VOLUNTARY ACTION NETWORK INDIA (VANI)

Draft

Information Technology Policy

Introduction:

VANI`s IT Policy outlines the guidelines and procedures for the responsible, secure, and efficient use of IT resources at Voluntary Action Network India (VANI). It aims to protect organizational data, ensure compliance with legal standards, and enhance cybersecurity measures.

This policy applies to all employees, consultants, volunteers, and third-party vendors using VANI's IT resources, including computers, networks, mobile devices, email, internet, and software.

Equipment Purchase:

All approved equipment, services or software will be purchased through the Procurement Department of VANI.

Complete details related to purchase of technological equipment, services or software can be found in VANI`s Procurement Policy Manual.

Inventory Management

The Procurement Department is responsible for maintaining an accurate inventory of all technological assets, software and tangible equipment purchased by the organization.

The following information is to be maintained for above mentioned assets in an Inventory Sheet/register:

a. Item
b. Brand/ Company Name
c. Serial Number
d. Basic Configuration (e.g. HP Laptop, 120 GB HD, 2 GB RAM etc.)
e. Physical Location
f. Date of Purchase
g. Purchase Cost
h. Current Person In-Charge

Proper information about all technological assets provided to a specific department, project must be regularly maintained in their respective Inventory Sheets by an assigned team member.

Equipment Allocation, De-allocation & Relocation

1) **Allocation of Assets:**

a. New employees may be allocated a personal computer (desktop or laptop) for office work on the day of joining, as per work requirement.

b. If required, employees can request their supervisor for additional equipment or supplies like external keyboard, mouse etc.

c. Allocation of additional assets to an employee is at the sole discretion of the Reporting Manager(s).

d. No employee is allowed to carry official electronic devices out of office without permission from Reporting Manager.

2) **De-allocation of Assets:**

a. It is the HR Department`s responsibility to collect all allocated organizational equipment & other assets from an employee who is leaving the organization.

b. Updating the Inventory sheet is mandatory after receiving back all allocated equipment.

c. The received assets must be returned back to the Admin. Dept.

Equipment Usage, Maintenance and Security:

1) It is the responsibility of all employees to ensure careful, safe and judicious use of the equipment & other assets allocated to and/or being used by them.

2) Proper guidelines or safety information must be obtained from designated staff in the IT Dept. before operating any equipment for the first time.

3) Any observed malfunction, error, fault or problem while operating any equipment owned by the organization or assigned to you must be immediately informed to the HR.

4) Any repeated occurrences of improper or careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people using them will be subject to disciplinary action.

5) If your assigned computing device is malfunctioning or underperforming and needs to be replaced or repaired, then written approval from your supervisor is required for the same. The malfunctioning device needs to be submitted to the IT/Admn Dept. for checking,

Acceptable Use Policy for employees

- IT resources should be used strictly for work-related activities.
- Employees must not access, store, or share unauthorized or illegal content.
- Social media usage should be responsible and in alignment with VANI’s values.
- Personal use of IT assets should be minimized during work hours.

Data Security & Privacy for employees

- Employees must maintain the confidentiality of organizational data.
- Secure passwords must be used and updated regularly.
- Personal and confidential data should only be stored in approved locations.
- Any breach of data security must be reported immediately to the IT team.

Internet & Email Usage for employees

- Internet access should be used responsibly and not for unauthorized downloads.
- Employees should avoid clicking on suspicious links or emails.
- Official email should not be used for personal communication.

All PCs being used in the organization should be enabled to connect to the organization`s internet.

Official Data Backup Procedure

Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that employees keep important official data in some external storage device also. All official data including publications will have back up by storing in external storage device by the Admn department on monthly basis.

Data Classification

The organization classifies data into three categories:

a. High Risk:

i. It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure.
ii. E.g. Payroll, personnel, financial, biometric data.

b. Medium Risk:

i. It includes confidential data which would not impose losses on the organization if disclosed, but is also not publicly available.
ii. E.g. Agreement documents, unpublished reports, etc.

c. Low Risk:

i. It includes information that can be freely disseminated.
ii. E.g. brochures, published reports, other printed material etc.

Backup and protection system:

Different protection strategies must be developed by the IT/Admn department for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.

High risk data must be encrypted when transmitted over insecure channels.

All data must be backed up on a regular basis as per the rules defined by the IT Dept. at that time. Organization will be installing a file server for backing up data of all employees. All employees are expected to keep official data on the file system. CEO and the Admn department will have access to that data.

3) Server backup:

a. Admin. Department is expected to maintain an incremental backup of all servers with at least 3 copies of all servers. At any time, 3 backups of all servers must be maintained.

b. The hard disk of every server should be in the custody of Admin department.

Software & Licensing

- Only licensed and approved software must be installed.
- Employees must not download or install unauthorized software.
- Any software requirement must be approved by the IT department.

Cybersecurity Measures

Antivirus software must be installed and regularly updated by the admin.

Employees are expected to make sure their Antivirus is updated regularly. The IT Dept. should be informed if the Antivirus expires.

Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.

- Employees must be cautious of phishing emails and cyber threats.
- External storage devices should be scanned before use.

Remote Work & Bring Your Own Device (BYOD)

- Employees working remotely must use secure VPN access.
- Personal devices used for official work must comply with security standards.
- Any loss or theft of a device must be reported immediately.

IT Support & Maintenance

- All IT-related issues must be reported to the Admn department of VANI.
- Regular system updates and backups must be performed.
- Unauthorized access to IT infrastructure is strictly prohibited.

Internet Login Guidelines

1) All employees may be provided with a Username and Password to login to the Internet network in the office and to monitor their individual usage.

2) Username and password for a new employee must be requested by the HR Dept.
3) Sharing the Username and Password with another employee, visitor or guest user is prohibited.
5) A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.
6) The Admn. Dept. will define guidelines for issuing new passwords or allowing employees to modify their own passwords.
7) Any password security breach must be notified to the Admn Dept. immediately.
8) Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.

Inappropriate Use

The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Management Committee as deemed fit.
Any disciplinary action considered appropriate by the Management Committee (including legal action or termination) can be taken against an employee involved in the activities mentioned below:

1) Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth.

2) Downloading images, videos and documents unless required to official work.

3) Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work
4) Accessing pirated software, tools or data using the official network or systems.

5) Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee.

6) Engaging in any criminal or illegal activity or violating law.

7) Invading privacy of coworkers.

8) Using the Internet for personal financial gain or for conducting personal business.

9) Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.

10) Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation

Policy Compliance & Violations

- All employees must comply with IT security guidelines.
- Any violation of this policy may lead to disciplinary action.
- The Admn team will monitor compliance and conduct periodic audits.

Policy Review & Updates

This policy will be reviewed periodically and updated as needed to align with emerging technologies and cybersecurity threats. Any changes will be communicated to all employees.