take any steps that endanger the security of the SFIMAR network. Specifically, He/ She will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the SFIMAR campus. SFIMAR authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of SFIMAR Resources.

10. [PENALTIES] User shall understand that any use of IT infrastructure at SFIMAR that constitutes a violation of SFIMAR IT Access Regulations could result in disciplinary / legal actions against user.

Information technology policies ensure that everyone's use of the Institute's computing and telecommunications resources supports its educational, research, and administrative mission in the best possible way.