IP Protection & Security Policies

Ver 2.0

Revision History

Ver No	Ver date	Written/Revised By	Comment	Reviewed By	Approved By	Approved Date
2.0	March 10th 2006	Prasanna	Changed content to Virus Protection	Sumitra Seshan		
1.0	March 9th 2003	Gopal Gopalakrishnan	Basic Content	Sumitra Seshan		

TABLE OF CONTENTS

1.0 Purpose of the Document

The purpose of this document is to explain to the employees of Fifth Generation Technologies the different IP protection policies of 5G.

2.0 IP Protection Policies

Every employee of the company plays a crucial role in protecting the IP rights, knowledge & other IT assets of the company. The following sections help in explaining the procedure that needs to be adhered by the 5G users in order to secure the different assets of the company and protect them from un-authorized access.

2.1 Non-Disclosure Agreements

- All employees are required to sign a non-disclosure agreement that clearly states the employees' responsibilities regarding the company's confidential or trade secret information.

- At the time of signing the agreement, the employees are made to understand which of the materials are considered to be confidential to the company.

2.2 Security

2.2.1 Virus Protection

All computers that are part of the 5G network have Anti-virus software Mcafee Virus-Scan Enterprise 8i software installed in them. These computers are configured to obtain latest virus definition updates from the server. In server the software Mcafee Protection Pilot is installed which will download the latest virus definition updates directly from the Mcafee server and will update the client PCs each day. With this Mcafee Protection Pilot software the IT support engineer will come to know how many PCs are updated, number of PCs pending for updates, the status of the PCs, virus infections in any of the PCs, name and type of virus, the file(s) which is affected by virus, the type of action (Cleaned, Deleted, Quarantined, Error) taken against the virus etc.

- Downloading files from unknown or suspicious sources should be strictly avoided

- Employees are encouraged to avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

- Employees should delete Spam, chain, and other junk email without forwarding them

2.2.2 Password Management

- Users are allowed to set passwords for their Windows Accounts, Email accounts and Application software passwords.

- Users are asked to set passwords which are hard to guess and not to give away their passwords to other users, unauthorized personnel and will be treated as breach of confidentiality.

- Users are requested to change their password regularly

- Users must avoid using features that "remember" passwords - this makes it easy for an unauthorized person to gain access to system and server.

- Users are encouraged to log off from the network (or) lock their PCs whenever they are away from their desk - for ex: while away during lunch hour. This ensures unauthorized users not using PC's under authorized user accounts and this also ensures all the active applications keeps running.

  Method To lock a PC
  Press ctrl+alt+del and choose "Lock Computer" option.

2.2.3 Encryption / Password Protection

Users should not use any encryption or password protection techniques to protect their files and folders other than standard Windows Permissions.

2.2.4 File/Folder: Sharing and Permissions

Users should consult with the IT support Engineer in setting the correct access controls for their files and folders to prevent access by unauthorized users.

2.3 Physical Protection of Personal Computers

Users are not allowed to open the PC cabinet physically or disconnect any I/O devices attached with the computer for any reasons. In case of a strange noise or any malfunction of any devices attached with the computer it has to be reported to the IT support Engineer.

2.4 Usage of other Equipments

Employees, vendors or visitors are not allowed to use any of their own devices (Desktop, Laptops, USB drives, Floppy, CD/DVD ROM's etc) with out the consent of the IT Support Engineer.

2.5 Access to Server Room

Only members of the IT support team has access to the server room.

2.6 Data Protection

The data stored on hard disk can be lost or corrupted due to disk failures. This is unpredictable but usually happens due to a improper shut down, skipping of check disks and due to power problems.

3.0 Firewall

5G uses DI704UP Router and disallows the following.

- IP directed broadcasts
- Incoming packets at the router sources with invalid addresses such as RFC1918 address
- TCP small devices

- UDP small services
- All sources routing

4.0 Backup

System backups will be performed on a regular schedule as determined by the overall Backup Policy

At minimum, Network/System Administrators shall schedule backups as follows:

- Weekly Twice incremental backup - to be retained for a period of 4 weeks;
- Full Weekly Backup on 2nd, 3rd, 4th and last week - to be retained for a period of 6 weeks;
- Full monthly backup 1st week - to be retained for a period of 16 weeks;
- Quarterly backup during the months of January, April, July, October - to be retained for a period of 1 year;
- Generate and record details of files that have been backed up, and tapes\CDROM that are used;

5.0 Securing Product Releases

The final release of product to every customer is physically written in two CDs. One CD is kept in a secure place within the office premises and the other CD secured in a third party locker.

6.0 Classification of Documents and Accessibility to documents

- The documents are classified appropriately and the accessibility of the documents are restricted based on their classifications.

- Any document related to cost estimates, quotes to customers, invoices, billing documents, financial statements, consolidated sales reports are restricted and only the Management and the CFO are authorized to view these documents

- Marketing personnel have access to the price lists and information

related to their own customers and a consolidated lists are not made available to sales and marketing team

- The design and project related documents are accessible only to the team members who are part of the project team.

- Company related information such as Financial, Corporate Profiles etc. is not accessible to employees.

7.0 Destroying of Confidential Documents

- All sensitive or confidential documents should be shredded before throwing them out. The documents should not be put in the garbage without shredding due to security issues.

- The confidential documents include: financial statements, cost sheets, proposals, sales reports, bills, invoices, customer information, design documents and any other document that has been classified as "confidential".

8.0 Planning the path for Exit of an employee

- While leaving the organization, the supervisor of the employee would oversee that the employees hand over all documents related to their work and any other confidential information such as client list, price list etc.

- The password for accessing the company's network and their mail-ids will be inactivated at the time of the employee leaving the company.

- Employees must turn in their access cards for the business premises, laptops, library books, other customer related files and information, keys to his or her desk, file cabinet or any other keys that are in their possession. In case any of the above is not returned, then the locks will be changed