Revision Record

Description	Revision	Created Date
Original Release	O	24-08-2009
SFO rev. Changed to 1.0 as per migration of documents to share point portal	1.0	17-07-2010
Testing backup period included in Clause 9.3	2.0	10-06-2014
Modified clause 9	*3.0*	***12-08-2018***

Provide Put tick mark on appropriate column

WIP	Use up		Rework		Reject		NA	√
FG	Use up		Rework		Reject		NA	√
Raw Mtl	Use up		Rework		Reject		NA	√

Orginator: Josna M J	Dept: SFM
Reviewed By: Bino S John	Dept: SFM
Approved By: Sudheer Nair	Dept: SFM

*OIR : ORIGINATOR INITIATED REVISON
FMT NO: E0406 REV: 5.0
This is an Electronically generated document, is the latest revision, and does not require signature.
All HARD COPY are UNCONTROLLED unless otherwise bears a CONTROL COPY stamp
Effective from the time of release through Share point portal

1.0 Purpose: This procedure outlines control on usage of all Software's & Electronic Data to ensure unauthorized use, proper storage, protection & back up.

2.0 Scope

This procedure cover the following activities

- Software Usage
- Access to the system
- Network Security
- Backup Procedure

The procedures outlined in this document are applicable to:

i. EMS (Electronic Manufacturing Service), Cochin(All units within CSEZ)
ii. EMS Bangalore

3.0 Responsibility

As defined in the procedure

4.0 Abbreviations

The following Abbreviations are used in this document

Abbreviations

SFM-System Facility Management (A division of Corporate IT Management)

CIT -Corporate IT Management

EMS-Electronic Manufacturing Services

SFM - System Facility Management

FTP - File Transfer Protocol

DU - Delivery Unit

VSS - Visual Source Safe

ISMS - Information Security Management System

SFM - System Facility management

VPN - Virtual Private Network

GM - General Manager

MR - Management Representative

P&A - Personal & Administration

CBR - CD Burning Request

DU - Delivery unit

GFS - GRANDFATHER-FATHER-SON

HDD - Hard Disk Drive

HMR - Hardware Movement Request

HRD - Human Resources Department

PC - Personal Computer

PD - Project Director

PL - Project Leader

PM - Project Manager

PR - Purchase Request

RMG - Resource Management Group

SFM - Systems Facility Management

TCP/IP - Transfer Control Protocol/Internet Protocol

5.0 Definitions

Terms used in this document are defined in the following paragraphs,

1. **Mobile Code:** Software code obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies and macros embedded within Office documents. Mobile code can also be downloaded and executed in the client workstation via email.
2. **Malicious code:** Software code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computing system. Examples of malicious code include Trojan horses, viruses, worms, and trapdoors.
3. **Fallback Arrangements:** A mechanism for carrying forth programmed instructions despite malfunction or failure of the primary device.
4. **Project specific software:** Any software that is exclusively used in the organization for project specific purpose like development, testing etc.
5. **System Utility:** The utility programs that might be capable of overriding system and application controls.

6. **Internal Networks:** Users with all WAN connections provided and managed by SFM team are considered "internal networks" located within the secure network perimeter boundary

7. **Senior Management:** All employees in Grade 5 or above in the organisation who are occupying key responsible positions
8. **Classified Area:** A restricted area within the NeST premises. These areas shall not be accessible to all employees. Currently all the server rooms are identified as classified areas
9. **Systems Facility Management:** All activities pertaining to the installation and maintenance of the computer systems in the organisation, maintenance of software repository, creation and maintenance of user accounts, servers, printers, network equipments, and the management of disaster backups including all infrastructure routine operations. This can also include any other IT related services assigned by the management.
10. **Time Server:** A computer that periodically synchronizes the time on all computers within a network .This ensures that the time used by network services and local functions remains accurate.
11. **Software** – Includes purchased software (Operating system, custom made software, Standard software like ERP etc) , Internally developed software , Customer supplied software
12. **Data** : All electronic data created by above software , manually created data which need control

6. SOFTWARE USAGE

6.1 Overview

This chapter describes procedure for management of all software within the organization. It also describes the method for controlling the malicious and mobile code in order to protect the integrity of the software and information.

6.2 Policy

Usage of software within the organization shall be controlled in order to ensure the security and integrity of information in operational systems.

6.2.1 Policy on Customer Supplied Software Security

Units getting Software from customer must consult corporate IT division and

verify that the product is compatible and appropriate before the purchase.

Installation, usage and maintenance of customer supplied software should also comply with the corporate IT security policies. The divisional head should ensure that the software is used for the specific purpose by authorized users only. Unauthorized use or unauthorized copying of the software should strictly be prohibited. The software is to be shipped to corporate IT wherever possible. Corporate IT will retain all setup mediums, licenses and manuals, excluding end-user manuals.

6.2.2 Policy on Software License

Software Installations

- No software will be installed without a proper license.
- All software installations will be performed by qualified IT staff.

License Control

- All licenses must be stored centrally within corporate IT. Corporate IT will maintain a license inventory of all restricted licenses. This includes all purchased, granted, “free” for educational use, shareware, or any other restricted license. Sof

Setup Medium Control

- All mobile setup mediums (disks, CDs, floppies, tapes, etc) must be stored centrally within DSC.
- Licensed Software without a setup medium (direct download) will be stored and managed by corporate IT. Corporate IT is responsible for maintaining backups of licensed software.

Responsibility:
CIT (Corporate Information Technology Management) shall be responsible to monitor and control the use of software within the organization.

6.3 Procedures

Procedures for modification, management and control of software are given in following paragraphs.

6.3.1 Management of software

The following points shall be taken care for management of software.

i. Internal and external IP details shall be documented and kept under configuration control.

ii. Any changes or updates to the operational systems shall only take place after the necessary testing in an independent network in order to assess the potential impacts due to such changes and formal approval from SFM head or respective department head.

iii. In case of changes or updates of the same operation system in multiple units, the testing shall be performed only any one of the units, as far as the changes has the same impact in all the units.

iv. All changes including, changes to operational systems and application software shall be documented as per prescribed formats. For all changes an analysis report shall be maintained in the Technology Analysis Report. The report shall take in to account the potential impacts, fallback arrangements, and action for aborting changes as well as recovering from unsuccessful changes.

v. All software except commercial applications and project specific software shall be installed, updated or removed in computers through SFM persons only.

vi. Project specific software can be installed, updated or removed in computers by project team. But all software including syngo etc must be installed only with permission of reporting officer. Project specific software licenses shall be maintained by the respective departments. SFM shall be informed of the same.

vii. The installation software or source code of licensed software used throughout the organization shall be maintained only by SFM and shall not be made available to other SFO employees in the organization without prior approval.

6.3.2 Modification of Purchased Software

If software purchased by the organization need to be modified, the following procedures shall be complied with.

i. The modification shall be done only after analysis by persons assigned by the Senior Management (like CIT, respective Unit from which modification request is initiated etc.)

ii. Consent shall be obtained from the vendor if the software was brought from outside the organization.

iii. Risks associated with the change shall be looked into and proper

contingency and mitigation plans shall be identified.

iv. All modifications shall be tested by CIT or respective department in a system that is isolated from the organizational network before implementation.

6.3.3 Control against Malicious code and Mobile code

The following points shall be addressed to protect the integrity of the software and information.

i. Only Licensed software shall be used for information processing facilities.

ii. Virus protection system shall be installed in all machines. SFM shall ensure that this is up to date with correct versions.

iii. Firewall shall be configured to protect the internal network.

iv. Virus affected machine shall be disconnected from network.

v. Occurrences of malicious code and unauthorized mobile code infection shall be properly recorded.

vi. Information regarding new malicious code and mobile code shall be collected ; documented and appropriate corrective actions shall be implemented regularly.

6.3.4 Other Guidelines

i. Information about new malicious code shall be collected through subscribing to mailing lists and/or checking web sites giving information.

ii. If a security risk that violates the organizations security policies and procedures is detected in a software update, the new feature shall be disabled and shall not be installed on the machines used by the employees of the organization.

iii. Upgrade of software to a new release shall be performed only if there is an organizational need to do so. This shall be done only after considering and verifying the security of the release by SFM.

iv. Background filtering of websites using Spam filter shall be done depending upon the Internet privileges set for the user.

7. System Access

7.1 Overview

This chapter describes the system access Policies and procedure to be followed by

the employees of SFO.

7.2 Policy

Controlled system access shall be implemented both within the organization and off premises by a suitable system access control mechanism.

7.3 Responsibility

This procedure abides to all the employees of SFO. The responsibility of tracking all the activities stated in this procedure resides with the CIT.

7.4. Procedures

7.4.1 Login process

The following points describes the standards to be maintained for securing the login process in the organization.

- There shall be a warning displayed on the system screen before login, indicating that only authorized users shall access the computer.
- There shall be no Help messages provided during the log-on process.
- There shall not be any display of application or system details until the log-on process is successfully completed.
- The Log-on information shall be validated only on completion of all data input. If an error occurs in input data, the system shall not indicate which part of the data is correct or incorrect.
- The allowed number of erroneous log-on attempts shall be restricted.

  The

  system shall be locked when the limit is exceeded.
- The SFM shall maintain a record of successful and unsuccessful attempts.
- The system shall send an alarm message to the system console if the maximum number of log-on attempts is reached. Authorization shall be required for further attempts. A mail shall be send to SFM by corresponding department head for reauthorization.
- There shall be a time limit set for logon procedure and if this limit is exceeded, system shall terminate the logon.
- The system shall display the password using symbols, while entering, and shall not transmit it as clear text over the network.

- The remote desktop connectivity shall be, by default, disabled for server machines and for specific purpose it shall be provided for a defined time period with the approval of concerned Group Head or Reporting Officer.
- Management of passwords shall be as per the Procedure for Password Setting

7.4.2 Password Policy

PasswordComplexityrequirements

1. The password must be at least eight characters long.
2. The password must contain characters from at least three of the following four categories

   English uppercase characters (A - Z)

   English lowercase characters (a - z)

   Base 10 digits (0 - 9)

   Non-alphanumeric characters (for example: !, $, #, or %)

3. The password should NOT contain three or more characters from the user's account name sequentially.

B) Minimum password length: 8 Characters.

C) Maximum password age: 30 Days

D) Enforce password history: 3 passwords. (The system will not allow reusing the last 3 passwords)

7.4.3 User identification and authentication

- A User ID, which is unique, shall be provided to all users. All relevant privileges shall be set to this User ID and available to the User holding the User ID.
- The User ID shall be shared for a group only for meeting any specific objective.

  This process shall require the documented request and approval from the Group Head in charge of the data being accessed. The usage of such User Ids shall be permitted for a restricted period of time and shall be kept track off by

the SFM.

- The regular user activities shall be restricted from common User IDs.

In case a User ID has to be created for third parties,

a. The corresponding department head shall send a request to SFM with the name and time period for the User ID.

b. SFM shall create the user ID as per the request.

c. At the end of the usage of the User ID, the corresponding department head shall be responsible for intimating SFM regarding the same.

d. SFM shall delete the User ID as per the intimation by the department head or at the end of the time period specified in the request.

7.4.4 Use of system utilities

Installation of system utilities shall be maintained separately from the commonly shared software and an approved list shall be maintained. Further, classifications shall be done for software and utilities, which affect the information security.

All system utilities and special software shall be tested in proper test beds and ensure that it is free from vulnerabilities. All the identified vulnerabilities shall be documented prior to deploying it for usage.

The access to and use of special software and utilities, which may be a threat to information security, shall be controlled and permitted only through approved authorizations. The authorization shall be applicable only for limited users for limited period of time. Such software shall be maintained in isolation from commonly used software. The record of system software and utilities installed in all machines shall be maintained.

7.4.5 Session time-out

- The session time out period shall vary based on the sensitivity of the data being protected and the location of terminal.
- The session timeout shall be implemented by setting automatic locking of terminals, which will occur after a definite period of time.
- Special authorization shall be required for any servers, which requires unique timeout, and record shall be maintained for the s

7.4.6 Data Security Policy (Internal and External)

With the objective of meeting all current and future demands on data security, we have the following policies.

- No matter where information is saved, or who it is being exchanged with, we must secure data on mobile and fixed computing devices, on removable media, servers and in e-mails.

- Maintain guidelines for protecting data stored in computers or on off-line backup devices
- Train employees on threats and vulnerability of their computer systems
- Data cannot be created, edited or deleted without authorization
- Data access shall be controlled by multilevel security. For example to access a
  commercial application, there should be at least two level of security checks - one at operating system level and the other at application level
- Maintain data integrity all the time. (Data stored in one part of the database system is in agreement with other related data stored elsewhere)
- For any reason if data integrity is lost, a disaster recovery group should restore integrity of data using appropriate tools
- As business environment is constantly changing and new threats and vulnerabilities are emerging constantly, we should strike a balance between cost effectiveness of security control and the value of informational asset being protected.
- Regularly assess threats emerging from inside and outside of the organization
- Scan all incoming data(internal and external) and make sure they are virus-free.
- Calculate impact that each threat would have on each asset and address them accordingly.
- QA team to evaluate effectiveness of security control measures.
- Implement **principle of least privilege** (An individual, program or system process is not granted any more access privileges than are necessary to perform the task)
- Maintain following 3 levels of controls
  - Administrative control (Through approved written policies, procedures, standards and guidelines. For example corporate security policy, password policy, hiring policy etc) ○ Logical controls (Through software/hardware. For example
    passwords, network and host based firewalls, data encryption etc are logical controls) ○ Physical controls (Monitor and control environment of the workplace
    and computing facilities. For example, doors, locks, air-conditioning, smoke and fire alarms, fire suppression systems, cameras, security guards etc).
- Implement **separation of duties**. For example an application programmer should not also be server administrator or Database administrator.

- The access rights, to the data and application system functions, shall be set for all users.
- A record shall be maintained for keeping track of the access rights, which shall be updated from time to time.

7.4.7 Sensitive system isolation

The Server Systems shall be explicitly identified and classified for various levels of sensitivity and isolated from the shared environment.

The network shall be segregated from common network while sharing sensitive data in-group.

Documented authorization shall be required for running a sensitive system in a shared environment.

Physical boundary shall be identified and set for isolating sensitive systems from the normal development area.

Audit logs shall be enabled and analyzed periodically while sharing sensitive data from data base applications.

Shared access for a group, to the sensitive systems, shall not be provided

7.4.7 Other Guidelines

User ID shall not give any indication of the user's privilege level like manager, supervisor etc.

While providing access privilege for sensitive systems to group of users, members of the group shall be identified clearly.

For the systems, which require strong authentications, mechanisms like cryptography shall be provided.

Whenever a data is shared through the network, care shall be taken that both the Security and Sharing options are equally applied. Sharing should be removed for the default options "Everyone" and only required members shall be added.

“Remember password” option while log on to sensitive systems shall be permanently disabled. On expiry, all authorizations shall be revoked.

Time limit for a logon procedure shall be 3 minutes.

The number of logon attempts shall be limited to 5 times.

Organization shall have a default set of privileges while allotting User Ids.

Automatic locking of a system shall be configured after 15 minutes of inactivity.

A limited time-out facility shall be provided for systems whose availability is

continuous and critical. Such systems include mail servers, ftp servers, and Internet and VSS servers. In these systems, at time-out the screen shall be cleared and unauthorized access shall be prevented, without closing down the application or network sessions.

8. Network security

8.1 Purpose

This document describes and clarifies policies, principles, standards, guidelines and responsibilities related to the security of the organization's IT network resources.

8.2 Policy

Access to both internal and external networked services shall be controlled.

8.3 Responsibility

SFM shall be the responsible authority for monitoring and managing the network security.

8.4 Procedures

8.4.1 General Network Controls

Network access of the user shall require proper authentication.

Equipment identification shall be applied additionally to user authentication.

An identifier in or attached to, the equipment shall be used to indicate whether this equipment is permitted to connect to the network.

VPN shall be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications.

Network access rights of the user shall be maintained and updated as per the access control policy.

All line junction points (cable and line facilities) shall be located in secure areas or under lock and key.

Routers, switches, hubs, modems and front-end processors shall be protected from unauthorized physical access.

Network routing control shall be implemented using appropriate security gateways.

Ports, Services and similar facilities installed on a computer or network facilities, which are not specifically required for business functionality, shall be disabled or removed.

Use of network protocol analyzers and test equipments, which are capable of monitoring data passed over the network, shall be tightly controlled.

The SFM team shall maintain up-to-date diagrams showing all major network components, to maintain an inventory of all network connections and ensure that all unneeded connections are disabled.

Default passwords on network hardware, such as routers, shall be changed immediately after the hardware is installed. Security updates and patches for software shall be kept current.

Information processing facilities provided by the organization shall be up-to date with all latest patches and anti virus updates provided by SFM to avoid vulnerability.

Wireless technology shall be monitored by SFM team for new threats, vulnerabilities and for changes to standards that enhance security features and for the release of new products.

Authentication and encryption methods shall be enabled and used in wireless technologies.

Physical controls shall be implemented to protect wireless systems and information

8.4.2 Perimeter Security (for Internet and Intranet Connections)

Perimeter security protection for the network shall be enabled by controlling access to all entry and exit points.

Networks shall be segregated using firewall as internal network domains and external network domains. Firewalls shall be used between wired and wireless systems.

SFM shall manage the security for all points of entry to and from the network.

Additional WAN connections that are not provided by the SFM team shall be considered "internal networks" if they are authorized and approved by SFM.

The SFM team shall develop and use an on-going process to assess vulnerability of the network and risk in order to maintain adequate perimeter security controls.

The SFM team shall work together to address ways to meet user needs within a secured environment.

8.4.3 Remote Access

Authentication of remote users shall be achieved through secure channels.

Remote access to information processing facility shall be controlled through

proper authentication, to ensure the integrity, availability and confidentiality of the information stored within, processed by or transmitted by a system.

Categories shall be established to rank systems and applications according to the criticality and sensitivity of the information stored within.

Other than user access to general information, access by dial-up or Internet shall require user authentication and encryption services to protect the confidentiality of the session.

8.4.4 Other Guidelines

Monitoring and intrusion detection shall be employed to provide a feedback mechanism to indicate the effectiveness of tools used to support this network security policy.

Internet access rights to user shall be given as per the Procedure for User Registration and De registration (ISPR11) and Special Permissions allowed for the users.

9. Backup Policy

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the File server, the Mail server, ERP Server and Production Control Servers the Domain Controllers.

9.1 Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

9.2 Scope

This policy applies to all equipment and data owned and operated by **SFO Technologies Pvt LTD.**

9.3 Definitions

1. Backup - The saving of files to a mass storage media (both in same location and in different geographical location) and for the purpose of preventing loss of data in the event of equipment failure or destruction.

2. Restore - The process of bringing off line storage data back from the backup media.

9.4 Responsibility

The IT manager shall delegate a member of the System Facility Management department to perform and verify regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

9.5 Backup Storage Space Allocation

The space required to store the data shall be allocated and necessary data storage unit shall be procured as per the requirement to store the data for the defined period as per procedure # 62190002.052 – Procedure for Control of records.

Dedicated Storage of 20TB is used for the storage of the documents as per procedure 62190002.052- Procedure for Control of Records.

9.6 Testing

The ability to restore data from backups shall be tested at least once per month.

Server Backup details -

1. Domain Controller

   System State backup Scheduled to run daily at 11 PM to \\chnserver12\h$\SERVERS\CHNDC5\

2. File server

   Incremental Backup Scheduled to run daily at 10 PM to\\chnserver12\g$\sfotech\

3. Mail server

   Incremental Backup Scheduled to run daily at 11 PM to \\chnhyperv2\Exchange Backup\

4. ERP Servers

   Full back up scheduled to run daily 5.00 AM to\\chnserver12\backup\nav

5. Production Control server

   Full Back up Scheduled to run daily at 7.00 AM to \\chnserver12\servers\sfosrv02

6. SharePoint Server 2013

Full Back up Scheduled to run daily at 9.30 PM to
\\chnserver12\h$\SERVERS\MSSHP\

7. EDHR

   Full Back up Scheduled to run daily at 12 AM to
   \\chnserver12\Backup\NAV\OTHERBACKUP

10. Other Procedures

10.1 Overview

This chapter covers procedures followed by divisions of Corporate IT for responding the service requests received from various divisions on a day-to-day basis.

10.2 Hardware Movement

The user shall request the Hardware Movement from one location to another through the respective unit head. The respective users shall ensure that all the data is backed up properly. SFM shall assist them if required. SFM shall take the necessary steps to initiate the physical movement of the machine and update the movement in asset database. The following guidelines shall be observed in case of hardware movement.

- Movement of Hardware between buildings has to be minimized.
- Any machine movements from one location to another shall only be done through the proper procedure following the Hardware Movement Request and only when all the stakeholders approve this.
- SFM team members shall only act on receipt of a approved movement request..

10.3 Relieving

A copy of the relieving order shall be forwarded to SFM and the user accounts and other privileges shall be deleted. In certain cases where the personnel were playing a crucial role, the account shall be disabled and kept for a time period which shall be decided by the HRD and intimated to SFM.

10.4 Call Registration

A Call Registration facility shall be made available in the company's ASSET system for users to log their hardware/software related problem in order to get assistance from SFM.SFM group shall check their calls and attend the problems. If a call ispending and waiting for a response from the vendor, user shall be informed

accordingly and will look at alternate solution to the problem. After attending the call, the assigned SFM member has to modify the call status in the Call Registration facility. The reports concerning call registration data shall be reviewed monthly by the SFM team .The reports can be taken from SFM call registration system as and when required.

10.5 User Management

Each computer has an account in the corresponding domain. Similarly each user also has an account in the domain. Domains are configured as trusted domains so that a user logging on to a domain shall have access to the computers in the other domain also.

Administrative rights are given only when they are required and approved by the concerned authorities.

10.6 Network Performance monitoring

All servers, switches and routers shall be monitored on a continuous basis using available software tools. The server's system log and application log shall be verified

by SFM on a regular basis. The retention period of system and application logs shall be for three months.

10.7 Maintenance of purchased software

All software purchased will be kept with CIT. Policy on usage of licensed software is as follows:

- Copying of licensed software to CDs (Pirating) shall not be allowed.
- Taking Licensed Software CDs outside the premises for personal use shall not be allowed.

10.8 Maintenance of Hardware

Wherever possible, the hardware shall be maintained in house by the SFM. Wherever it is not practical to maintain the hardware in-house, Annual Maintenance Contract shall be awarded to external agencies. Necessary spares required for maintaining the hardware in-house shall be procured by SFM as and when required and kept in stores.

10.9 **Clock Synchronization**

For all the computers in a network, computer clock is synchronized automatically by a network time server. The clocks are all synchronized with an agreed accurate time

source. (GMT+5:30)

10.10 Technical Compliance Checking

For all servers, technical compliance (including vulnerability checks, penetration

testing) will be performed once in every quarter by Certified Ethical Hackers present in SFM

10.11 Other responsibilities of SFM

I. User ID and e-mail ID creation and deletion
II. Maintenance of Software repository
III. Routine System Administration
IV. Attending Calls – Help desk for internal customers
V. Monitoring the performance of network
VI. Hardware maintenance

Annexure 1

1) All Operating system/ Machine software maintained in the Master List
2) All Purchased softwares maintained in the master list
3) All Controlled documents maintained with Document control
4) All test programs maintained with Document control
5) All critical data
   - Accounting data
   - MRP data
   - Yield data
   -

   Testdata