Information Security Policy Ver 3.1

Document Details

Document Path	http://192.168.1.102:9073/Mindshare/5gpal/policies/OPD_ Information Security Policy
Document Version	3.1
Document Date	Jan 27th, 2017
Document Status	Final
Circulation Type	Internal
Circulation List	All@ 5G

Revision History

Date	Version	Content Added/Revised	Prepared by/Revised by	Approved by
March 9th 2003	1.0	Basic Content	Gopal Gopalakrishnan	Sumitra Seshan
March 10th 2006	2.0	Changed content to Virus Protection	Prasanna	Sumitra Seshan
June 16th 2008	3.0	Content Update	Jai Srinivasan	Sumitra Seshan
April 5th 2012	3.0	Review done - no change	Jai Srinivasan	Sumitra Seshan
April 4th 2015	3.0	Review done - no change	Jai Srinivasan	Sumitra Seshan
Jan 27th 2017	3.1	Logo Changes	Jai Srinivasan	Sumitra Seshan

Table of Contents

1.0 Introduction

The Information Security Policy of 5G (herein '5G' refers to Fifth Generation Technologies India (P) Ltd., 5G Automatika Ltd., 5G Energy Ltd., 5G Technologies Ltd.) has been developed keeping in mind its specific operational needs that govern the organization.

2.0 Purpose of the Document

The purpose of this document is to describe the Information Security policies that govern the organization. All employees shall keep themselves abreast of these policies and shall adhere to them without fail in their regular day-to-day work.

3.0 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 details of the IP policies have been described in a separate policy document (OPD_ IP Protection Policy document) and the readers of this policy are requested to cross-reference the IP Policy as well. The following sections help in explaining the procedure that needs to be adhered by the employees in order to secure the different assets of the company and protect them from un-authorized access.

3.1 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.

3.2 Security

3.2.1 Physical Access

At the time of joining the organization, all employees are provided with a security badge, only using which the employees can gain access to the physical building. Employees are required to do finger print scans to gain access to various facilities within the office. Access to these facilities are maintained based on ACL (Access

Control List) and goes through CCB (Change Control Board) for changes. During employee separation process, the employee's security badges and biometric profiles are disabled from the system.

3.2.2 Virus Protection

All computers that are part of the 5G network shall have Anti-virus software installed in them with daily automatic full-scan enabled. These computers shall be configured to obtain latest virus definition updates from the server on a continuous basis. Apart from computers, the IT Administrator shall ensure all the computers are behind the corporate firewall and the firewall has anti-virus enabled by default so as to prevent any malware attack from external networks.

The IT Administrator shall do an audit trail on a daily basis of the following:

- Number of PCs that are updated with the latest definitions of Anti Virus software
- Number of PCs that are pending for such updates;
- Virus infections if any;
- Impact of virus infection (local or global).

If the impact is local, then the IT Administrator shall record the

- name & type of such virus;
- the file(s) affected by virus;
- type of action taken (Cleaned, Deleted, Quarantined, Error) against the virus.

If the virus infection is found to have a global impact and cannot be quarantined, then the IT Administrator shall shut down the server and escalate this as defined by the Organization’s Structure and reporting protocols as part of immediate escalation and emergency remedial action. Emergency remedial action shall include Business Continuity Plan (BCP) of the organization upon getting the approval of the Chief Executive Officer of the organization.

- Downloads of files or any other digital data from unknown or unauthorized sources shall be strictly avoided.

- Employees are encouraged to avoid direct disk sharing with read/write access unless there is an absolute business requirement to do so.
- Employees shall delete spam, chain, and other junk email without forwarding them.

3.2.2 Password Policy and Management

- Employees shall be allowed to set passwords for their Windows Accounts, Email accounts and Application software.
- The password policy is enforced based on Windows AD. Such a policy, automatically forces all users to change their password after a duration. Each password change needs to conform to the following rules
  - Passwords must not contain the user's entire account name.
  - Passwords to be of minimum length of 8 characters.
  - Passwords must contain characters from three of the following five categories:
    - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
    - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
    - Base 10 digits (0 through 9)
    - Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
    - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- Employees shall not keep a written copy of the passwords in places that are easily accessible to third parties and/or shall not verbally disclose their passwords to other users, unauthorized personnel as the passwords are strictly non-transferrable. Such an act shall be treated as breach of confidentiality.
- Automatic alerts are sent requesting the users to change their passwords from time to time.
- Employees shall avoid using features such as “remember” passwords.

- Employees shall 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.

  Method To lock a PC

  Press ctrl+alt+del and choose "Lock Computer" option.

3.2.3 Encryption / Password Protection

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

3.2.4 File/Folder: Sharing and Permissions

Employees shall consult with the IT Administrator in setting the correct access controls for their files and folders to prevent access by unauthorized users.

3.3 Physical Protection of Personal Computers

Employees shall not 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, employees shall report to the IT Administrator.

3.4 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) without the consent of the IT Administrator.

3.5 Access to Server Room

Only members of the IT support team shall have access to the server room. The server room shall be monitored using a 24/7 video surveillance system.

3.6 Data Protection

Any data related to clients/company's IP and personnel are within the scope of data that needs to be protected. All electronic data are kept in secure servers to which only restricted members shall have access. Proper and adequate audit trails shall be maintained for any such access made to the said data.

Papers, drawings, scribble notes, CDs, reports, presentations, analysis, etc. containing data relating to internal projects, client projects, company's products, third party's products, company's corporate information, clients' corporate information, business/marketing plans, commercial information, client agreements, partnership details and/or any other confidential information such as intellectual property, patents, trademarks, copyrights etc. shall not be kept open to disclosure on desks, or any other places in the work environment which are physically accessible to un-authorized personnel.

4.0 Firewall

All digital assets of 5G are accessible only within 5G network. 5G network is protected using a firewall. The firewall rules are defined based on Access Control Lists (ACL) and authorized devices. Such rules are also identified as a configurable item, hence goes through CCB for changes as defined in the OPD_Change Management and Control Policy document. Remote access to 5G digital assets are allowed only though secured VPN with specific policies defined for remote access based on user groups.

Suitable firewall is used to protect the corporate networks from the external world and to ensure prevention of intrusions, data sniffing and denial of service attacks. Actions of such a firewall tool include as a basic minimum but are not limited to the following:

- Disallow IP direct broadcast;
- Disallow incoming packets with invalid address;
- Disallow TCP small devices;
- Disallow UDP small services;
- Disallow all sources routing;

- Log all attempts to enter private network or an individual computer and set an alarm (in the form of a pop-up or other notice) when suspicious or hostile activity is attempted.
- Monitor and log all outbound data traffic and prevent unauthorized access to resources on external networks.

5.0 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.

6.0 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 is secured in a third-party locker.

7.0 Classification of Documents and Accessibility to documents

- The documents are classified appropriately and the accessibility of the documents is restricted based on their classifications.
- Any document related to cost estimates, quotes to customers, invoices, billing documents, financial statements, consolidated sales reports are restricted to authorized personnel only.
- Marketing personnel shall be privy only to their respective customer related

commercial documents.

- 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. are classified as restricted and shall not be accessible to all employees.
- All sensitive or confidential documents shall be shredded before throwing them out. The documents shall 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 IT/IS Training

- Every employee who joins 5G goes through an induction program, where they are trained in the IT Security Policies of 5G. The contractors or consultants who have access to the digital assets of the company are also trained and kept informed on these policies.
- All documents related to organizational policies are maintained in the intranet knowledge repository of the company for ready access at any time.
- Whenever there is change to any of the policies, as per the company's standard Change Management and Control Policy, the documents are updated and a company-wide communication is done to inform the changes to the Information Security Policy.
- Security Awareness and Training programs are conducted intermittently to update the employees.

9.0 Planning the path for Exit of an Employee

- While leaving the organization, the supervisor of the employee oversees the relieving process of the employee. The supervisor ensures that the employee hands over all documents related to his/her work and any other confidential information such as client list, price list etc.
- 5G's relieving process also includes the IT/System Administrator. At the time of

relieving, the IT/System Administrator ensures that the password for accessing the company's network and their mail-ids are inactivated and all digital assets are secured from the employee before getting relieved from the company.

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

10.0 Incident Reporting and Management

- All incidents (systems and security) once identified are immediately tracked as part of 5G Issue Tracker system with highest severity.
- Such items get automatically notified to impacted groups, the moment the item gets created.
- The IT team immediately assigns a resource to attend to the incident based on the type of incident. The resource immediately works on 'containment' action followed by 'remedial' action. At the end of each action, the issue is updated for the status.
- Upon recovery of systems after remedial, the issue is classified as a problem in order to identify the root cause and to formulate plan for prevention of such incidents in future.
- Each stage of the incident action is bound by SLA duration and any delay in SLA duration is to be automatically escalated.
- In case of emergency and complete shutdown, the business continuity plan and recovery process shall take over and appropriate persons shall be notified.

11.0 IS Audit

- Periodic audits of Information Security shall be planned by a designated Audit team at the beginning of every fiscal year.
- Audit team shall perform the audit based on the standard operating procedure (SOP) prescribed by the company.
- Audit reports are submitted within 24 hours of performing the audits.
- Upon review of the audit reports by the Company's Steering Committee, necessary actions shall be taken.

- The audit reports shall be filed safely and appropriately for future reference.

- End of Document -