NITIN FIRE PROTECTION INDUSTRIES LIMITED
(L29193MH1995PLC092323)

POLICY FOR INFORMATION TECHNOLOGY & COMMUNICATIONS

BACKGROUND

This document lays down the framework of Information Technology & Communications at Nitin Fire Protection Industries Limited (hereinafter referred to as the 'Company' or 'NFPIL') and defines the policy for the same. This document shall be under the authority of the Board of Directors of the Company. It seeks to identify and manage the communications through the platform of the information technology (including telephone, facsimile and computers etc.) inherent in any business operations of the Company.

REGULATORY

Information Technology & Communications Policy is framed to secure and manage the communications through the platform of the information technology as required under various acts, regulations as specified, if any.

POLICY STATEMENT – E-MAIL AND INTERNET USAGE:

E-mail and Internet activities will be confined to business related activities. The Internet and E-mail system hardware is Company property and therefore all messages sent or received on the E-mail system are and remain Company property. In-appropriation and illegal uses of the information technology infrastructure of the Company will be liable for penalty as per the decision of the management. All employees/representatives of the Company should understand that internal and external E-mail messages as records of that may be required for business or legal reasons.

No Employees will use another person's personal computer (PC) or access code / password to access the Internet or on-line services, without the prior permission or request of that person. No employees must retrieve or read any E-mail messages that are not sent to them without prior authorization of other employee.

Employee must be aware of security issues in their communications, and must ensure that they do not disclose any confidential or secret information or material to any unauthorised persons. Doing such activities will be treated as breach their Confidentiality Agreement and / or their Contract of Employment with the Company. No Employees will not transmit sensitive or confidential Company or client materials via the Internet or E-mail, unless authorized to do so.

APPLICATION OF IT INFRASTRUCTURE OR ASSETS OF THE COMPANY:

Employees who possess Company-supplied computing and communications facilities must not use the Company hardware of software for the following purposes:

- Generate, transmit or store potentially offensive material;
- Access or download material or send messages or material, which are not related to activities of the Company or against Company policy. This could include material, which is pornographic or sexually explicit, contains comments or innuendo (including jokes) of a discriminatory, sexual or racist nature, or makes inferences about a person's sexual preference. In addition other offensive material includes content or messages that are fraudulent, defamatory, embarrassing, obscene, harassing, abusive, intimidating, derogatory and/or other unlawful material;
- Originate or distribute chain letters, junk E-mail, broadcast mailings or other electronic material which is for political (e.g. elections for private or other organizations) or other non-work related purpose;

NITIN FIRE PROTECTION INDUSTRIES LTD
MUMBAI
COMPANY SECRETARY

MONITORING OF COMMUNICATION NETWORKS:

The Board or Management has the right to monitor and audit any use of its computing and communication networks and to access or retrieve any material or data that is accessed, stored or transmitted on or via these networks. All E-mail and Internet access is automatically recorded and may be monitored by the management. Reports from the log files detail which sites each user has visited and which files each user has downloaded to their PC or server will be placed before the management as and when required. The management reserves the right to block or limit access to any service or activity that affects or diminishes the effectiveness of its networks by whatever means necessary.

DISCIPLINARY ACTION FOR BREACHES OF POLICY:

If complaint is made about or material discovered reflecting inappropriate use of computer and communication facilities, it will be investigated. If complaint is substantiated, disciplinary action will be taken, which depending on the circumstances, may range from counseling and re-training, to formal warning and summary dismissal.

PROCEDURE:

The Employee looking after Information Technology department will intimate about the relevant information of this policy at the time of employment or at the time of amendment of Policy. On request they can take a copy of the same. Current staff that already has system access will also be intimated about the policy and any amendment thereof by the head of the Information Technology department.

The head of the Information Technology department in consultation with the management will make available or procure the requirements of the Information Technology infrastructure.

For breaches of the policy outlined above, the preferred option is to make a formal complaint. The employee can approach the Management about the in-appropriate use of Infrastructure of Information Technology. The individual will be asked to provide details of the complaint in writing, including the offensive or inappropriate material or message, the name of the person against whom the complaint is being made (the respondent) if this is known, the names of any witnesses or relevant parties, and any suggestions they might have about how the issue could be resolved. The management will make every attempt to manage the investigation in a confidential, impartial and efficient manner with the aim of finding a satisfactory resolution to the process.

REVIEW:

This policy shall be reviewed by the Risk Management Committee and the Board from time to time as may be necessary.