21 INFORMATION TECHNOLOGY POLICY

Purpose

The purpose of this policy is to ensure:

- ✓ The provision of reliable and uninterrupted IT support & services
- ✓ The integrity and validity of data
- ✓ An ability to recover effectively and efficiently from disruption
- ✓ The protection of all the IT assets of Company including data, software and Hardware & removal media's.

Management shall ensure that the requisite levels of information asset protection are provided through compliance with this policy.

Scope

This policy applies to all employees, contractors, consultants, and temporary staff etc. using Company's computing resources. All are expected to be familiar with and comply with this policy.

Policy

The term IT assets relates to all IT hardware device which carries official data in any form viz. desktop, laptop, Tablets, ipad's, blackberry, smartphones, Network based Xerox Machines etc.)

21.1 Network Access

Information is a company asset and must be managed to ensure its confidentiality, integrity, and availability for authorized business activities. All information must be safeguarded against unauthorized modification, disclosure, or destruction, using controls that are commensurate with its value.

User Identification and Password:-

- Login passwords must not be written down or disclosed to another individual. The owner of a particular user name will be held responsible for all actions performed using this user name.

- Requests for new computer accounts and for termination of existing computer accounts must be formally authorized by HR and sent in writing in advance to IT by HR.

- Requests for additional access to specific business applications or folders/files/rights must be authorized in writing by the Reporting Authority/ Application owner and sent to IT in advance.

- HR department must notify IT and Admin in advance when moving any personnel to a new location so that It takes appropriate precautions in relation to the data security & IT asset.

- Passwords used should not be easily guessed so the password must have atleast 8 characters & must have alpha numeric character with one special character in place.

21.2 Access to Company’s Information

- All information held on the networks including e mail, file systems and databases are the property of Company and Company personnel should have no expectation of privacy for this data.

- Data and software stored on a Company’s PC are Company’s property any unauthorized deletion of files or software or unauthorized copies of any programs, files & data is prohibited, also the same must not move out from the Company’s premises - either physically or electronically.

- Requests to access the computer account of a colleague who is absent from the office must be directed to IT in writing with the approval of the “Relevant” Functional head/Manager.

- Office personnel must not issue any information to third parties unless they have authorization to do so.

- Users are only permitted to access electronic information and data that they require to perform their duties. If the users find that they have access to information that they are not concerned with, IT or their Functional head should be intimated of the same immediately.

- If confidential information is lost, either through loss of a notebook computer, backup media or other security breach, IT must be notified immediately.

21.3 Personal use of Computer systems

- IT assets provided to Company personnel is for business use, it is not acceptable to use them for personal use.

21.4 IT Assets Security

21.4.1 General

- IT assets must not be left unattended for long periods while signed- on e.g. during lunch, coffee breaks , etc. Users must either logoff, lock workstations & Switched off the monitor when not in use. And on closer of office hours IT assets must be switched off in all respect

- IT assets must not be removed from Company’s premises unless written approval has been received from IT. All equipment being sent for service/ repairs /relocation etc must be signed for in a Gate Pass available at front desk security.

- BYOD (Bring Your Own Device) shall be allowed to Company’s personnel subject to management approval

21.4.2 Software

- Any Software viz licensed, in-house etc must not be copied, removed or transferred to any third party or NON - Company equipment such as home PCs without written authorization from IT .

21.4.3 Confidentiality

- Confidential data held on computer media (e.g. CD-ROM, DVD, removal media) must be stored securely when not in use.

- All company related unwanted information must be disposed by shredding / destroying the media completely, so that the information is not recoverable by anyone

21.4.4 Notebooks, Tablets, Smartphones.

- The equipment must not be left unattended in any public place. Damage, loss or theft must be immediately reported to the IT. The user will be held responsible & necessary action will be taken.

- Data must be backed-up to the network on a regular basis and notebook users must ensure that the data on their notebook computers is adequately backed up.

21.4.5 Computer Viruses

- Corruption of PC's or notebook's data or software by malicious software (e.g. a computer virus or a worm) must be reported to IT immediately.

- Users are **not permitted to disable or remove antivirus** software under any circumstances.

- Virus, Trojen, hoaxes are common. If propagated by innocent recipients, hoaxes cost time and money. Please do not forward virus warnings and chain mails whatever the source to any employee, other than to IT.

21.5 Internet and Email

21.5.1 General

- All Company personnel have a responsibility to use the Internet in a professional, ethical and lawful manner. Users must regard Internet access as a privilege, which can be revoked if found being misused.

- Company will accept no liability for losses arising through the transmission of personal or financial information (e.g. Credit Card / Debit Card or any online media numbers) over the Internet.

- Users must not publish data on the Internet without the express prior written permission of Head Compliance Officer.

- Users shall not enter into legally binding contractual commitments using the Internet, either by Internet email or through the use of the World Wide Web, except where you have been authorized by the relevant Chief Executive Officer.

- The use of, or access to, web based e-mail systems, such as 'Hotmail, Gmail', for business purposes is forbidden including web sites which are no value addition to business purpose.

- All emails that are sent externally must carry a standard Company disclaimer. Users must not attach their own disclaimers to emails.

21.6 Telecommunications

21.6.1 Remote Access

- Remote Access can be defined as "Access to Company's IT resources or data from a location external to Company. This access may be by a third party or an employee who is located off-site.

- ▪ For cost and security reasons remote connections must be closed as soon as the purpose of remote access has been met with.

- ▪ Third Party Access can only be provided after the Third Party has signed a confidentiality agreement that must be included in their formal contract with Company. Company personnel must never permit another individual to utilize their user name to access the Company network.

21.7 Software Licenses

21.7.1 Copyright

- All software developed within and or for Company is the property of respective Company and must not be copied or distributed without prior written authorization from the IT & Management.
- The unauthorized installation of software on Company's IT assets is forbidden.

21.8 Data Backups

Users must inform the IT of their critical data so that the IT will take necessary action for the backups of the important data. This ensures that the data is available for recovery purposes. However IT should not be held responsible if the file/ folder apart from the user mentioned is not backed up.

21.9 Pornography

If users find any image(s) or media (picture, graphic, booklet, audio tape, video etc.) of pornographic nature on Company PCs, notebook computers or servers, they must report it to the IT & Company reserves right to take appropriate action.

21.10 Damage to IT Equipment

Intentional or threatened damage to data or IT infrastructure will not be tolerated. While in your possession you must take the necessary precautions to protect data and equipment provided to you.

21.11 Collection of Personal Information

If users have access to personal information, users must ensure that it was obtained fairly, is accurate, protected against unauthorized disclosure, used only for the purpose(s) for which it was collected and is held no longer than is necessary for that purpose(s).

21.12 Auditing and Monitoring

- IT Asset – IT personnel reserves the right to access any IT hardware if found suspicious in accordance with the IT policy.

- Email & Internet - Company reserves the right to review, audit, intercept, access, block access to sites deemed unacceptable and disclose all access to the Internet. This includes emails sent and received in addition to websites visited and files downloaded from the Internet.

21.13 Software - Regular reviews of IT hardware & license and or in house software are undertaken and the presence of unauthorized software will be investigated. Company reserves the right to remove any files, data and Software from systems including any information it views as offensive, illegal or personal.

21.13.1 Software Change Control

All alterations to system and application software must follow change control procedures to ensure the integrity of Company computer systems. For major changes this should include:

- ✓ Authorization of request for change
- ✓ Risk assessment of change
- ✓ User Acceptance Testing
- ✓ Relevant Functional Head/Manager sign-off
- ✓ IT sign-off Roll back procedures in the event that the change failed, on case basis
- ✓ Release notes for the changed software
- ✓ Adequate controls should be in place over any test data that is used in the testing process, as this data quite often is a mirror of live data.

21.13.2 Physical Security

The following standards must be applied to Server Room Access

- Access to the Server rooms (Data Center) must be restricted to authorized & nominated IT personnel's only & the same will be monitored regularly with the help of log book maintained in the Server room.

- Third parties who have been granted access to the Server Rooms must be accompanied at all times by IT personnel.

- Access to the Server rooms must be controlled by a physical access control mechanism such as an electronic/combination lock.

21.13.3 Fire Detection / Prevention

The Server Rooms must be fitted with smoke/fire detectors and fire extinguishing equipment, which should be set to automatic operation when the computer room is left unattended for long periods.

21.13.4 UPS / Backup Generator

The entire Server room and the equipments housed within it must have a UPS backup to protect against power surges/failures.

21.13.5 Control of Computer Media and Documentation

- Computer media e.g. tapes and documentation must be stored securely, e.g. in locked cabinets or vaults, when not in use.

- Magnetic media that is no longer required and which may contain confidential data must be disposed of securely, i.e. all data must be erased or the media must be rendered inoperable.

- Back-ups of sensitive, critical, and valuable information must be stored in an access-controlled site.

21.13.6 Business Continuity Planning

- Business Head /IT is responsible for business continuity planning for IT systems. The business continuity plan must be fully documented, maintained and tested on a regular basis.

- IT must take daily backups of all the main servers. These backups must be stored off-site for ease of access or should the computer room become inaccessible. The media should be tested for recovery purposes on a regular basis.

Distribution of the policy

The IT Security Policy is an internal document and is meant for internal usage within the company. Duplication and distribution of this policy without an authorized release is prohibited. The HEAD TECH TEAM will decide on the number of copies that will be in circulation and the persons with whom the document will be available.

Every person in custody of the document has the responsibility for ensuring its usage limited to “within the organization”. The custodian of the document will also ensure that the document is continually updated with amendments that may be issued from time to time. Any loss or mutilation of the document must be reported promptly to HEAD – TECH TEAM.