DATA CONFIDENTIALITY POLICY

Version History

Ver. No.	Release Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
1.0	29th July 2015	Baseline & Release	Rahul Raj	Dhananjay	Ajay Kumar Zalpuri
1.1	5th July 2017	Update section 4.0	Rahul Raj	Dhananjay	Ajay Kumar Zalpuri
1.2	12th Sep 2019	Update section 4 & 7 for responsibilities and data classification	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri

1. NST Data Confidentiality Policy

NST hereinafter referred to as 'the Organization' is committed to providing a confidential service to its users. No information given to the Organization will be shared with any other organization or individual without the user's expressed permission.

For the purpose of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organizations (confidential information), which comes into the possession of the Organization through its work.

The Organization holds personal data about its employee, users, members etc. which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of the organization without prior permission.

All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

2. Purpose

The purpose of the Confidentiality Policy is to ensure that all employees, members, vendors and users understand the Organizations requirements in relation to the disclosure of personal data and confidential information.

3. Principles

- All personal paper-based and electronic data must be stored in accordance with the policy and must be secured against unauthorized access, accidental disclosure, loss or destruction.

- All personal paper-based and electronic data must only be accessible to those individuals authorized to have access.

4. Responsibilities

- For authorized personnel confidential data may be made available on a need to know basis as and when required. For all other person's access to such information must be prohibited.

- Unauthorized modification, transmitting or other dissemination of confidential information is strictly prohibited. Unauthorized dissemination of this information may result in disciplinary or legal action as appropriate.

- Confidential information should be safely stored and protected while on file servers, network drives, workstations, and during any type of transmission. Authorized access should be enforced.
- Confidential information should be erased securely from network drives, file shares etc. after proper authorization.
- Network or directory share information showing where the confidential information is stored must not be publicly viewable.
- Confidential data must not be emailed or faxed through personal email id or number; Upon prior authorization, confidential information sent via email must be sent from their official email id.
- Employees must not download and store confidential information unless encrypted on their personal computers, external hard drives, pen drives and CD/DVD, or any removable device.
- Printed reports that contain confidential data must not be left available to the public. All printed confidential data must be shredded or disposed of into locked bins.
- Employees must not take printed or unencrypted confidential data off-campus.
- Employees must not discuss confidential data in public or to another employee/ colleague
- All attachments or electronic files received from external sources must be scanned for viruses or malicious code to protect existing confidential information.
- The NST will periodically audit employees to ensure compliance and enforcement of policy.
- Any incidents of non-compliance may be reported to the Chief Information Officer (CIO).

5. Ensuring the Effectiveness of the Policy

Existing and the new employee will be introduced to the confidentiality policy via induction and training program. The policy will be reviewed annually, and amendments will be proposed and agreed by the SEPG Team.

6. Non-adherence

Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate. Each employee is liable for appropriate disciplinary action in

case of any information security breach related to confidentiality, integrity & availability of information security assets. Above Disciplinary action statement will also be signed by the employee at the time of Joining in "**Internet & Electronic Messaging Usage Policy" under section 9**

7. Data Classification

Confidential

Confidential data is subject to the most restricted distribution and must be protected always. Compromise of data classified as Confidential could seriously damage the reputation, mission, safety, or integrity of the company and its employees. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required management.

Examples: Personal Identifiable information such as Social Security Numbers, Driver's License Numbers; Employee Personnel data-Salary, Appraisal data, etc.

Restricted

It is sensitive but does not rise to the level of Confidential. Data classified in this category is for internal use only, the release of which must be approved prior to dispersed outside the company. Its compromise may inconvenience the NST but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity. Protection of this information is required and would be determined by the NST.

Examples: Daily NST finances Data; Research data; Test questions and answers. Minutes of meetings; etc.

Public

Data classified in this category is for general use and is approved by the company as available for routine public use. Security at this level is the minimum required by the company to protect the integrity and availability of this data.

Examples: Newsletter; Quality Management System, Annual Reports, NST website etc.