

## **IT Security Policy**

### **Regulations for the use of computer facilities offered**

These regulations apply to the use of all local facilities and to facilities provided by the Company to its employees for use at home or off site. Please note that breaches of this policy will be considered Gross Misconduct and you may be dismissed.

Hardware owned, leased, rented or otherwise by **IFIN Global Group** employees or third parties approved by the Company may be directly connected to the network only by arrangement with, and with the explicit approval of Seshadri Vangala, Chairman & Group CEO.

Such equipment may access the network or other facilities only in accordance with the terms of these regulations.

The facilities may be used only in connection with employees' work for the Company. They must not be used for work of undeclared financial benefit to employees or the transmission of unsolicited commercial material without the express permission, in writing, of Seshadri Vangala, Chairman & Group CEO.

You must not interfere with the work of others or the system itself. The facilities must be used in a responsible manner – in particular, you must not:

- Access, store or distribute material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence;
- Access, store or distribute obscene or indecent material, pornography, etc.;
- Access, store or distribute defamatory material;
- access, store or distribute material such that the copyright of another person is infringed;
- Use computing equipment for playing games, gambling;
- use for any kind of personal gain (e.g. advertising goods or services);

- Gain deliberate unauthorised access to facilities or services accessible via local or national networks or access, store or distribute programmes designed to facilitate such access;
- Engage in activities which waste resources (including your own or other people's time, networks or computers) or which are liable to cause a disruption or denial of service to other users. This includes the following: introduction of viruses into computer systems; use of Internet Relay Chat facilities; use of peer-to-peer networking products; use of internet TV, radio or similar streamed media services
- Engaging in any lobbying or political activity
- Use the Company's IT systems to keep a personal "blog";
- Engage in activities which are illegal or which might contribute to the commission of an illegal act; or
- Engage in any transaction purporting to be representing the Company when not authorised;
- Enter into any contract or subscription on the internet on behalf the Company, without specific permission from Seshadri Vangala - Chairman & Group CEO.

### **Computer and Password Rules and Management**

You must not gain unauthorised access to or violate the privacy of other peoples' files, corrupt or destroy other peoples' data or disrupt the work of other people.

You are responsible for the security of your computer terminal (whether desktop or laptop) and must not allow the terminal to be used by anyone not employed by the Company.

You will be issued with a login ID and password. You must keep these secure and you must not disclose them to anyone else. You must not:

- permit anyone else to use your login ID or password;
- use any other person's login ID or password; or

Change your login ID or password unless otherwise instructed by the Company Secretary or your Manager.



If you leave your workstation for any period of time you should ensure that you lock it to ensure no-one else is able to gain unauthorised access.