SYSTEMS POLICY

Preamble

The Computer World is changing by the nano-second and is compelling us to be on our toes and driving home the fact that we need to be flexible enough to meet the ever-changing needs of the customer. In an effort towards the same we have decided to formulate a policy for use of our IT resources and embrace the same for serving our customers better.

The overall aim of the Policy is to minimise damage to the organisation, its assets and reputation, by preventing and reducing the impact of security incidents.

The Policy focuses on electronic information processed by computer devices and on protecting the technology used to hold, process and transmit the organization's information. However, the principles apply to paper records and spoken conversation.

Objectives

The objectives of forming this policy are as under:

1. To comply with requirements relating to use of computers, hardware and software;
2. To promote efficient, effective and ethical use of information and IT;
3. To ensure integrity, availability, confidentiality and appropriate retention of information;
4. Ensure appropriate systems for handling, storage, retaining and destroying records created in the regular course of business;
5. Information owned or processed by the organisation is protected against threats, be they internal or external, deliberate or accidental (Cyber attacks).
6. Confidentiality of information is assured – we will protect our information from unauthorised access, use, disclosure or interception;
7. Integrity of information is maintained – we will protect information from unauthorised changes or misuse, so that it can be relied upon as accurate and complete;
8. Availability – information is available when and where it is needed;
9. Legal and regulatory requirements are understood and met;
10. Information and training on information security is up to date and available to all employees;

- **It is employee's responsibility to make themselves aware of the Policy and to adhere to it.**
- **<u>All Employees</u> must ensure they have read the Information Security Policy Statement.**

Though the onus of implementation of the policy rests with Systems Department, it shall be incumbent upon all user departments "HODs" and on each individual to follow the guidelines laid down for the purpose.

Employees are responsible for ensuring others working on their behalf (temporary staff, contractors, partners) are aware of and abide by the Policy when undertaking SPACO's business.

<u>Breaches of this Policy</u>

Policy breaches should be reported to systems department immediately after the incident. Breaches of the Policy are regarded as a disciplinary matter and those classed as gross misconduct may lead to a serious action.

Procurement of Resources

The procurement of various resources related to systems shall be done vide the "Purchase Requisition" procedure. The department raising the requisition shall forward the same giving justification for the requirement through the concerned Functional Head. Requirements for R&D shall be raised on a separate PO. New facilities shall have appropriate approval, authorizing their purpose and use.

Maintenance of Hardware and Software

The company has entered into Annual Maintenance Contracts with various parties for maintenance of various H/W and S/W. However, it shall be binding upon all user departments to follow the procedure laid down in case of break down of H/W or in case of problems with the S/W.

All users are required to comply with the following guidelines

- Whenever there is a need to shift any hardware, the user departments need to contact the Systems Department (and not shift the same themselves).
- Employees are not authorized to make any changes in the configuration of the IT resources without the explicit permission of the Systems Department.
- Users shall not make use of any external software / data on their PC.
- In case there is a problem with the hardware and the users require the services of the Hardware Engineer, they are required to communicate the same to systems Department.
- Users shall take appropriate precaution to ensure that their hard disk is not shared and when necessary a password is to be used so that confidentiality is ensured.
- Users are required to take care of their PC / Printer by keeping them clean.
- Whenever it is seen that the PC may not be used for long time users shall shut down the PC properly.
- Users shall save their work & shutdown the PC immediately in case of power failure.
- Users shall always logout from SAP Server when they are not using it.
- While printing, users are required to check the No. of copies setting (Lever) of the dot-matrix printer. Special care to be taken for multi-part printing.
- For important Excel / Word files users are advised to use Password.
- In case of any problem in power supply, get it repaired from Maintenance Department. In the event of ANY maintenance work on Electrical Supply, wiring, cables etc are undertaken for ANY reason, prior notice to SYSTEMS is required. Users should ensure that proper earthing and connections are provided that shall not in any way damage the Hardware / equipment.
- DH should have all the passwords of their subordinates (PC, mail, MS office files).
- No external device such as laptops, tabs, mobile, any USB device, hard drive etc. shall be allowed or connected to any PC, without prior approval of Systems Department/CIO.

Backups

1. **SAP Servers**: Systems ensure backup of data on SAP servers.
   All back-up media are stored in the safe area with back-up media taken
   Offsite every day.

2. However, for **individual PCs: R**espective department will be responsible for taking backup of important data on another PC. If required, backup can be taken on CDs/DVDs with the help of Systems Department.
3. **For R&D Servers & PCs**: R&D department will be responsible for their own backup. Hard Disks are provided to take back up at their locations.
4. For precaution Systems Department is taking quarterly backup.

Virus Protection

- Follow the instructions given by Systems Department regarding the Antivirus Software. Deliberate non-compliance with advice given will be a disciplinary matter.
- Do not open suspicious emails, email attachments or Internet links, particularly if they come from an unknown sender or are executable files (end with .exe, vb, scr)
- If a virus is suspected or detected, Systems will isolate the computer and any potentially infected media (disk, CD etc). We will investigate the incident and take the appropriate action.
- No media (CD, DVD, USB devices (memory sticks), mobiles etc) should be used on organisation’s Computer until it has been approved and checked for viruses.
- On the Internet do not open programmes which “pop-up” when you are on a site. If in doubt, seek guidance from the Systems Department.
- Users shall not use internal floppies/CDs/DVDs/USB devices on outside PCs.
- In the event of any virus detection, users should immediately inform the Systems department and avoid forwarding / sending any file / attachment.

Hardware Problems

All users shall communicate their major hardware problems to Systems through e-mail. In case user’s PC is broken down, the mail can be sent through e-mail from any other available PC.

Software Development / Modifications / Data Update

1. In case of Software Development / Modifications / Data Updation, users shall give their requirements in writing.
2. In case of reports, users shall specify columns, grouping, subtotals, sequence etc.
3. Systems Department will decide the priority & will give the feedback to the user.

AMCs of Software & Hardware

All AMCs will be finalized by Systems Department in consultation with concerned Department.

User Meetings: User Requirements & Review

Systems Department may have user meetings to review & understand the user requirements.

Network' requirements

In order to comply with code of connection to the 'SPACO's network', unauthenticated or other un-secure connections to systems on the LAN are not allowed.

Log on procedures

All users have their own user id and access to the computer systems cannot be obtained by any other means. For SAP, after 3 unsuccessful attempts to log in, the user id will be invalidated.
Users are responsible for logging out of computer systems and switching off PCs on leaving work each time. Where appropriate, each PC should have a password-protected screen-saver to prevent unauthorised access when PCs are left unattended, e.g. at lunchtime or when users are attending a meeting. The screen-saver should be set to come on after 5 minutes of inactivity.

Registering users

All employees are entitled to use the network and office software applications (Word, Excel, Power Point, Outlook etc). Access by any other person or any other software will require the written authorisation of the appropriate person.
Access to other systems is dependent upon staff role and functional area.

Access control

Access control to secure areas

The Server room is secure area and is kept locked at all times. Only an authorised member of staff is allowed access to the server room. **It is also equipped with smoke detector and security personnel are trained to act in case of disaster.**

Security of third party access

No external agency or person will be given access to any of the Spaco's networks unless that agency/person has been formally authorized to have such access.

Hardware

The Systems Department maintains an inventory of all hardware assets.

Software

The Systems Department maintains an inventory of all software assets. The media is kept in locked storage & the software can only be installed on organisation's hardware. Other Departments shall maintain inventory/media in the same manner. (UG, AutoCAD, CNC programs/settings etc)

Power supplies and telecommunications

All critical computer equipment is fitted with an uninterruptable power supply that has been tested and will provide stand-by power for at least 10 minutes of normal usage in the event of power failure. All existing data communications lines are installed via conduits or other adequately protected routes.

Reporting software malfunctions:

Procedures are established for reporting software malfunctions. The following actions are considered.

a) The symptoms of the problem and any messages appearing on the screen should be noted.

b) The computer should be isolated, if possible, and use of it should be stopped. If it is to be examined, it should be disconnected from any organizational networks before being re-powered.
c) The matter should be reported immediately to the Systems department.

Computer and network operations

All outbound and inbound traffic including e-mail and Internet browsing is controlled and logged at the Proxy Server.

User password management

Any password provided to a third party must be changed as soon as the task is complete.

Equipment security

The keys of systems department are kept in a safe location.

Care should be taken to ensure that computer screens and papers or printouts cannot be seen by visitors.

Remote diagnostics

Remote access to SAP for diagnostics & support will only take place via SAP router.

Security of equipment off premises

Other than Laptops, IT equipment must not be relocated or taken outside the premises without the permission of the Systems Department.
Users issued with Laptops will be given a written letter of the guidance on secure use of laptops. Users of laptops must take care not to leave portables unattended in a public place e.g. on a train or in a parked car.

Disposal of equipment

The system department will make a list of E-Waste after using the major parts of the Desktops, and the same will be shared to Accounts/Purchase/Admin Department for further action.

Building Repairs

Staff arranging for building repair or alteration work, including painting or changes to telephone lines, are responsible for ensuring that IT equipment including cable runs are not interfered with or damaged.

Cyber Attack:

A cyberattack is any type of offensive movement or action employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can also be labelled as either a cyber-campaign, cyberwarfare or cyberterrorism in different context. Cyberattacks can range from installing spyware on a personal computer to attempt to destroy the infrastructure of entire nations. Cyberattacks have become increasingly sophisticated and dangerous.

Firewall : A firewall is a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic.

A firewall acts as a barrier between a trusted network and an untrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied.

AntiVirus : Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems.

Firewall and antivirus are installed to prevent disasters.
Proxy server: A proxy is a computer system or program which acts as a kind of middle-man. In computer networks, a proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. It is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer sends your requests to the proxy server which then processes your request and returns what you were wanting. User internet access is controlled.

Protection from malicious software

The Systems Department will maintain a software inventory and will ensure that the legality of software licensing is met. User must not install personal software onto the SPACO's hardware (including portables). Users must not install or use games on the SPACO's hardware. The authorisation of the systems department must be obtained for the introduction of non-standard software. System Department needs to be satisfied by the source and legality of the software as well as its compatibility with other products before authorising its use.

Security incident management

All users are responsible for reporting any actual or suspected breach of security to their manager and to the Systems Department. An IT security incident is defined as any event that results, or could result in the loss or damage to hardware or software or the disclosure of confidential information to any unauthorised individual.

Business continuity planning / Disaster Recovery: Business continuity plans will be prepared for the core systems and will be subject to annual review.

Printing : Avoid printing unless it is very much required. As far as possible recirculate the paper. Try and use both sides of the paper. Do not use bigger size paper than required. As far as possible try to become paperless. Save paper save trees.

INTERNET & EXTERNAL E-MAIL

The purpose of this policy is to ensure proper use of Spaco's email system and make users aware of what Spaco deems to be acceptable and unacceptable use of its email system.
The e-mail system is to be used for official business and this applies to both sent and received e-mails.
An e-mail has the same status as written communication and is therefore actionable e.g. for defamatory remarks. Staff must take care to only include statements in an e-mail that they would be prepared to put in a letter head paper.
Security measures are in place to protect the 'SPACO network' messaging but the Internet, beyond the 'SPACO network', is insecure.

Email is a business communication tool and users are obliged to use this tool in a responsible and effective manner.

The following rules are required to be **strictly adhered** to. It is **prohibited to**:

- Send or forward emails containing offensive or disruptive content, which includes, but is not limited to defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
- Forward a message without acquiring permission from the sender first.
- Send unsolicited email messages.
- Forge or attempt to forge email messages.
- Send email messages using another person's email account.
- Copy a message or attachment belonging to another user without permission of the originator.

I. BEST PRACTICES

Spaco considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should ensure the same in drafting an email as they would for any other communication. Therefore it is mandatory for users to adhere to the following guidelines:

a. Writing emails:

- Write well-structured emails and use short, descriptive subjects.
- Sentences should be short and to the point. Users should start the e-mail with Dear Sir / Madam or Dear (name). Messages can end with 'Best Regards / Best Wishes'.
- Users must end the message with the sender's name, job title and company name. A corporate disclaimer will be added underneath the signature (see Disclaimer)
- Users must spell check all mails prior to transmission.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
- Fonts in Capitals / Lower case.
- Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him / her and knows what action, if any, is to be taken.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only mark emails as important if they really are important.

b. Replying to emails:

It is expected that emails be answered within at least 8 working hours, but users must endeavor to answer priority emails immediately. Priority emails are emails from existing / potential customers and business partners.

c. Maintenance:

Delete any email messages that you do not need a copy.

II. PERSONAL USE:

It is strictly forbidden to use Spaco's email system for purposes other than business purposes. Therefore, the sending of personal emails, chain letters, junk mail, jokes and executables is prohibited.

III. CONFIDENTIAL INFORMATION:

Never send any confidential information via email. If you are in doubt as to whether to send certain information via email, check this with your superior first.

IV. SYSTEM MONITORING:

If there is evidence that you are not adhering to the guidelines set out in this policy, Spaco reserves the right to take disciplinary action.

V. EMAIL ACCOUNTS:

Passwords should not be given to other people.

Internet services will only be used for those purposes directly related to a user's work or areas of legitimate research and operational services. Participation in online chat, gambling or game is forbidden.
No illicit material, pornographic, violent, racist, defamatory or offensive, religious or pertaining to gender discrimination will be viewed / downloaded or obtained via email.
Unlicensed or unauthorised software must not be downloaded or installed on any PC.

It should be understood that all Internet sessions are monitored and that activity logs are kept.
Modems, Mobiles must not be connected to PCs on the Spaco's network.
Users must not store personal data on the hard disc of a PC.

Information security:

Information is an important asset and of significant value, so we must protect information from threats; internal and external, deliberate or accidental, that could disrupt the work of organisation.

a) **Confidentiality:** ensuring that information is accessible only to those authorized to have access:
All the departments have their own logins & passwords. Wherever necessary form-level passwords are provided to avoid unauthorized access by users.

b) **Integrity:** safeguarding the accuracy and completeness of information and processing methods
All the information is entered by users thru applications with required validations & logic. In case of any problem, system persons are allowed to make the changes with proper documentation.

c) **Availability:** ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that **the specific security objectives of the organization** are met.

Users will be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.
e.g. log-on procedure, use of software packages, before access to information or services is granted.

VI. EMAIL ACCOUNTS DELETE:
In event of a person leaving the organization the mail file (PST)and important files/folders are backed and the mail-id is deleted.