SALASAR TECHNO ENGINEERING LIMITED

INFORMATION SECURITY

Policies & Procedures

Introduction

IT Policy of STEL can be defined as the rules & regulation that Guide Us how STEL manage and protect its information data and computing resources etc. The security policy basic purpose is to outlining what the company's critical assets are, and how they need to be protected. Its main purpose is to provide brief overview to the staff and appropriate use "of any of the Information Assets.

Information Security Awareness

- Information is a vital aspect of STEL. Everybody needs to take some appropriate steps to ensure that sensitive user information remain protected and confidential.
- The minimum steps that we must take to fulfill this requirement are listed below:

Unique User IDs

- All users must have their individual User ID's and password for login for ERP System

Lockup

- All files, Documents, CD's, backup disks or other Sensitive information IT people shall be put them in drawer & Elmira's or locker.

Disposal

- Properly dispose of Sensitive Information when required.

Licensed Software

- Authorized licensed & freeware software need to be installing on each and every computer.

Information Sharing

- Never share any Sensitive Information with other employees. Employees are intimated do not send any Sensitive Information over the Internet unless it is encrypted (Password protected file,).
- Do not leave Sensitive Information un-attended and in loose where any unauthorized person can access it.

Definitions Used in This Policy

- **Administrative Unit:** A department or division that provides and facilitates computing and networking services to the employees of the STEL
- **Central Database:** All Official personal, biographic, and demographic data are stored in STEL Data-Centre.

- **Information Technology {IT}:** The Department of Information Technology is the unit which provides specific software, training and information to Network/System users & coordinators;

- **IT Executives:** These steps may be taken only after authorization by the IT Head Unless the situation represents an emergency or immediate threat to network Security &
  integrity. In such case, the Network/System coordinator must document the circumstances of the Incident and notify the administrative unit, Management and IT. Actions should be taken in such way that any impact to non-offending users shall be minimized.
  The Network/Systems coordinator shall maintain and keep hard copy (readable) of any updation related to IT.

  The report must include the following information:

✓ Manufacturer, model and serial number.
✓ Operating System and revision number.
✓ IP address of all network system.
✓ Physical location of the equipment.
✓ User's name and User access ID

STEL Users Security

Password: Password is set by STEL TT Dept. and for the change of password, IT Dept. need to be contacted.

Virus Protection: System should be scanned manually & automatically, update of the software should be done, tips for protection against malicious (virus/Trojans/worms);

Software Installation: Freeware software's are forbidden if allowed conditions need to be considered for eliminating software piracy. Games and entertainment related activity completely prohibited as well the installation of any other program coming from unknown and untrustworthy sources;

External Equipment (CD's, Pen drive etc.): "Acceptable Use" measures (perhaps by way of a AUP- Acceptable Use Policy) need to be established because any external data source subjected to risk for company network or any other critical system need to be explained as well.

System Backup: Data backup of all STEL users linked with online Cloud Backup System. To avoid any loss of data in any circumstances.

Incident Handling: By now your staff should be able to define a potential security problem, while you should be established the rules of action to take in case of an incident.

Internet Threats Explained:

One of the greatest security risks in the company is the Internet connectivity and its misuse. It is fact that most employees will surf the sites those are strictly prohibited, and most probably will end up downloading untrusted files and /hostile code from hacker site.

Define what constitutes a "prohibited site", and explain why it is prohibited, including the problems that could occur just by visiting them.

Web Browsing: Web browsing represents a threat to the security of the workstation and causing password hacking. As well as the whole organization get exposed to the risk of web browsing. It's very easy that hostile scripts could be downloaded, and executed automatically; all it takes for example: an outdated version of web browser, patches etc...

E-mail Use: Generally the company E-mail systems are a high risk area due to their constant availability to the outside world. The use of e-mail to communicate business, contact clients, and its integration in many other business-related processes expose company mail address and (mail) system to potential attackers.

Information Security Web Site: It is recommended that an information Security web site is created and successfully implemented, which is an invaluable asset for STEL security.

Physical & Environmental Security

Cabling

- Documentation on, and marking of, cabling
- Provision of redundant lines

Server Room

- Intruder and fire detection devices
- Locked doors
- Avoidance of water pipes
- Emergency circuit-breakers
- Air conditioning
- Local uninterruptible power supply
- Remote indication of malfunctions
- Technical and STEL requirements for server room

Company Information Security Best Practices

General Guidelines

- STEL information must be stored in a secure area with process to restrict access & only server person get access.
- Facility should be protected by fire safety alarms & systems.
- Ensure that is available, it is adequate for a contingency plan, and it is protected from theft and damage.
- Antivirus software must be installed on all PCs and a process established for regular updates (at least weekly) and these should be checked periodically. e.g.: Trend Micro etc.
- Ensure all sensitive and confidential data are secured during transmission and storage (e.g. Entrust encryption, VPN connectivity etc.)
- If documents are stored overnight there should be adequately sized safes/cabinets should be there whom access is controlled by lock devices.
- All cybersecurity incidents shall be reported to designated officers within the time duration as specified in Section 2.

Section -2:

The SIRT Process (Reporting Security Incidents)

What is SIRT?

□□ SIRT stands for Security Incident Response Team. It is the process for Security Incident.

Detection and Response:

□□ All employees of company should be on the alert for potential breaches of Information Security. Attempts to compromise the security of our processes, systems, facilities or assets should be reported to Supervisor/Officer/H.O.D who will guide you on how to handle the matter.

Examples of SIRT:

Security incidents can take many forms, including:

- □ Theft/loss of laptop / PC
- □ Misuse of systems ID's
- □ Sensitive Information sent to incorrect email address
- □ Unauthorized modification of data
- □ Sharing of passwords
- □ Theft/ loss of STEL confidential data
- □ Misuse of privileged systems access by technology or support staff
- □ Misuse of e-mail and Internet
- □ Hacking of STEL system, network & websites.

NOTE: Virus/worm infections are not normally considered SIRTs. All infections should be reported to the IT Support.

Whom to Contact?

Reporting deadline: **2 hours** (30 minutes for Critical ones)

FUNCTION	NAME	PHONE NO.	EMAIL
IT MANAGER	SUMIT KUMAR	9027240464	Sumit.kumar@salasartechno.com
Sr. EXECUTIVE	YASPAL	9891510634	epr@salasartechno.com
EXECUTIVE	UMESHSINGH	821-8248002	Umesh.kumar@salasartechno.com

Ext. No-222

SANCTIONS AND DISCIPLINARY ACTION

Any violations of this policy may be resulted any of the following actions mention below, Consistent and approved by STEL, including the Faculty Manual where applicable:-

- Suspension or termination of access to computer and network resources.
- Suspension or termination of employment.
- Breach of contract for computer and network services.
- Criminal and Civil prosecution.