IT Policies

Version: V4.0

SHEELA GROUP

50 YEARS OF EXCELLENCE

Contents

Document Name: Information Security & Business Continuity Standards

Document No: SFL/IT Policy/2

Documents Control:

Version No	V1.0
Date of Issue	01-April-2020
Verified by	VP – IT
Signed Off by	CIO
Last Review Date	31-May-2023
Next Review by	31-Mar-2024

Revision History

Revision Date	Version No	Remark
31-March-2021	V2.0	Policy reviewed and approved for changes
31-December-2021	V3.0	Policy reviewed and approved for changes
31-May-2023	V4.0	Policy reviewed and approved for changes

Document Status: Released & Implemented. This is a controlled document.

1. Sheela Foam Limited (SFL) IT Policy

Applicability: This process is applicable on the following location of Sheela Foam Limited, (hereinafter will be referred as **SFL**)

Location

1. Plot # 14, Sector 135, Noida, Uttar Pradesh 201301, India

2. IT Policy Overview & Control

SFL users will share common technology infrastructure and facilities to manage IT (Information Technology). Usage of these policies enables authorised persons to effectively carry out operations.

Scope: These policies and procedures shall be applicable to all the Employees (Full Time, Part Time, Contractual, Consultants, Auditors, etc.) and stakeholders (in some cases Customers & Vendors) of SFL.

3. Review and Evaluation

The IT Policy and all related controls and procedures as mentioned in this document, shall be reviewed at least once a year. However, an earlier review shall be done, in case there is major change in Business & Information Technology environment.

4. Password Management

Objective: Passwords are an important aspect of security. A Strong password ensures secure access for network, database and applications. The purpose of this section is to establish a standard for creation of strong passwords, the protection of those passwords and frequency of change.

1) All Server level passwords (OS & Database) shall follow the below guidelines:

- Passwords shall contain **minimum eight alphanumeric characters**.
- Password shall be a combination of **Upper and Lower-case characters**.
- Password shall have **at least one special character** (like #, @)
- Password shall be changed at least once in **90 days**. On expiry of 90 days the old password shall get disabled.
- Old password **cannot be repeated** for next three changes.

2) Application-level passwords shall follow the below guidelines:

- Password shall be saved in data base in **encrypted form**.
- All the applications, which have their **own password management process**, the same shall be followed.
- All in-house developed application shall have **password management** to meet user level password requirements.
- All administrator level passwords shall have the **same structure** as mentioned **for Server level password.**
- Any exception in the password policy for any application or any hardware resources shall be recorded and **approval from CIO** shall be kept on records.

Restrictions: Password-sharing shall be **strictly prohibited**. It shall be treated as breach of this document and disciplinary action shall be taken against the individual(s).

5. Cyber Security

Objective:

• To provide support and direction on different aspects of cyber security
• To act as a guiding factor in developing relevant guidelines, templates etc
• To create and maintain a security-conscious culture
• To ensure compliance of legal, regulatory, and contractual requirements.

Review of Cyber Security Policy (CSP):

The CSP should be reviewed at least annually or whenever significant changes occur in relevant ecosystem. Chief Information Officer (CIO) is the owner of the CSP document. The overall owner of

the cyber security initiative within the Sheela Group is CIO.

Cyber Security Governance*:*

Cyber Security Governance Structure consists of the CIO, Security Head, IT Head, System Admin.

CIO shall also be part of the overall Cyber Security Governance Structure.

These personnel are responsible for development, implementation, operation, maintenance, and continual improvement of Cyber Security.

Information Sharing & External Relations*:*

Contacts with law enforcement authorities, fire department, emergency services shall be maintained by Admin office through CIO office. CIO shall put in place information sharing arrangements with CERT-In.

Information Asset Owner shall ensure compliance to each of the Laws and Acts relevant to its operations. These shall include but not limited to the Information Technology (IT) Act, Intellectual Property Rights (IPR), etc.

6. Business Continuity

Objective: Enable Business operations to run smoothly i.e. as close to normal as possible in case of a disruptive incident or force majeure. The objective of this policy is to establish standard practices & guidelines for securing all company's electronic information.

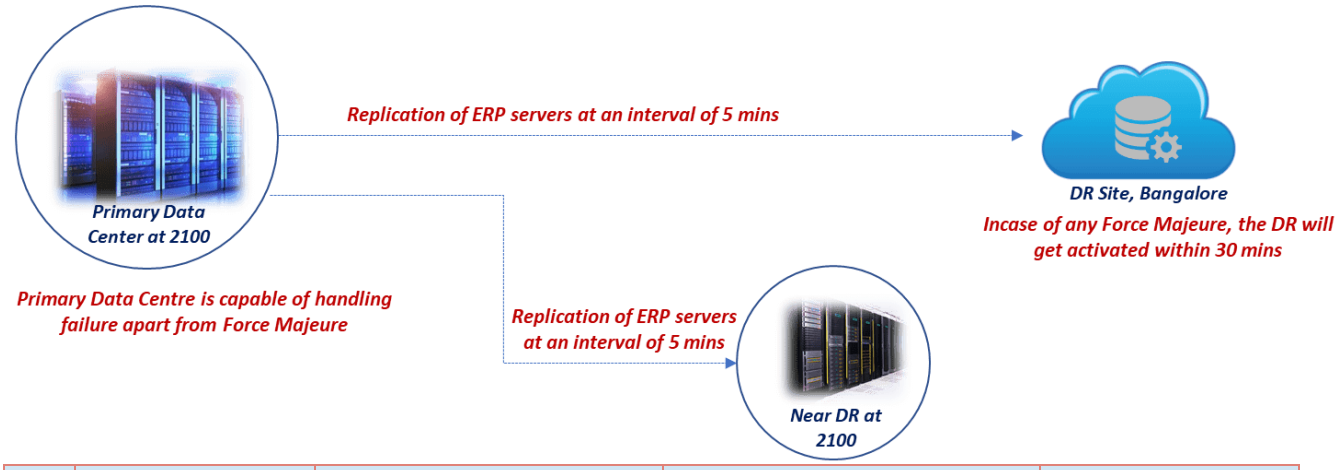
Scope*:* This is applicable to entire data / information generated / maintained by Business Systems.

1) Infrastructure under scope:

1. Centralized Data Centre at 2100 with VM environment and Clustering of Physical Servers.
2. Near DR at 2100 with VM environment.
3. Standby Server for Hardware Failure at Centralized Data Centre, 2100.
4. DR site at Bangalore on the model of 'Pay as Used', which is scalable.

2) Data Backup

S#	Details	Local	DR (Bangalore).	Responsibility



1	Database	Standby Database Real Time	Replication at 5 mins interval. Replication through Zerto	Technology Head
2	Application Server	Mirror Image	Replication through Zerto	Technology Head
3	File Server	Data Backup Daily & Weekly.	Not Needed	Technology Head
4	Email Server	On Gmail: On Cloud. Gmail has its own Policies.	Not Needed	Technology Head

Frequency of backup for all the data shall be defined by the data owner and the responsibility for backing up the data shall be fixed based on role and responsibility. Backup log shall be maintained for whatever backup has been taken. In case of use of a tool, the output record of the tool can be considered as record.

3) Ownership of Restoration & Restriction

Email request needs to be sent to restore any VM level backup by the Infra team.

Restoration should be checked by the owner of the database (ex SQL database by Database administrator) on the very next day of restoration request for the confirmation of the data integrity.

4) Business Continuity Model

1. Local level failures are handled by standby databases & Redundancy on Hardware.
2. Mirror Images of Application Servers.

3. Apart from this, database backups are also maintained on weekly basis & are kept for a month.
4. For security attaches, firewall is in place & the entire DC is under DMZ.

5) BIA (Business Impact Analysis)

The Business impact analysis is done to set the priority of information system, in order of their business-criticality depending on defined parameters. Once critical systems are identified, the continuity of the business is planned.

BCP leader and BCP team members- in consultation with respective function owners, technology head, and information security head- shall carry out Business Impact Analysis for infrastructure and business transactions.

Business impact analysis will result in categorization (like vital, essential and desirable) of infrastructure and business information followed by disaster scenarios (Catastrophic, major, minor, trivial) for various disaster causes (fire, flood, system failure, etc.)

Business Categorization (Vital / Essential / Desirable): Below mentioned parameters are used to Categorization.

S#	Criteria	Definitions			Weights
		Low *(Score of 1-4)*	**Medium** *(Score of 5-8)*	**High** *(Score of 9)*	1 - 5
1	**Legal Impact**	Minor legal implications	Major legal impactions	Critical Legal Impact, Penalty associated, etc.	4
2	**Organization Strategic Impact**	Low strategic project due to expectation of repeat business, aligned with strategic competencies.	Medium strategic project due to expectation of repeat business, aligned with strategic competencies.	Highly strategic project due to expectation of repeat business, aligned with strategic competencies.	4
3	**Customer Impact**	No impact on customer revenue loss.	Customer revenue impact (Minor)	Customer revenue impact (Major)	5
4	**Revenue Impact**	0-10% of revenue loss.	11-79% of revenue loss.	80-100% of revenue loss.	5
5	**Gross Margin Impact**	Planned vs. Actual GM variance between 5-10%	Planned vs. Actual GM variance between 10-15%	Planned vs. Actual GM variance more than 15%	3
6	**Business Dependency**	5 -15% Business users are impacted	15% to 50% Business Users are impacted	More than 50% Business Users are impacted	5
7	**Urgency / Timing**	Application can be down for more than 48 hours	Application can be down between 4 and 48 hours	Application cannot be down more than 4 hours	5

Categorization of Infrastructure & Business Information: If the score is 150 & above service will be on high priority and for others it will be on low priority.

S#	Infrastructure	Independent	Legal Impact	Org Strategic Impact	Customer Impact	Revenue Impact	GM Impact	Business Dependency	Urgency / Timing	Total Score
1	Storage	Independent	2	7	9	9	4	5	5	180
2	Database	Dependent	1	7	9	9	2	5	5	170
3	Sheela App	Dependent	1	4	5	4	2	7	5	114
4	Physical Server 1	Dependent	0	2	2	0	2	3	4	54
5	Physical Server 2	Dependent	0	2	2	0	2	3	4	54
6	Matrix Server	Independent	0	3	4	4	5	3	5	106
7	AC (CRV Unit)	Independent	0	9	7	6	4	9	9	189
8	Network (Router, Modem, Firewall, Switches, SSl, ISP, Routers)	Independent	0	9	9	7	6	9	9	212

6) Business Continuity Process

- For catastrophic and major disasters, the BCP Leader shall invoke the BCP process in consultation with the BCP Team Members.
- BCP Team members shall maintain the BCP document in an easily accessible, and secure, location.
- The BCP shall be reviewed at least once every year or whenever major additions, upgrades, deletions take place to the underlying hardware, network environment, office infrastructure or key personnel and updated, if required.
- Any changes to the BCP shall be notified to the entire BCP team with the updated BCP.
- The BCP testing process for vital services shall be done once every year.

7) Data Leakage / Theft

- To prevent data leakage / theft we have deployed tools to monitor data movement from Individual system.

8) BCP Testing

- The service resumption procedures shall be validated through a periodic testing (at least once in six months). The procedure shall be once tested, and threshold to be fixed so that future testing can be done against the set threshold. Based on these thresholds, the RTO and RPO can be decided.
- The test plan shall simulate the disassociation and respective BCP procedures shall be invoked.
- BCP Team leader shall be responsible for conducting the BCP testing.
- The result testing records shall be retained for at least one year & will be made available.
- Sample test scenarios are made part of template which is available separately along will all the information required for business continuity plan.
- The BCP Team leader shall ensure that all members of the BCP team have been trained on the BCP.
- Training records shall be maintained and kept.

9) BCP Change management

- Any change in BCP shall be approved by the BCP leader.
- Any changes to the BCP shall be notified to the entire BCP team with the updated BCP.

10) Roles and Responsibility for Business Continuity

Role of BCP Leader

- Coordinate the development and maintenance of the BCP policy manual and get approval from BCP Team.
- To identify and declare disaster-scenario according to the gravity of the disaster.

- Enforce BCP among teams as per disaster scenarios.
- Reviewing and auditing of BCP once a year
- Testing and updating of total BCP at least once a year.
- To facilitate functional training of the members for BCP execution.
- To co-ordinate with outsourcing partner wherever applicable.
- To ensure that adequate spare resources are available for recovering from disaster in the infrastructure level.

Role of Team Member

- To execute BCP activities.
- To co-ordinate with outsourcing partner wherever applicable.

7. IT Procurement

Objective: The primary objective of this section is to document controls related to the IT procurement including IT Infrastructure, IT software and services in SFL.

1) Process for Procurement

- User shall request by filling up the request form **(Annexure 1: Requisition form IT Equipment's),** duly approved by the concerned HOD.
- Technology Infrastructure Team shall provide the necessary specifications, suggest model and approximate cost along with quotation (in specific case); else shall go with the standard finalized specification and shall take approval from VP -IT /CIO / Directors. If good working equipment is available with IT and is less than 4 years old, then instead of procuring new equipment the same can be issued to the user.
- For procurement, the approval form shall be sent to purchase department for further processing. The purchase shall be executed directly through the manufacturer / OEM or the authorized sales & service partner. The purchase department shall scan and upload the Capital Sanction Form while generating the Purchase Order.
- Technology Infrastructure Team shall maintain inventory of Standard Laptops so that the laptops can be provided to users on need. Standard Laptops shall be purchased through OEMs directly.

2) Software, IT services and Hardware Purchasing Guidelines

- The Infrastructure Team shall be the sole authority for defining the scope of the work for placing orders for IT software, services and hardware on behalf of SFL.
- All requests for purchasing of equipment or software, whether as individual items or as part of a larger project, shall be sent to the IT procurement Team who shall process the request as per the policy guidelines.
- The Infrastructure Team shall review the procurement requirement and accordingly decide to approve /modify / reject the procurement requirement.
- The Infrastructure Team shall understand the technical requirements and draft the scope of work for the procurement.
- The scope of work shall have full approval and authorization prior to requisitioning from VP – IT / CIO.
- The further procurement process shall be aligned with the wider range of procurement and financial policies, standing orders and standards of SFL.

8. Asset Management

Objective: The primary objective of this section is to create awareness related to management of Information Assets.

1) Acceptable use of Assets

- Acceptable use of assets shall be ensured by owner of the asset.
- Everyone shall use these facilities responsibly. Any misuse of these facilities has the potential to negatively impact productivity, disrupt company business and interfere with the work or rights of others.
- Every user shall ensure that these policies are uniformly followed.
- Any usage of asset, for any use other than permitted use, shall be considered as an act of not adhering to this document. Owner of the asset shall be held responsible for any such act.

This section does not stand in isolation and must be implemented in conjunction with the wider range of procurement and financial policies, standing orders and standards of the Trust.

Inventory of Assets: An inventory of all assets shall be maintained by the Infrastructure team in the form of **Asset Register**. SFL maintains appropriate protection of the organizational assets. It aims at confidentiality, integrity and availability. The information such as Asset details, category, owner, procurement date, configuration /specification of the asset, warranty expiry date etc shall be maintained in the asset register.

2) Process for Replacement

- For replacement / up -gradation of all IT equipment's Procurement Procedure shall be followed.

3) Process for Management of removable media

Where appropriate, paper and computer media shall be stored in locked cabinets when not in use, especially after working hours.

4) Process for Disposal

- If the Server / Desktop / Laptop required to be disposed-off, the hard disk /or any form of storage media shall be removed and destroyed, so that no data is sent out of the company. Record of disposal of equipment shall be maintained with evidence of data / hard disk removal and of destroying by the person, other than owner/ person in-charge of disposal.
- The equipment to be disposed shall be handed over to the stores department and from there these shall be disposed-off by Admin Department with the help of IT, wherever required.

5) Process for Physical Media Transfer

- No removable media such as USB, DISK, removable Hard Disk etc., shall be purchased except when it is specifically approved. In exceptional circumstances, approval of Competent authority (Information Security head / HOD / VP -IT / CIO / Directors) designated to permit the usage of USB / External Hard Disk, etc.) shall be taken; and the list of such user with all desired information such as name, purpose, date, period, type of device etc, shall be kept for future reference.

6) IT's Responsibilities

- IT will be responsible for providing IT equipments in good working conditions to the concerned user / department. Before handing over the desktop / laptop to the individual user IT will ensure that all the required softwares, antivirus, etc are properly installed.
- Corporate IT department shall maintain list of all IT Equipments, software and licenses for SFL.

9. Remote Access

Objective: The SFL's use of Information Communications Technology enables its workforce to access its ICT systems, services, information and data while away from normal working environments and in remote locations. The purpose of this section is to ensure that the security of information and systems, accessed through tale-working and mobile working, is given due importance.

Remote working – an explanation

- Tele-working is defined as working from a fixed remote location. Mobile (remote) working is defined as working in a place that is not an individual's normal work base.
- Processing devices that can be used as part of tele-working or mobile working include PCs, laptops, notebooks, tablet, smart phones, personal digital assistants (PDAs), digital cameras, mobile phones and any other mobile device that record and/or process information.
- SFL uses Citrix & Accops (Application Virtualization Middleware) to access applications remotely. These are scalable platforms.
- SFL strictly prescribes Virtual Private Network (VPN) for Software Development Team. Currently, we have the capabilities to support 600 concurrent users on VPN.

10. Virtual Private Network (VPN) Policy

Objective: Virtual Private Network (VPN) service at SFL is managed and provided to employees & stakeholders who require remote and secure, access to database, application server, file servers and various web-based services when at home or travelling. In an effort to ensure the security and integrity of the service, certain requirements and guidelines must be met by the administrators and users of this service. It is strongly recommended to use the VPN connection when connecting to Central Data Centre over any unsecured (open or public) wireless network.

VPN creates a virtual "tunnel" connecting two endpoints by encrypting end-to-end communication and protecting the data from unauthorized access or interception. Telecommuters and mobile users, who require seamless access to corporate network for regular work, can use IPSec VPN or Client based SSL VPN from any Internet Service Provider; and access internal applications, do remote administration, monitoring and management of resources which are, otherwise, not accessible from Internet. Apart from these Clientless SSL VPN can provide secure access to sensitive applications as email, intranet Web application from Internet.

Acceptable use policy

- VPN connection is provided for accessing the servers, applications, database hosted Central Data Centre at SFL for remote administration services, development, maintenance and application access.
- VPN access requirement for user shall be verified by the HOD / reporting officer and approved by Information Security Officer / VP – IT / CIO.
- Using a VPN to access internal resources comes with responsibilities to uphold network security, as well as to safely, and equitably, use company resources.
- Hardware, software, network services, and support provided by the organization for VPN or remote usage are for the exclusive purpose of performing or fulfilling job responsibilities.

- The VPN is an IP-only resource. Other protocols are not supported.
- Dual (split) tunnelling is not permitted, only one network connection is allowed.
- VPN access is controlled using ID and password authentication.
- VPN users should disconnect the VPN after a predetermined amount of inactivity. The user can immediately log on again to reconnect VPN if the job requires so.
- It is the responsibility of those with VPN privileges to ensure that unauthorized users are not allowed to access SFL's internal networks.
- VPN gateways / concentrators will be set up and managed by the Infrastructure Team.
- When actively connected to the SFL's network, the VPN will force all traffic to and from the workstation over the VPN tunnel: all other traffic will be dropped.
- Once VPN is connected, all traffic between the user's PC and VPN server will be through VPN tunnel and user will have access to the servers listed in the application form.
- Any change in the Web applications/ server IPs which are to be accessed through VPN, has to be intimated to the Information Security Officer.
- VPN Log of min 2 months needs to be maintained.
- VPN account can be issued for max one year. The access rights should be reviewed and a fresh approval should be taken to renew the VPN account. The access rights should be reviewed in Feb – March every year.

11. Network Security Management

Objective: The primary objective of this section is to ensure networks shall be managed and controlled to protect information in systems and applications.

Scope: This policy is applicable to specify what security features are required for delivery of a network service, to ensure the security of information in networks, for the protection of connected services from unauthorized access, to improve overall network security posture, to ensure protection of critical network segments from unauthorized access, to assist in detecting and responding to an intrusion easily.

1) Network controls

Network controls shall be assigned to ensure safeguarding of information in networks and protection of supporting infrastructure. It shall also be applied to protect the network services from unauthorized access.

Network Controls Details: Network control shall be managed and controlled in the following procedure.

- The network shall provide high degree of performance and control to meet the business needs through access controls and privilege restrictions.

- Connections shall be made only from authorized equipment's and shall ensure security of access when access is made through diagnostic ports.
- Computer connections and information flows shall not breach the access control policy of the organization.
- Security of information on shared networks shall be ensured.
- Authorised user only shall have access to VPN.
  Internet bandwidth shall be regularly monitored for abnormal use.
- Network devices like router/switches/hubs shall be physically controlled and access to them shall be restricted.
- Factory-set passwords in network devices shall be immediately changed.
- Administrative access to these devices shall be restricted to network administrator or designated persons.
- Password Policy and Segregation in networks shall apply to the SFL Team.
- Appropriate firewall configuration and policies shall be implemented for the devices.
- Stand-by supporting devices in the data centre shall be incorporated for any future disruptions due to same devices.
- All the data cables shall be routed through the protected areas within the organization premises.
- Network bandwidth utilization and performance shall be monitored at defined frequency.

2) Segregation in networks:

Segregation of networks shall be identified and implemented to Groups of information services, users and information systems shall be segregated on networks. Use of VLANs and Managed switches shall be part of network diagram to depict the same.

12. Third-Party Access and Outsourcing

Objective: The purpose of this section is to maintain the security of the organization Information-processing facilities and Information assets during any access by the third parties and when the information-processing has been outsourced to another organization.

Scope: The scope of this policy includes all third parties, end-users and personnel who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system / service has access to the SFL network, or stores any information on the SFL's data servers. These include personnel with their designated desktop/laptop systems. All connections and network resources access between third parties that require access to SFL resources fall under this policy.

Controls

- Third-party resource shall take responsibility and comply with SFL's Information security and Business continuity policy and any other policy, as applicable.
- Third-party agreements and contracts shall specify
    - The SFL information resource to which the vendor shall have access
    - How SFL information shall be protected by the vendor
    - The duration for which the access is granted to the third party / vendor
    - Acceptable methods for the return, destruction or disposal of SFL information in the vendor's possession at the end of the contract.
- The Vendor shall only use SFL's information and Information Resources for the purpose of the business agreement and this information or data shall not be copied, divulged or distributed to any other party or self-gain.
- The third party shall ensure protection against spread of Computer Viruses.
- The third party shall ensure required physical protection measures to protect access to systems only to authorized person or device.
- SFL shall reserve the right to monitor activities and revoke access to SFL assets issued to third parties.
- The third party shall ensure that any username(s) and password(s) that they are granted remain confidential and are not used by unauthorized individuals.
- The third party shall use up-to-date Virus scanning software on all relevant computers that are being used to access SFL's data.
- Access to SFL devices (network and servers) shall be restricted to specific servers on specific ports as required.
- Any other SFL's information acquired by the vendor in the course of the contract shall not be used for the vendor's own purposes or divulged to others.
- SFL's shall provide an IT 'point of contact' for the Vendor. The 'point of contact' will work with the Vendor to make certain the Vendor follows these policies.

13. Logging and monitoring

Objective: The primary objective of this section is to establish a mechanism to log and monitor all the events including security, user activities, that occur in day-to-day operations of the IT environment.

Controls

- All the logs of system shall be checked for any possibilities of failures and even a faulty module in O.S that can hamper process.
- Proper monitoring of critical technology infrastructure shall be in place. This includes the alert generation to designated executive of technology infrastructure team. A critical infrastructure is defined as one the failure of which, affects a group of users or the entire

organisation. Use of a tool may be put in practice, for checking live status of the IT infrastructure to monitor the entire list of Servers/workstations, wherein any server/workstation fails, or any critical error has occurred it automatically alerts the Technology infrastructure team about the same.

- Windows Event logs for all critical servers shall be reviewed. It is a practice, wherein minute details can be of importance.
- All Physical servers, wherever possible, shall be set up with event-triggered mail alerts for any hardware prone to failure.
- Report shall be generated on number of issues that are identified so that the required action can be taken in time.
- A practice shall be made to keep a track of users that logged into services and the user pattern shall be analysed. This shall be done with a view to strengthen security and provide safer, and trouble-free, services.
- Audit logs shall be enabled for unsuccessful login attempts.
- Logging facilities and log information shall be protected against tampering and unauthorised access.
- System administrator and operator activities shall be logged.
- All the logs will be reviewed periodically.

Clock Synchronization

Clock synchronisation shall be ensured by syncing the time of each equipment of technology infrastructure- here time is being maintained, with a central server or a national infrastructure. For the correct setting of computer in the SFL network, clock is important and shall be carried out to ensure the accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases. One Server is identified as Time Master Server & other Servers of the network are synchronized with the Master.

14. Anti-virus

Objective: The objective of this section is to minimize the impact of various types of malicious codes such as virus, worms, Trojan horse, spyware, adware, harmful mobile code etc. SFL technology infrastructure.

Controls

IT infra team shall ensure that precautions are implemented to detect, and prevent, the introduction of malicious code into Technology Infrastructure of SFL.

- IT Infra Team shall ensure implementation of necessary technical, and operational, procedures for centralized antivirus definition updates.

- The Anti-virus product shall be operated in real time on all servers and workstations and it shall be ensured that no server/workstation is connected to the internal network without authorized anti- virus software.
- Anti-virus software shall be implemented at various levels (e.g. Desktop, laptops, emails gateways, Proxy Servers, instant messaging, systems etc.) in the network and system infrastructure as part layered approach to minimize malicious code entry into the Technology Infrastructure of SFL.
- Anti-virus software shall be configured to install automatic updates of signature files promptly without requiring user-participation for updates.
- Anti-Virus software shall be configured in a way so as to prevent users from disabling it or modifying configuration settings.
- Necessary controls shall be deployed to control virus spreading through email attachments.
- Anti-Virus software shall be configured to scan for virus prior to use of any internal / external diskette and any storage media for virus before use.
- Periodic scanning for virus-detection in all systems in SFL network shall be scheduled during non-peak traffic hours. (E.g. lunch hours or after-office hours).
- All activities relating to virus-protection shall be logged, maintained and reviewed periodically.
- Any activities intended to create and / or distribute malicious programs onto the SFL network (e.g. viruses, worms, Trojan horses, email-bombs, etc.) shall be prohibited
- All email, including attachments, shall be scanned at the email gateway or server before it reaches a user's mailbox.
- When a virus or malware is found in an email, the infected / attachment shall be quarantined and message shall get forwarded to the recipient.
- The email server or proxy server shall block all emails with attachment types listed here but not limited to (exe, asp, bat, html, scr, vbs, cmd etc).
- Antivirus management Server from which the workstations are updated shall be updated from Antivirus update website on a daily basis.
- Antivirus management Server to workstation/server notification shall happen on a daily basis.
- Antivirus for roaming users shall be updated from internet directly.

15. Patch Management

Objective: To keep the Technology Infrastructure safe and to ensure that operating system and software shall be updated with patches in a timely manner.

Controls: Technology Security / Infrastructure team shall ensure:

- Manual scans and reviews shall be conducted on systems for which automated tools are not available.

- An informal risk assessment shall be performed on the receipt of notification of patches. If a determination regarding the applicability of the patch or mitigating controls cannot be made in that time a formal risk assessment shall be done.
- Vendor-supplied patch documentation shall be reviewed in order to assure compatibility with all system components prior to being applied.
- Where possible, patches shall be successfully tested on non-production systems installed with most critical applications/services prior to being loaded on production systems.
- Successful backups of mission critical systems shall be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching shall be identified.
- Patches shall be applied during an authorized maintenance window in cases where the patch application may cause a service interruption for mission-critical systems.

16. Vulnerability Assessment & Penetration Testing (VA/PT)

Objective: This document outlines controls on carrying out Vulnerability Assessment and Penetration Testing of critical SFL's IT Applications and IT Infrastructure.

Control: IT Infra team shall ensure that

- Technical compliance, covering penetration testing and vulnerability assessments, shall be carried out internally or by independent experts specifically contracted for this purpose.
- Vulnerability assessments shall be carried out at least once in a year on critical applications / devices and the results are documented and shared with the management, post which action shall be taken to close the vulnerabilities found.
- A closure plan for all identified insecurities shall be prepared with responsibilities and timelines assigned to each action item. The closure plan shall be tracked and reviewed regularly to monitor the progress.

17. Physical and Environment Security Policy

Objective: The Physical and Environmental Security policy provides direction for the development and implementation of appropriate security controls that are required to maintain the protection of information systems and processing facilities from physical and environmental threats.

The key objectives are to:

- Prevent unauthorized physical access, damage and interference to the organization's premises and information;

- Ensure that critical and sensitive information systems are in secure areas, protected by the defined security perimeters, with appropriate security barriers and entry controls.
- Protect the information assets by implementing environmental controls to prevent damage from environmental threats; and
- Regularly conduct the preventive maintenance of the utility equipment to ensure their faultless services.

Scope: This policy is applicable to all the critical IT Infrastructure, Physical Information, IT Applications and Information residing in IT Infrastructure.

Ownership:

Basic Infrastructure Facilities, Admin, Physical & Environmental Controls are being maintained by Admin and Fire & Safety Department of Sheela Foam Ltd (Parent Organization). The same shall apply to SFL until, and unless, otherwise stated.

1) Physical Security measures for Visitors

- All visitors shall be registered and credentials should be verified before issuance of guest ID-Card. The ID-card must be collected back at the time of return of the visitor.
- The movement of visitor shall be restricted and shall not be allowed to the identified sensitive areas.
- The visitor records shall be reviewed and random checks shall be carried out by the Admin. In case of biometric access, the logs of biometric access shall be reviewed randomly.
- Visitors to secure areas shall be accompanied / supervised or specifically cleared to work independently.
- All personnel carrying laptops shall declare and enter the details of the same in records.
- Surveillance mechanism such as CCTV may be installed at all locations to monitor and record activities

2) Access Control Mechanism

- Appropriate entry points, exit points, emergency exit plans shall be visible including emergency symbols.
- Access to Central Data Centre shall be based on permission.
- The security / Admin / HR Department shall undertake surprise (at least once in three months) verification of access validation of access control mechanism.
- Access rights to secure areas shall be reviewed at least once in 6 months.
- Access logs for secure areas shall be maintained.

- List of contacts (i.e. fire, ambulance, police, critical vendors etc.) when emergency arises, including third parties, should be maintained. These numbers shall be displayed at various places.
- Technical mechanisms may be provided at the entry gate to validate all current employees.
- Any equipment entering or leaving premises shall be controlled through authorization and gate pass mechanism.
- Office premises shall be guarded on a 24 x 7 basis.

3) Ensuring Basic Infrastructure Facilities

Video Surveillance

- Surveillance mechanism such as CCTV may be installed at all locations to monitor and record activities especially ingress and egress,
- All CCTV Camera shall be recorded and stored for at least 7 days.
- CCTV camera monitoring station may be established, and random watch should be kept on live stream of CCTV camera.
- Compliance with security Surveillance policies as issued, time to time, by the admin / physical security department shall override the policies made above.

Fire Safety

- All computer systems shall be housed in an environment equipped with fire & smoke detection and prevention measures.
- The server rooms and data centre shall have fire-suppression system for handling electrical fire.
- Portable fire extinguishers of appropriate class shall be placed in locations from where they can be easily accessible. These locations should be well marked, preferably with fluorescent paint.
- The Fire safety equipment must be checked regularly in accordance with the manufacturer's instruction. The maintenance sheet shall be attached with the equipment.
- Employees shall be regularly trained in the use, and operation, of fire safety equipment.
- Comprehensive fire and emergency instructions shall be displayed in prominent location and a floor plan showing fire-fighting equipment and fire routines shall be place.
- Exit routes shall be marked.
- Floor plan and emergency exit plan shall be displayed in common areas. More plans may be placed where considered appropriate.
- Mock drills shall be conducted on predefined interval (at least half yearly) to ensure effectiveness of equipment and the instructions to be followed in the event of fire.
- Evacuation drill (in case of fire, earthquake or poisonous gas leaks) shall be conducted at least once in six months.
- This policy shall stand modified for any building compliance requirement as ordered by the appropriate government authorities.

4) Physical Security Controls

SFL has defined the physical security perimeter for all office locations, facilities and the geographies where information assets of SFL are located. It is recommended that physical access restrictions, commensurate with the criticality value of information assets, are implemented at perimeter of all such facilities where these are hosted.

Following controls are in place to ensure above stated objectives are met:

- Access to offices, facilities and secure areas (such as Data Centres, Network Operation Centres, Switch Locations) is provided to authorized personnel only. Access to critical areas shall be controlled and monitored.
- All premises and facilities, where information assets of SFL are hosted, have been classified into separate zones.
- Access shall be provided for Personnel on 'need to have' basis only.
- Physical movements in such areas shall be monitored and recorded as far as possible; and
- All equipment (such as servers, routers, switches, backup media) receive an appropriate level of protection against physical and environmental threats;
- Equipment installed outside the organization premises shall be monitored at regular intervals specially ingress and egress to the controlled zones.

5) Protection from External and Environmental Hazards

- Computer equipment shall not be in areas susceptible to water seepage and dripping.
- If computer equipment is installed in ground floor or in basement areas, then safety from flood and rainwater shall be implemented and documented.
- Hazardous and combustible material shall be stored at a safe distance from the site.
- Combustible items such as stationery shall not be stored in the computer room.
- The computer environment including power, air temperature and humidity control shall be maintained to meet the machines operating tolerance restriction as recommended by the respective manufacturer.
- Premises shall be secured from natural, environmental threats such as fire, flood, and earthquakes as in accordance with compliance requirement as ordered by the appropriate government authorities.
- Appropriate mechanism hall be instituted to protect against man-made threats such as rioting and commotion.
- Routine pest-control shall be implemented to ensure protection from rats and bugs.

6) Environmental Security controls

Protection against damage from environmental threats shall be designed and implemented. Designed system comprises of the following attributes:

- Air-conditioning and humidity control systems shall support information systems and equipment;
- Implementation of flood-protection measures;
- Implementation of appropriate fire-protection measures, including installation of fire-suppression systems in areas such as Data Centres;
- Implementation of adequate power supply controls to ensure continuous power supply; and
- Creation and implementation of emergency evacuation plans including the formation of an Emergency Response Team (ERT) to ensure emergency evacuation.

7) Controlling access to delivery and loading areas

Information Owners and Information Custodians, planners and architects shall ensure that access to delivery and loading areas or access from Reception Zones is controlled when considering building design and specifications. The following factors must be considered:

- Delivery and loading areas shall be designed so that supplies can be unloaded without delivery employees gaining access to restricted access zones;
- Protection of the delivery and loading areas shall begin at the perimeter with continuous monitoring in place (e.g., gated fence, CCTV, separation from public access);
- Access to delivery and shipping areas shall be restricted to authorized employees only;
- Setting and maintaining hours of operation for delivery and pick-up to ensure minimum or no impact on work;
- A combination of internal and external locking doors or gates shall be used to provide security;
- Incoming and outgoing shipments shall be segregated when possible;
- Incoming material shall be inspected for potential threats before being moved to or from the delivery and loading area.
- Hazardous materials shall be appropriately packaged and identified as to safety precautions;
- Bills of lading shall be compared to goods delivered;
- Loading docks and delivery areas shall be regularly inspected and actively monitored;
- Records shall be kept for internal and external deliveries and shipments;
- Reception areas shall confirm the identification of all visitors for restricted zone access; and,
- All visitors shall be accompanied while in restricted operational and security zones.
- For facilities that include delivery and loading areas, and / or reception zones, a Security Threat and Risk Assessment and inspection shall be conducted to determine that access can be adequately controlled.

8) Supporting utilities

Information Owners and Information Custodians, planners, architects and engineers shall collaborate in the planning and design of an information processing facility to ensure that supporting utilities (e.g., water, power, sewage, heating, and ventilation) are adequate to support employees and systems that will be in the facility. This includes estimating current, and future, utility capacity

requirements for the facility. In addition to meeting the building code and other regulations, the following shall be included in facility planning and specifications:

- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements;
- Emergency power off switches located near emergency exits in equipment rooms;
- Emergency lighting;
- Alarms to indicate inadequate water pressure for fire suppression;
- Alarms to indicate malfunctions in heating, ventilation, air conditioning, humidity control and sewage systems;
- Multiple connections to the power utility for critical systems and equipment;
- Multiple telecommunications connections to prevent loss-of-voice services; and,
- Adequate voice communications to meet regulatory requirements for emergencies.

9) Cabling Security

- Cables shall be laid and maintained in an organized manner.
- Ducts and entry points into building shall be secure.
- Cables running between buildings shall be through secured channels.
- Core cables may be identified and given special attention; tagging is a must.
- Power and Communication cables shall be kept in separate channels to ensure protection from electromagnetic interference. (at least 9 inches)
- Power, Communication and any other cables shall be well-tagged to identify the connected / free ends.
- Access to patch panels and cable rooms shall be controlled.

10) Authorized Removal of assets

Information Owners and Information Custodians shall establish a formal authorization process for the removal of assets for re-location, loan, maintenance, disposal or any other purpose. Authorization
forms for asset removal shall include:

- Description and serial numbers;
- Information about where the asset will be located; the removal date and return date;
- The identity of the individual responsible for the asset; and,
- Reason for removal of the asset.
- The description and serial numbers must be verified when the asset is returned.
- Removal of asset shall be authorised by owner of the asset. The authorisation shall include the responsibility and, protection of the asset (e.g., Terms and Conditions of Use) including the methodology for removal. In case the asset is moved within the organisation then there is a need of joint responsibility of both the parties, the receiver of the asset and sender of the asset. In case asset is being moved out of organisation then approval of movement outside the organisation shall be in place.

- Whether the asset has any storage media, if yes how the data is protected after removal of asset.

11) Protection of unattended equipment

Information Owners shall ensure that employees are aware of their responsibilities to secure unattended equipment to prevent unauthorized access to information systems by:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling password-protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password-protection on mobile devices including portable storage devices; and,
- Being aware of their responsibility to report security weaknesses where the above controls have not been applied.

18. System Acquisition & Development Policy

Objective: To ensure that security is built into information systems, including IT infrastructure and IT applications, acquired or developed internally by SFL.

Scope: This policy is applicable to all the IT systems, including IT infrastructure and IT applications owned, controlled and used by SFL's and users, including employees and third- party users.

Policy Statement: Security requirements shall be identified and agreed prior to the development and / or implementation of information systems.

1) Initiation Phase

- A risk analysis shall be performed to determine the threats associated and the corresponding security controls required for the system or system application under development.

2) Acquisition/ Development Phase

- The following points shall be considered at a minimum while preparing the security requirements for the system application:
    - Impact on existing systems.
    - Security vulnerabilities involved when connecting with other systems and applications.
    - Operating environment security.

- While purchasing a system or software, the security requirements shall be identified, and the selection criteria shall be based on secure functionality.
- For Business-critical application, there shall be a separation between the operational, test / development facilities.
- All development and new systems (Critical) shall be checked for malicious and mobile code embedded within the software.
- All the applications developed in-house must follow secure coding and SDLC practices.
- Application controls shall be designed into all application systems to prevent loss, modification or misuse of user data. These controls shall include, but not limited to, Validation of input data
    - Message Integrity
    - Validation of output data.
- Where software development is outsourced, the following points shall be considered:
    - Licensing arrangements, code ownership and intellectual property rights
    - Accuracy of the work carried out
    - Rights to audit for the quality and accuracy of work done
    - Testing before installation to detect backdoors or Trojan code.

3) Testing

- For Business-critical applications, all modifications, enhancements and installation of new systems shall be subject to testing for Integration testing, UAT, Functional Testing, Non-Functional Testing, capacity, stress testing, etc.
- The appropriate users shall do design testing and unit testing on the new systems prior to installation into the production environment.
- Where production data is copied or used in the test system, it shall be subject to a similar level of controls as the live version.
    - Separate authorization shall be required every time the operational data is used for testing.
    - Use of sensitive customer information or confidential information shall be avoided.
    - Sensitive operational information or personal information shall be depersonalized/ scrambled.
    - Copying or use of operational information shall be logged to provide an audit trail.
    - Operational information shall be erased from a test application system immediately after the testing is complete.

4) Implementation

- For software packages, system default settings shall be reviewed prior to installation to determine potential security loopholes.
- Acceptance testing shall be done by the concerned users after the implementation of the system.

- For software packages, all third party-supplied default passwords shall be changed prior to the system being placed in a production environment.
- Appropriate training shall be given to the users of the new system.

5) Operations/ Maintenance

- All requisite procedures for operational tasks shall be documented. Access to this documentation shall be restricted.
- The systems shall be continuously checked for any malfunctions / possible compromise of the systems.
- All changes to the system shall be carried out in line with Change Management Procedures.
- Libraries containing application source code, production and executable shall be secured from unauthorized access and only an authorized person shall have "read-write" access to these libraries.
- The development team shall not have access to operational systems. For occasional and essential support purposes, the development team may be granted special access for a limited period (for example, by issuing secure passwords via "Change Control" procedure).
- System utilities other than organization application like compilers, source code, and editors shall be disabled from the operational systems.
- An audit log shall be maintained of all updates to operational systems and system applications.

6) Restrictions on Changes to Software Packages

- Vendor-supplied software packages shall be used without modification as far as possible.
- If it is necessary to make changes in the software package, the required changes shall be made with the consent of the vendor or may be obtained from the vendor.
- Analysis of the impact shall be done, where applicable, if the organization becomes responsible for the future maintenance of the software as a result of the changes.
- The modifications shall be tested and documented as per the Change Management Policy.

7) Operating Procedures Documentation

- All critical and key procedures that ensure a smooth functioning of Operations shall be documented in detail and must be available for viewing and understanding purposes after suitable authorization.

8) Securing application services on public networks

Prior to initiating or implementing application services on public networks, Information Owners and Information Custodians shall:

- Ensure that the Security Threat and Risk Assessment is conducted and address threats and risks related to electronic commerce;
- Confirm that a 'Privacy Impact Assessment' has been conducted and approved;
- Determine the security classification of the information and information system(s) involved;
- Ensure that the user notification and acceptance of terms and conditions of use comply with government policies and standards;
- Ensure multi-factor authentication is used commensurate with the sensitivity and value of the information;
- Develop and implement processes to maintain content currency;
- Confirm the information system has received security certification and accreditation; and,
- Develop Business Continuity Plans and supporting Disaster Recovery Plans.

9) Protecting application services transactions

Security controls shall be implemented to prevent incomplete transmission, misrouting, repudiation of transaction, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls shall include:

- Critical information shall transfer to the concern person over mail and shall be password protected.
- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

10) Protection of program source libraries

Information Owners and Information Custodians shall implement procedures to control access to program source code for information systems. Information Owners and Information Custodians therefore ensure that:

- Program source code shall be isolated and stored separately from operational information systems;
- Privileged users' access shall be defined and monitored;
- A change control process shall be in place to manage updating of program source libraries and associated items;
- Program source code shall be contained on any media and protected;
- Accesses and changes to program source libraries shall be logged.

19. Incident Management

Objective: The aim of this policy is to ensure that Organisation's information systems and data are protected from any actual or suspected security incidents. The definition of a security incident is an adverse event that has caused, or has the potential to cause, damage to an organizations assets, reputation and/or personnel. Security Incident management in IT is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

Scope: This policy applies to all users of the Organisation's facilities and equipment including staff and any third-party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

Policy: All Organisation employees, contractors and users with access to Organisation's equipment and information (in any format including electronic and paper records) are responsible for ensuring the safety and security of Organisation's systems and the information that they use or manipulate.

1) Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported to the IT Manager. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by IT Manager.

2) Reporting Information Security Events for IT Support Staff

Information security events and weaknesses must be reported to a nominated central point of contact within Information Services as quickly as possible and the security incident response and escalation procedure must be followed.

Security events can include:

- Uncontrolled system changes
- Access violations
- Breaches of physical security
- Noncompliance with policies
- Systems being hacked or manipulated

Security weaknesses can include:

- Inadequate firewall or antivirus protection

- System malfunctions or overloads
- Malfunctions of software applications
- Human errors

The reporting procedure must be quick and have redundancy built in. All events must be reported to IT Helpdesk.

3) Management of Information Security Incidents and Improvements

A consistent approach to dealing with all security events must be maintained across the organization. The events must be analysed and the security advisor must be consulted to establish when security events become escalated to a security incident. The security incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the organization on continuing operation during the security incident.

4) Collection of Evidence

If a security incident may require information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation for example concerning computer misuse, contact the IT Manager for advice.

5) Reporting Business impacting security incidents

A consistent approach to dealing with all business impacting events must be maintained across the organization. The events must be analyzed. The security incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the organization on continuing operation during the security incident.

6) Informing Stakeholder

- All business impacting incidents must immediately be informed to senior management.
- All such incidents must be attended to immediately and RCA must be provided.
- All incidents must be reported / presented to the management in review meetings.

20. Legal, Regulatory and Contractual Requirement

Objective: The primary objective of this section is to ensure all relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

Information Security Council along with legal department shall identify statutory, legal, regulatory and contractual requirements pertaining to information systems and shall communicate internally to ensure:

- Compliance with all relevant applicable laws and regulations related to information security.
- Legal restrictions imposed by Intellectual Property Rights (IPR) and copyright.
- Information security Officer (ISO, nominated head of Information security council) shall ensure adherence to all the information security policies of SFL.
- Activities involving personal data collection, processing and transfer shall be designed to protect the privacy of personal information. Access to personal information shall be given to authorized persons only.
- Purchase and use of third-party tools / software shall be in accordance with third-party licensing agreements.
- IT infra team shall maintain an inventory of existing Applications, Software, Operating Systems and databases that SFL is licensed to use.
- List of allowed shareware / freeware software shall be maintained with approval.
- Periodic review shall be conducted for compliance and check for any deviations.
- The inventory shall be updated whenever there are any version updates, addition of newer applications etc.
- All users of software on SFL information systems shall strictly abide by "Copyright Law" and restrictions detailed by the software manufacturer.
- Purchase and use of third-party software shall be in accordance with third-party licensing agreements. The restrictions shall be considered for such software:
    - Specific user restrictions such as the number of copies allowed to be installed, the number of machines the software can be installed on, or the number of concurrent users of the software allowed at any one time.
    - Customer support levels (emails or phone)
    - The use or copying of purchased software so that it can be used on a computer other than the computer for which it is licensed shall be strictly prohibited
    - The duplication of the media, documentation etc shall be prohibited.
- All restricted software / freeware/ shareware except the software mentioned in allowed list shall be removed immediately, if found. Parties responsible for loading and/or using non-compliant software shall be subject to disciplinary actions by SFL.
- Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
- Important records shall be protected from loss, destruction and falsification and securely retained to meet statutory or regulatory requirements, as well as to support essential business activities as specified by the owner of the information.
- Any use of information and information assets for non-business use shall be restricted for defined purpose only (sometimes the assets are used for meeting social responsibilities identified by organisation or government directives)

- Periodic audit shall be undertaken to ensure compliance with SFL information security policies.
- ISO shall ensure technical compliance-checks like vulnerability assessment or/and penetration testing to identify vulnerabilities in IT systems. These assessments shall be conducted periodically and/or when significant changes are applied to IT systems.
- ISO shall ensure corrective actions for all information security incidents that are reported and a periodic review of the same.

21. Non-compliance

- All employees and third-party staff using SFL Information assets shall comply with this Policy.
- Non-compliance with the IT Policy is ground for disciplinary action(s), up to and including termination. Decision of disciplinary authority shall be final.
- If it is found that the action is inadvertent or accidental, first violation shall result in a warning. A relevant warning letter shall be placed in the involved individual's personal file. Subsequent violations could result in dismissal.

22. Exception Management

If, due to any constraint in the application or infrastructure environment or business mandate, it is not possible to implement any controls specified in the policy, an exception to override the security policy shall be requested. The exception shall have a valid business justification and be approved by the Head of Business Function (which is requesting the exception), and CIO.

These exceptions shall be valid only for the period substantiated by business function. Within this period, an alternative solution shall be put in place to avoid overriding the security policy. In a case where there is a need to renew the exception request, this shall be treated as a new exception.

23. Glossary

Head	Description
Changes - Statutory	Which are received as statutory guidelines from process owners.
Changes - Emergency	Which are received in any functional module in order to meet an immediate and critical need. These shall be with approval of Functional Head / VP -IT / CIO. Such changes generally affect only one process or function in a system.
Changes - Minor	Which is brought on by a change in user requirements or for ease / simplicity of working or a technical problem. Such changes typically affect only one process or function in a system.
Changes - General	Which is a modification in reporting formats, addition of filters / options, additional of some rows / columns.
Assets - Physical	Includes computer equipment (CPU, Peripherals etc.), communication equipment (routers, switches, etc.), magnetic media (CDs, Tapes, Disks).
Assets - Software	Includes various applications programs, system software, development tools and utilities.
Assets - Information	Databases, data files, archived information, documentation.
Assets - Services	Include communication services, general utilities like power, AC etc
Role - ISO	Information Security Officer.
Role - CIO	Chief Information Officer.
Role - OS	Operating System
Information - Confidential	It is defined as data, which if compromised, is likely to result in significant and/or long-term harm to the SFL or institution owning the data. This type of information shall be strictly protected from unauthorized access, modification, transmission, storage, destruction, or use. Access to confidential information is restricted to those who have a legitimate purpose for accessing such information
Information - Internal	Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This data shall not be shared outside the organization while the use internally in SFL is permitted.
Information - Public	Information that may or must be open to the general public. Public data, while subject to disclosure rules, is available to all employees and all individuals or entities external to SFL.

Annexure 1: Requisition form for IT Equipment

To be filled by the User

User's Name	
Department & Unit	
Equipment Type	☐ Desktop ☐ Scanner ☐ Server ☐ Laptop ☐ Software ☐ Net Work Equipment ☐ Printer ☐ Licenses ☐ Others…… In case of Laptop, please specify why a desktop cannot be used…… …… …… *If personal printers (not shared) are required then, please ensure that there should be substantial amount of confidential document printing or a shared printer is not accessible within 30 meters.*
Reason for Purchase	☐ New Recruitment ☐ New Requirement ☐ Replacement
Reasons & Benefit	

To be filled by the Concerned Departmental Head / HOZ Date:

Name		
Designation		
Remark		Signature

To be filled by the IT Team Date:

Is there any existing equipment available?	Yes No	
Make		
Specification		
Approx. Cost		
Quotations (If Required)		
If replacement, mention the no. of years for which the old equipment was used.		
Remarks (If any)		Signature (VP-IT / CIO)