Sudarshan Chemical Industries Limited

IT & Cyber Security Policy

Doc. No. SCIL/IT Policy/3.0

Release & Version Log

Rev. No.	Release Date	Nature of amendment	Supersedes ver.
3.0		Change in Policy	NA

Review Log

Activity	Date	Responsible	Role	Department
Prepared by	30-Sept-2022	Manish S. Pawar	Infra Lead	Business Technology
Reviewed by	06-Oct-2022	Sandeep T. Mhalgi	Head IT	Business Technology

1. **Purpose:** Policy is drafted to effectively manage and safeguard the use of all IT equipment, information, data, infrastructure and facilities by Sudarshan employees.

2. **Objective:** Optimal utilization of IT resources for maximizing business benefits while adhering to legal and Information Security requirements.

3. **Scope:** Management of IT infrastructure, Procurement of hardware/Software, SAP Basis Administration, SAP ABAP Development and Functional Support.

4. **Responsibility:** Process owner: Manager IT - (HOD)
   Others: Administrators, Developers, Functional Team Members, Hardware Coordinator

SUDARSHAN

Index

IT & CYBER SECURITY POLICY

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

A. Cyber Security

1. PURPOSE

Sudarshan Chemical Industries Limited and all subsidiaries ("Sudarshan" or the "Company") are committed to achieving a targeted level of protection from internal and external cyber security threats, and accordingly, will implement ongoing governance, policies, and practices which address the following objectives:

- Ensure business continuity, including the recovery of data in the eventof a security breach.
- Ensure compliance with all applicable laws, regulations, and Sudarshan's policies, controls,standards, and guidelines.
- Comply with requirements for confidentiality, privacy, integrity, and availability for Sudarshan's employees, contractors, vendors, and other users.
- Establish controls for protecting Sudarshan's information systems against any forms of harm or loss.
- Orient employees about information security to maintain the responsibility for, ownership of, and knowledge.
- Ensure the protection of Sudarshan's data and information assets.
- Ensure the availability and reliability of the network infrastructure, systems and the services.
- Ensure that external service providers are made aware of, and comply with, Sudarshan's information security needs and requirements.

2. SCOPE

This policy applies to all permanent and temporary employees of Sudarshan and all subsidiaries, and to directors, independent contractors, consultants, vendors, suppliers, agents, and other users of Sudarshan's IT resources (together referred to as "users") wherever they may be located. The policy is structured in the following categories:

A. Governance
B. Human factors
C. Information risk management
D. Data Security/Handling
E. Operations technology

Any breach of this policy is a serious offence and will result in the consideration of appropriate actions up to and including termination of employment, contract, or legal action.

IT & Cyber Security Policy

3. DETAILS

A. Governance

The assessment and management of Cyber Risk is integrated into our Enterprise Risk Management Systemfor the Company as a whole. Accordingly:

- The development and promulgation of a cyber security plan at the Company is the responsibility of the Business Technology.
- The implementation of the cyber security plan is the responsibility of Business Technology accountable for the results.
- Oversight of the effectiveness of the cyber security plan is the responsibility of the Business Technology.
- Cyber risk should be reflected in reports and updates to operations management, seniormanagement as well as the Board of Directors of the Company at least half-yearly.
- Cyber risk shall be considered for changes made to information and technology environment.

B. Human Factors

Authorized use: Sudarshan provides access to information technology to users, including the internal environment, the internet, where relevant and useful for their roles within or for Sudarshan. Sudarshan prohibits use of IT resources for any purpose other than business, unless otherwisestated in this policy. All users must behave honestly with vigilance, respect the intended business use of technologies. Users must comply with Sudarshan's Code of Conduct, Sudarshan's policies, and all applicablelaw when using Sudarshan's information technology resources, including without limitation privacy and intellectual property laws.

Limited personal use is acceptable provided that it does not affect job performance, is not for personal financial, commercial, or third-party gain, and if the user adheres strictly to this policy. Sudarshan systemsmust not be used for the creation or distribution of any material considered inappropriate, offensive, threatening, abusive, defamatory, unlawful, sexually explicit, sexist, racist, discriminatory, embarrassing,fraudulent or disrespectful to others. Sudarshan restricts all users from using the Internet to perform any task contrary to the law orknowingly accessing websites with content that is illegal, obscene, hateful, defamatory, indecent, objectionable, or inappropriate.

To maintain the integrity of Sudarshan's corporate image and reputation and to prevent the unauthorizedor inadvertent disclosure of sensitive, confidential or personal information, employees must exercise caution and care when using any system, service or technology platform, both internal and external, including email or third-party services, such as Cloud-based and social media. Personally identifiable information, which is any data that could identify a specific individual, should not be transmitted via emailor shared using any other service. Employees must also exercise caution against suspicious messages and technologies, which are often intended to bait a user into a malicious cyber event.

Passwords: Users are responsible for utilizing effective passwords and for keeping those passwords secret and secure. Employees must not disclose someone else's login or password.

IT & Cyber Security Policy

IT Department will support the mechanisms that evaluate the strength of passwords and define the password change frequency as stated in IT Password Policy **(Password Policy)**

Active Directory Accounts: Named accounts used by users must have a unique User ID and password and cannot be used by or shared with anyone other than the for whom it is intended. Personnel external to Sudarshan (i.e. consultants and/or contractors) should also be provided with uniqueuser IDs and passwords, and follow the same internal controls relating to the granting and/or revoking ofaccess as internal Sudarshan accounts.

Contractors, vendors and/or consultants must ensure all accounts/passwords assigned to them cannot be used by or shared with anyone other than for whom it is intended.

***Confidentiality*:** Sudarshan prohibits the release of confidential information to any third party, or use of confidential information, except as required in the performance of Sudarshan-related work and in accordance with the terms of the applicable confidentiality agreement.

Privacy: Users should have no expectation of personal privacy in anything they create, store, send or receive by e-mail or when using any corporate application if they use equipment (e.g. mobile device, computers) owned or provided by Sudarshan. Sudarshan reserves the right to review and collect all information contained in e-mails, whether or not stored solely in personal folders on the computer operated by the user, and in all equipment owned or provided by Sudarshan.

***Ownership*:** Data and user's work and work products belong to Sudarshan, including all messages,sent or received regardless of the device or application used to produce, send or receive it.

***Security*:** If used unwisely, the Internet can be a source of security problems that can do significant damage to the Company. Users must adhere to **(Internet and Intranet Acceptable Usage Policy).**

IT & Cyber Security Policy

Awareness, Communication and Training:

New Employees: To mitigate the risk of unintentional disclosure of confidential information by employees, Human Resources will refer newly onboarded employees to this policy and will require formalacknowledgement that it has been read, is understood and will be applied.

New and Existing Employees: To mitigate the risk of unintentional disclosure of confidential informationby employees, cyber security policy training and awareness sessions will be provided as an integral part of employee onboarding and existing employees. In addition, acknowledgement of this policy,that it is understood, and that the employee agrees to apply it will be included along with the sign off from employees.

Third Parties: Third parties, vendors, suppliers, partners, contractors, service providers, or customers requiring connectivity to Sudarshan's network or access to Sudarshan's data must comply to (**Third party Service Delivery Policy)**

C. Information Risk Management

The Company will develop, maintain, and periodically review risk statements that:

- Articulate its position with respect to cyber risk.
- Specifically address the degree of protection (as measured by a "cyber maturity index" or someother appropriate benchmark) that we are targeting.

The Company will develop, maintain, and periodically update as required, an inventory of major types ofinformation and systems based on criticality to the business. This list, on a priority basis, will be used to formally assess the degree of cyber protection that the company has, the target degree of protection as well as the plans that are in place to achieve the desired level of protection. The target level will reflect the nature of the information or application as well as the risk statements defined above.

D. Data Security/Handling

Business Technology is responsible for the Data Security to ensure the protection and business continuity. Critical data across organization is created/captured/stored by means of software application or by way of using the office automation tools. Such critical data is further categorized into 2 groups. One is structured data and other is un-structured data.

Data Security

Structured data

1. Every user is provided with username & password after registering on Windows AD (Active Directory) to be able to access Sudarshan network
2. Software application specific credentials are issued to end users to access an application. This is required over and above the credentials provided as per point no 1
3. Authorizations within application are provided based on the role of user
4. Backup schedule is in place which ensures that, application data is backed up at a set frequency

Un-Structured Data

IT & Cyber Security Policy

1. Every user is provided with username & password after registering on Windows AD (Active Directory) to be able to access Sudarshan network
2. Department/Function wise data storages are created on File Server.
3. Access is provided to user for his/her own Department/Function storage for storing critical data.
4. User cannot access data other than his/her own function
5. Backup schedule is in place which ensures that, un-structured data is backed up at a set frequency

Data Handling

Approved services for the uploading or sharing of company data

Approved Services provided by Sudarshan.

- Sudarshan's SharePoint
- Sudarshan's OneDrive for Business Online
- Sudarshan's Email System

Use of SharePoint and OneDrive to provide shared access to information with authenticated external users

SharePoint and/or OneDrive may be used to share information / data; users should keep in mind disclosure and confidentiality considerations as materials on SharePoint and/or OneDrive can be downloaded / manipulated / distributed.

- A folder or file can be created and shared externally via SharePoint and/or OneDrive and access, such as read, modify, delete, download can be granted to an authenticated external user depending on requirement.

- Anexpiration date should be set, for folder or file shared with external user via OneDrive, to ensure that post expiry date, folder or file cannot be accessed.

Exception

- In case data needs to be shared using other than the approved services mentioned above, approval of HoD of concerned department, at the level of Band 1/ 2 is required.

IT & Cyber Security Policy

E. Operations Technology

Data, applications, and networks, new software and IT equipment along with change management: No infrastructure/software should be installed/changed on Company-owned devices unless approved by the Business Technology. This should comply with the **(Change Management Policy)**

Viruses and Malware: To defend the company from computer viruses and malware, all computers anddevices connecting to Sudarshan' s infrastructure must be approved devices and have the standard, authorized antivirus and malware protection software installed. It is responsibility of the Business Technology to keep this software updated and of users to report to the Business Technology for any sign of infection. Refer policy **(Anti-Virus Policy)**

Remote Access: Users must secure their remote access credentials. 'Save Password' options should not be used. Users must avoid public / open network while connecting remotely to Sudarshan's network.
Remote access will be provided through VPN client only.

Bring-Your-Own-Device (BYOD): Users must comply to the BYOD Policy **(Bring you own device policy)** in order to use personally-owned devices to access Sudarshan's information and resources.

***Equipment*:** Users are responsible for the hardware assigned to them. Relocations and transfers ofequipment must be approved by the Business Technology.

Incident management: To promptly respond to threats, users are expected to communicate informationsecurity incidents to Business technology. Security incidents include any violation of this security policy that compromises corporate data, uninstallation/non-functioning of antivirus, presence of unknown software, non-functioning of approved applications. **(Incident Management Policy)**

IT & Cyber Security Policy

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

1 Acceptable Use of Information and Information Assets Policy

1.1 Objectives

This policy covers the general information security policy of SUDARSHAN.

1.2 Applicability

The Policy applies to all SUDARSHAN Employees, contractors, vendors, and entities identifying threats to information assets or information systems. Exceptions to this policy must be approved by the IT Head.

1.3 Policy

All employees, contractors and vendors, as well as anyone using or accessing SUDARSHAN's information assets shall comply with this policy. Violators of any policy are subject to disciplinary action of the organization's policy.

a. All information assets and systems within the organization are property of SUDARSHAN and shall be used in compliance with SUDARSHAN's policy statements.

b. Any information placed on SUDARSHAN's information system resources and on cloud resources shall be property of SUDARSHAN

c. Copyright and licensing agreements shall not be violated.

d. Any attempt to circumvent SUDARSHAN's security policy procedures shall be strictly prohibited.

e. Unauthorized use, destruction, modification, and/or distribution of SUDARSHAN's information assets or information systems shall be prohibited.

f. All employees shall acknowledge understanding and acceptance by signing the appointment letter / client specific NDA prior to use of SUDARSHAN's Information Assets and Information Systems.

g. All contractors and vendors, as well as anyone using or accessing SUDARSHAN's information assets shall acknowledge understanding and acceptance by signing the Non-Disclosure Agreement prior to use of SUDARSHAN's Information Assets and Information Systems.

h. All users shall report any suspicious activity found / observed about Information Assets to IT Head immediately up on detection.

i. SUDARSHAN's Information Systems and Information shall be subject to monitoring at all times. Use of SUDARSHAN's information systems constitutes acceptance of this monitoring policy.

IT & Cyber Security Policy

j. All policy statements shall be reviewed once in a year and updated as & when required.

k. Through its legal office, SUDARSHAN shall cooperate with law enforcement authorities regarding information security and related incidents.

l. SUDARSHAN shall protect the data & privacy of personal information.

m. Use of any information systems or dissemination of any information in a manner bringing disrepute, damage, or ill will against SUDARSHAN shall not be permitted.

n. Release of information shall be in accordance with SUDARSHAN's policy statement.

o. Users shall not attach their own or any third-party computer or test equipment to SUDARSHAN's computers or networks without prior approval of IT Head.

p. Management constraints and supplemental controls (such as checklists, operating instructions, and so on) shall be in place to provide an acceptable level of protection against unintentional human threats such as inadvertent blunders and improper maintenance.

1.4 Roles, responsibilities and authorities

RACI Chart

Activities	HR Head	IT Head	Employee
Policy / NDA Acceptance Document Signing	R	A	I
Policy Implement/Monitor	R	A	R

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

2 Access Control Policy

2.1 Objectives

SUDARSHAN recognizes that user access control is important in order to safeguard information and computing resources from unauthorized access. This policy is designed to provide guidance on development, communication and implementation of procedures for access control.

2.2 Applicability

The Policy applies to all organizational employees, contractors, vendors, and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the IT Head.

2.3 User Access Management

2.3.1 User Registration

A formalized user registration and de-registration (provisioning) process shall be in place for granting and revoking access to all information systems and services.

User registration processes and system access decisions must take into account the following principles:

2.3.2 Unique ID

Each user shall be uniquely identified when authenticating to any SUDARSHAN or managed system so that users can be accountable for their actions. This identification must be sufficient to trace the initiation and/or completion of any system process or transaction. Appropriate controls to allocate privileged access rights allowing users to override system controls, shall be in place.

Generic or multi-user usernames and passwords are prohibited, except as specifically authorized by the SDM IT.

Default system accounts such as 'Guest' and 'Administrator' shall be renamed wherever technically possible.

2.3.3 User Registration Process

A documented process for providing and approving user access to applications, systems, databases and networks shall be implemented. The process shall consider the following internal control principles for access control:

a. A documented request shall exist for the creation of all new user accounts or changes to user's access.

IT & Cyber Security Policy

b. The provisioning of a new user shall be initiated by HR as part of the new hire process; with user's direct supervisor and system 'Owners' approving the account setup process.

c. Authorization access shall be provided on the basis of least privilege concept.

d. IT manager shall obtain formal approval from system owners prior to granting a user access to the system.

e. Access privileges on information systems may be granted only after the authorization process is complete.

f. Auditing and logging of the administration process to grant privileges should be implemented and provide adequate information to recreate privilege changes, role changes, access level/privilege by system, user, etc.

g. Requests for system access and approvals should be well documented and retained for audit and compliance purposes.

2.3.4 User De-Registration/Terminations Process

A documented termination process, to be administered by Human Resources, shall be established. This process shall ensure all application, system and network access is immediately removed. The de-registration process shall include removing user access for the following:

a. Workstation/PC/laptop

b. Network

c. Applications

d. Database

e. Remote access/VPN

f. Physical security controls (access cards, etc.)

g. Mobile phones and other mobile devices

h. Other physical property issued to the associate

These procedures apply to the termination of all SUDARSHAN employees, contractors and other third parties.

2.3.5 Role Changes

As a user moves into a new role, process shall exist to revise the user's new access requirements. The process, principles and standards required for the user registration process should be applied to role changes as well. All requests, approvals, etc. for role changes shall be well documented and retained for audit and compliance purposes.

2.4 Privilege Management

User access privileges shall be based upon predefined user. Certain other considerations apply to user privilege management including the following:

2.4.1 Least Privilege Principle

IT & Cyber Security Policy

Access control decisions must comply with the principle of least privilege, which mandates providing minimum access to perform assigned duties and responsibilities.

2.4.2 Privileged Rights Accounts

A request/approval process shall be established for the management of privileged credentials. This process may be the same as the user registration process but may require additional levels of approval.

Privileged credentials shall be limited to a small number of trusted employees. The following standards shall be followed:

a. For Approved Purposes: Privileged IDs must be used only for the approved purpose (i.e., data transmission, system-level ID in Client/Server application, transaction ID, etc.).
b. There are identified privileged ID's and are having privileged access across the landscape, and they are with IT team only. (ARIBA, BASIS, DDIC, FFUSER, FFUSER7, PLANVISAGE, SAP_WFRT, SAP*, SAPCONNECT,SAPOSS)
c. In SAP application – User and owner will be the same If transport request pertaining to approved authorization changes created by BASIS ID.
d. Not to Supplement System Access**:** Associates are not allowed to use privileged IDs to supplement their individual system access.

System activities performed with privileged access rights shall be logged, monitored and audited for inappropriate activities.

2.4.3 Credential Management System

Access to systems and applications by internal users shall be authenticated against an established credential management system where technically feasible and appropriate (e.g., Active Directory).

2.4.4 Emergency Access

Associates, who require emergency access credentials, must be pre-approved by SDM IT. Emergency access must be reviewed at least on a Monthly basis by the SDM IT and/or system owner.

The process for obtaining emergency access credentials shall require the following:

a. Documented justification for the emergency access requested (in ticketing system or other tracking system).

b. Specification of the individual employee who shall obtain such emergency access and the access type required.

c. Timeframe for validity of such access (not to exceed 48 hours).

d. Unless renewed based on written request, emergency access must terminate on the date/time specified in the original request.

Employees approved for emergency access must adhere to the following requirements:

e. The emergency access procedure shall be based on pre-staged emergency user accounts, managed and distributed in a way that can make them quickly available once approved.

f. The use of emergency accounts shall be carefully monitored and audited through security

audit trails at least daily to identify any misuse.

g. Automated procedures shall be established to deactivate emergency access after an emergency account has been used.

h. Within 24 hours of activating the emergency account, a report shall be documented to account for the nature of the situation and actions taken. This record shall be received and approved by management and the SDM IT.

2.4.5 Segregation of Duties

Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Adequate Segregations of Duty (SOD) shall exist among the originators and implementers of changes, employees with privileged system access, and those responsible for monitoring/governing privileged access.

Protection of System Audit tools:

Access to system audit tools, i.e. software or data files, shall be protected to prevent any possible misuse or compromise. Such tools shall be separated from operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection. Access to these audit trials shall also be logged.

2.5 User Password Management

The allocation of passwords shall be controlled through a formal management process.

Fire-call Ids shall be maintained with IT head in physical format & stored in a locker & updated periodically.

2.5.1 Enrollment and Account Activation

Accounts shall be activated securely, and the account administrator shall not know the password assigned to an account. If required temporarily, a mandatory password reset shall be in place to ensure prompt creation of a new password by the user upon their initial login. The use of generic and easily guessable 'default' passwords (e.g., 'Sudarshan', 'sudarshan123') is prohibited.

2.5.2 Transmission of User Credentials

User credentials shall be communicated through secure channels such as voice and sealed envelope. If transmitted using email, credentials shall be encrypted.

2.6 Review of User Access Rights

Management shall review user access rights at regular intervals using a formal process. The following User Access Review Standard applies to SUDARSHAN systems, devices and facilities. Access to all SUDARSHAN systems and devices shall be reviewed on a six monthly basis by system Administrator or by their designee. The review process shall be formalized and includes, but is not limited to, the review of the following areas:

a. Active and inactive user accounts

b. User access privileges, particularly to sensitive and privileged functions or locations

c. User access to conflicting application functions that may present Segregation of Duty conflicts

d. System administrator or privileged user accounts

e. Access to powerful system utility programs

f. Access to sensitive areas such as data centers, utilities, etc.

In the absence of automated control processes for user access and privileges reviews, manual reviews shall be performed once in six months. All user access reviews shall be documented and maintained for audit and compliance purposes. Access reviews shall be performed against Access Control Lists, which are generated directly from the system being reviewed and are already validated for accuracy.

Employees that perform user access reviews shall not be responsible for reviewing their own access rights and shall be independent from administrators. Reviewers shall not have update/delete access to the system. Additional related controls for managing user access rights include the following:

2.6.1 Inactivity Deactivation

All user accounts inactive for 90 days shall be disabled or deleted after confirmation from HR.

2.7 Network Access Control

2.7.1 Use of Network Services

a. Users shall only be provided with access to the services that they have been specifically authorized to use.

2.7.2 Internet Access Controls

a. Associates may use only the SUDARSHAN-approved internal or preapproved instant messaging solution.

b. Associates are not permitted to use publicly available facilities or programs for business related purposes (or as defined in the Code of Conduct) such as chat rooms, bulletin boards, peer-to-peer file sharing software, social networking sites, instant messaging clients and news groups.

c. Associates may use only the SUDARSHAN-approved internal or preapproved instant messaging solution.

d. Web content filtering software shall be used to manage the internet traffic of all employees.

e. Use of Social Media and Networking services is prohibited

2.7.3 Segregation in Networks

IT & Cyber Security Policy

a. Groups of information services, information systems shall be segregated on networks.

2.7.4 Guest Access

Access shall be given as per BYOD policy

2.7.5 Production Network

SCADA Network shall be isolated & shall not be connected to main IT Network.

2.7.6 Network Connection Control

a. Physical access to perimeter Network Devices shall be controlled as per physical security standards for production systems.

b. Users with permission for network device configuration changes (Enable) should be kept to the minimum.

c. Changes to network device configurations shall be made as part of an established change control process.

d. There shall be a documented policy on Mobile Computing and Teleworking.

2.7.7 Network Routing Control

Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

a. Run the latest stable and available, sanitized router operating system version after due testing. Allowance will be given for specific instances where certain devices are required to run older releases, as recommended by the vendor, as part of workaround/remediation efforts.
b. Test the security of mission-critical routers, firewalls regularly, especially after any major configuration changes.

2.7.8 Network Device Security Checklist

This security checklist is designed to help the IT manager to review the status of the security configuration associated with network devices.

a. Operating system version checked and up-to-date.

b. Configuration kept off-line, backed up, access to it limited.

c. Configuration is well-documented, commented.

d. Users and passwords configured and maintained.

e. Password encryption in use, enable secret in use.

f. Enable secret difficult to guess, knowledge of it strictly limited (if not, change the enable secret immediately).

g. Unneeded network services and facilities disabled.

h. Necessary network services configured correctly (e.g., DNS).

i. Unused interfaces and VTYs shut down or disabled.

j. Port and protocol need of the network identified and checked.

k. Access lists limit traffic to identified ports and protocols.

l. Access lists block reserved and inappropriate addresses.

m. Static routes configured where necessary.

n. Routing protocols configured to use integrity mechanisms.

o. Logging enabled and log recipient hosts identified and configured.

p. Devices' time of day set accurately, maintained with NTP.

q. Logging set to include consistent time information.

r. Logs checked, reviewed, archived in accordance with local policy.

s. SNMP disabled or enabled with strong community strings and ACLs.

2.8 Operating System Access Control

Operating system controls shall be in place to prevent unauthorized access to operating systems. For more details, please see Password Policy.

2.9 Application and Information Access Control

Access to information and application system functions by users and support associates shall be restricted in accordance with the defined access control policy.

2.10 Mobile Computing, Teleworking, and Remote Access

Mobile Computing, Teleworking, and Remote Access policies shall be put in place to ensure information security when using mobile computing and teleworking facilities.

System Requirements

Only corporate-approved security products and services must be used to connect and authenticate to SUDARSHAN networks.

2.11 Teleworking

Policy shall be developed and implemented for teleworking or remote access activities.

2.12 Roles, responsibilities and authorities

RACI Chart

Activities	HOD	IT Head	Sys. Admin	User	HR
Policy enforce/change	A	R	C	I	I
Adherence to policy	R	A	R	R	R
Monitor / Review access control	R	A	R	I	I
Access control configuration	C	A	R	I	C
User registration process	C	A	R	I	R

Note: R- Responsible, **A-** Accountable, **C-** Consult, **I-** Inform
HOD- HOD of respective business function

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

3 Asset Management Policy

3.1 Objectives

This policy supports the implementation, identification, and management for all SUDARSHAN information assets.

3.2 Applicability

The Policy applies to all organizational employees of SUDARSHAN, contractors, vendors, and any other person using or accessing Organizational information or information systems. Exceptions to this policy must be approved by the IT Head.

3.3 Policy

a. All staff shall have the necessary and suitable equipment to perform their duties and to ensure that copyright and licensing regulations are observed.

b. All staff members are responsible for the assets issued to them. Ownership of Assets remains with the organization.

c. Equipment shall be effectively and safely operated and maintained according to manufacturer's specifications.

d. The upgradation, maintenance and replacement of information technology equipment shall be planned through Change control process.

e. Vendor's information of all vendors shall be maintained who all are responsible to support the assets.

f. All information assets shall be tagged and labelled with unique identity and standard.

a. IT Asset	b. As per asset code allocated by Finance Dept.
c. Non-IT Asset	d. Unique serial number by IT Dept

g. Asset management is an integral part of the organization's operation, and its application ismonitored and reviewed on a six-monthly basis

h. All assets are appropriately covered under maintenance and necessary assets are insured and recorded on the asset register.

i. Each staff member shall be responsible for the security of assets under their control. Assets shall be safeguarded against theft and damage and removed from the premises only with approval (In & Out Asset Process need to check)

j. Asset movement register shall be maintained to track the in and out of the asset from the premises.

k. Any changes to an information asset shall be documented on the Information Asset Register and follow the correct change control process.

l. Necessary procedures and controls shall be in place to ensure the confidentiality, integrity, and availability of the information assets.

m. Promoting information asset awareness throughout the Organization by conducting training, awareness campaigns and providing written procedures/guidance that are widely disseminated and available to staff.

n. The purpose of the Information Asset Register is to obtain information about the information assets within the Organization, what their purpose is, where they are, what type of information is stored and who is responsible and has access to them.

o. Approved Business Continuity Plans must be in place for all critical Information Assets and all staff members are aware of their roles and responsibilities. (Refer to BCP policy & procedure)

p. Asset disposal may occur through auction, tender, private sale, destruction, donation and transfers to other organizations.

q. The method of asset disposal will be based on consideration of what offers the best return and best furthers organization's objectives and considers environmental responsibilities.

3.4 Roles, responsibilities and authorities

RACI Chart

Activities	Fin. Dept.	IT Head	Sys admin	User
Endorse & Comply Asset Management Policy	A	R	C	I
Maintenance of Assets	I	A	R	R
Acceptable usage of Assets	I	R	C	A
Maintain Asset Inventory	I	A	R	I
Asset disposal	A	R	C	I

Note: R = Responsible, A = Accountable, C = Consult, I = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

4 Backup & Restore Policy

4.1 Objective

This policy covers the copying of data to a medium from which it can be restored in the event the original data is destroyed or compromised. A sound backup plan involves keeping backup media off-site and developing procedures for replacing system components after a system failure.

4.2 Applicability

The Policy applies to all employees of SUDARSHAN, contractors, vendors, and any other person using or accessing information or information systems of the organization. Exceptions to this policy must be approved by IT Head.

4.3 Policy

a. All business essential data shall be considered in backup policy and backed up as per Backup and Recovery Procedure.

   i. Business Essential data as follow, but not limited to the list specified below:

   ii. Project Data

   iii. Financial data

   iv. HR Data

   v. Admin

   vi. IT support Data

   vii. Email Data

   viii. Production Data

   ix. Third Party Software's

b. Active Devices (e.g. Firewall. Storage, Switches)

c. SAP Data

d. Email backup shall be taken daily as per approved schedule.

e. Records and logs of Backup and Restore shall be maintained as per log management policy.

f. Monthly backup shall be located off-site, in case on site backup becomes unavailable for any reason.

g. Backups shall be tested for reliability and data integrity quarterly.

h. Data restore request ticket shall be raised by authorized people (Data owner/Management)

i. Storage of backup should be stored at safe and controlled environment and only authorized people should have access to it.

j. All full backups shall have retention period as per approved period given in the followingtable.

Backups shall be run off-hours or required efficient mechanism will be used for online backup to minimize the impact to users and systems.

a. Backed devices are labeled and stored in a safe place

b. Backup shall be taken on approved media.

c. Backup of Data stored on local devices is the responsibility of the respective individual user.

d. Users shall store its local data on shared folder assigned to them.

Exclusion

Backup Policy is not applicable to Cloud Applications.

4.4 Roles, responsibilities and authorities

BACKUP FREQUENCY & RETENTION TABLE AS PER TABLE AVAILABLE WITH IT MANAGER

RACI Chart

Activities	Data Owner	IT Head	Sys Admin	User
Identification of Critical data	A	R	I	
Backup Restoration testing	R	A	R	I
Maintain Backup Records & logs	R	A	R	I
Offsite Backup	C	A	R	
Scheduling of Backup	R	A	R	

Note: R- Responsible, **A-** Accountable, **C-** Consult, **I-** Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

5 Bring Your Own Device Policy

5.1 Objectives

This document provides policies, standards, and rules of behavior for the use of personally-owned smart phones and/or tablets, Laptop by SUDARSHAN employees to access company's resources and/or services. Access to and continued use is granted on condition that each user reads, signs, respects, and follows the SUDARSHAN's policies concerning the use of these resources and/or services.

This policy is intended to protect the security and integrity of SUDARSHAN's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms

5.2 Applicability

The BYOD Policy applies to all employees of the organization, contractors, vendors, and any other person using or accessing information or information systems of the organization. Exceptions to this policy must be approved by the IT Head.

5.3 Policy

Acceptable Use

The company defines acceptable business use as activities that directly or indirectly support the business of SUDARSHAN

The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

Devices may not be used at any time to:

a. Store or transmit illicit materials

b. Store or transmit proprietary information

c. Harass others

d. Engage in outside business activities

Employees may use their mobile device to access the following company-owned resources:

a. Email

b. Teams

c. One Drive for Business

IT & Cyber Security Policy

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

SUDARSHAN has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

The following devices are supported:

a. iPhone

b. iPad

c. Android Phone

Note- Employees should contact the device manufacturer or their carrier for operating system or hardware-related issues

Security

a. In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.

b. The device must lock itself with a password or PIN

c. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

d. Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the network.

e. Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network.

f. Employees' access to company data is limited based on user profiles defined by IT Team and automatically enforced by Mobile device management software.

g. All those employees who are provided access to above company-owned resources through Mobile Device Management software must access the resources through profile created by Mobile Device Management software.

h. Accessing company-owned resources by any other means than mentioned above is strictly prohibited.

Risks/Liabilities/Disclaimers

a. The company reserves the right to disconnect devices or disable services without notification.

b. Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

IT & Cyber Security Policy

c. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.

d. The employee is personally liable for all costs associated with his or her device.

e. The employee shall be liable for risks including, but not limited to, the partial or complete

loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

f. SUDARSHAN reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy

5.4 Roles, responsibilities and authorities

RACI Chart

Activities	User	System Admin	SDM IT
BYOD Health Check	I	R	A
BYOD Declaration	R	I	A

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

6 Capacity Management Policy

6.1 Objectives

The purpose of this document is to detail the correct performance and capacity management procedure that is to be followed for systems and applications utilized in SUDARSHAN

6.2 Applicability

The Capacity Management Policy applies to all employees, contractors, vendors of the organization and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the IT Head

6.3 Policy

This policy is to ensure that the IT operational environment is well maintained to achieve stability of day-to-day processes and activities.

All IT equipment must be monitored regularly and a uniform process for performance and capacity management must be established. Equipment used to run key applications should be monitored more regularly.

IT operations management

A stable IT infrastructure must be designed and maintained.

The following areas must be managed at a minimum:

a. Server environments

b. Networks

c. Storage and archiving

d. Databases

e. Desktops / Laptops

f. Backups

g. ISP Bandwidth

Server Environment

Server equipment must be documented, and the following information must be maintained at a

minimum:

a. Host contact information and location of server equipment

b. Sever hardware and operating system version and serial numbers

c. Purpose/function of server equipment and applications

d. Configuration information (server name, IP Address, and application specific information)

All critical and security related patches/hot-fixes released by vendor(s) must be installed.

This must be installed in accordance with the SUDARSHAN's Patch Management Policy, and this applies to all services installed on the server equipment, even though those services may be temporarily or permanently disabled.

Server performance and capacity management

a. The System Administrator must ensure that controlled processes are in place in the server environment and that equipment remains current, with the appropriate patches/hot-fixes. All services and applications that are unused or not serving business requirements must be disabled except were approved by the Administrator.

b. Remote system administration (through privileged access) must be conducted using approved VPN secure solutions in accordance with the SUDARSHAN's Remote Access Policy.

c. All server event logs must be kept as per log management policy.

d. The Administrator must complete the Daily Operations Tasks Checklist

Monthly Performance and Capacity Management Checklist

a. Evidence of the completed and approved checklist(s) must be retained.

b. The Administrator must ensure that the configuration of server equipment, at a minimum the definition must document:

   I. Host contact information and location of server equipment;

   II. Server hardware and operating system/version;

   III. Purpose/function of server equipment and applications;

   IV. Configuration change management processes;

   V. Back-up requirements;

   VI. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO);

   VII. Escalation procedures.

c. The Administrator must isolate or otherwise disable any server equipment that has been compromised by an attacker or, otherwise places the SUDARSHAN's systems, data, users,

and clients at risk as stipulated in the SUDARSHAN's IT Security Policy.

d. The Administrator must ensure that servers are named in accordance with the server and device naming conventions to ensure consistency.

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

Monitor IT infrastructure

The Administrator must ensure that monitoring for system alerts and failures capture the following details:

a. Alerts or messages from consoles;

b. Exceptions in system logs;

c. Alarms generated by network management devices or access control systems; and

d. Logs required by the Company.

The Administrator must ensure that monitoring for system access captures the following details:

a. The ID of the user;

b. The date / time of key events;

c. The type of event;

d. The files accessed and their type; and

e. The programs or utilities used during access.

f. Rules that identify and record threshold breaches and event conditions must be defined and implemented. A balance must be found between logging minor events and significant events so event logs are not logging unnecessary information, thus impacting data storage capacity.

The following IT infrastructure capacity planning elements must be monitored:

a. **Server CPU utilization** - Check if CPUs are running at full capacity or being under-utilized. By monitoring server CPU utilization, you can monitor server Performance and restart a process or application to improve response time for the application;

b. **Server Disk utilization** - Monitor the hard disk space utilized by the system and ensure critical processes on the server have sufficient system resources;

c. **Server Process utilization** - Monitor memory and CPU utilization of processes. This helps identify system processes or server applications using high Server Resources;

d. **Network Availability** – to identify data bottlenecks or specific devices on the network using more resources than expected;

e. **Network traffic and Bandwidth usage** - Monitor Network Interface traffic on the server and understand how much network load is being handled; and

f. **Network devices** (routers, switches etc.) – Ensuring that network devices are functioning as

required.

g. Event logs and key indicators for critical systems and applications must be monitored and signed-off by the Administrator using the Daily Operation s Task

h. Incidents must be logged, as per the Helpdesk and Incident Management Policy, in a timely manner when monitoring activities result in the identification of deviations and/or violations.

6.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys. Admin	SDM IT	Sec. Forum	IT Head
Network monitoring	R	A	C	I
Server Performance monitoring	R	A	C	I
IT Infrastructure Monitoring	R	A	C	I
ISP Performance / Capacity Monitoring	R	A	C	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

7 Change Management Policy

7.1 Objectives

Change Management deals with the set of activities required when a change in the hardware, software and/or information assets profile of a user is initiated due to changes in the role, responsibilities or business needs of the user.

This policy addresses the process of controlling changes in applications and IT resources.

7.2 Applicability

The scope of this policy is applicable to changes in the information and IT resources of company involving implementation / modifications of new / existing systems, networks, applications, information processing facilities and relevant IT documents, plans and procedures.

7.3 Policy

All employees, contractors and vendors, as well as anyone using or accessing organization's information assets shall comply with this policy.

a. Changes in the information and IT environment shall encompass:
   - Assessment of probable impact of such changes on business and on security
   - Any implementation of new infrastructure / application/ functionality within existing applications
   - Any modification of existing resources
   - Any removal / disposal of existing resource

b. Changes shall be initiated through a formal Change Management Procedure/ Service Ticket.

c. With regards to applications, the development/test and operational environments shall be kept separate to protect from unauthorized access or change to the information assets.

d. All major changes shall require the approval of the IT Head

e. All changes shall be tested prior to their release in the environment.

f. The necessary updating shall be made in Asset inventory for changes pertaining to infrastructure.

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

7.4 Roles, responsibilities and authorities

RACI Chart

Activities	HOD	User	IT Head	Sec. Forum	Sys Admin
SR initiator	R	--	I	C	C
SR evaluation	I	--	A	R	R
SR approval	I	--	A	C	I
SR implementation	C	I	I	A	C
Post implementation review	I	I	C	A	C
SR documentation	R	--	C	A	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform
SR = Service Request
HOD = HOD of Respective Business Function

8 Clear Screen Policy

8.1 Objectives

This Clear Screen Policy directs all users of screens / terminals to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially.

8.2 Applicability

The Policy applies to all organizational employees of SUDARSHAN, contractors, vendors, and entities identifying threats to information assets or information systems. Exceptions to this policy must be approved by the SDM IT / designated representatives.

8.3 Policy

a. Confidential, sensitive or critical business information, on paper or on electronic storage media, should be locked away when not required, especially when the office is vacated.

b. Users should log off / lock their machines when they are not at their desk.

c. The users shall have password protected screen savers activated after Ten minutes or screen locking mechanism.

8.4 Roles, responsibilities and authorities

RACI Chart

Activities	HR	Sys. Admin	Admin	SDM IT	Employee
Policy Change	R	R	R	A	I
Policy Implement/Monitor	I	R	C	A	R

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

9 Cloud Computing Policy

9.1 Objectives

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on.

This cloud computing policy is meant to ensure that cloud services are **NOT** used without the IT Manager/Management's knowledge. It is imperative that employees do **NOT** open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the IT Manager/Management's input. This is necessary to protect the integrity and confidentiality of SUDARSHAN data and the security of the corporate network.

IT department of SUDARSHAN remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby SUDARSHAN employees can use cloud services without jeopardizing company data and computing resources.

9.2 Applicability

The Policy applies to all employees of SUDARSHAN, contractors, vendors, and entities identifying threats to information assets or information systems.

The policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded. One should contact the IT department if unsure of the scope and consideration of cloud computing. Exceptions to this policy must be approved by the IT Head

9.3 Policy

a. Use of cloud computing services for work purposes must be formally authorized by the IT HEAD

b. The IT HEAD will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

c. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by IT HEAD.

d. Non-disclosure agreement shall be signed with the cloud service provider

e. The use of such services must comply with SUDARSHAN's existing Acceptable Use Policy/ Internet Usage Policy/BYOD Policy.

f. Employees must not share log-in credentials with co-workers. The IT department will keep a confidential document containing account information for business continuity purposes.

g. The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by SUDARSHAN

h. The IT HEAD decides what data may or may not be stored in the Cloud.

i. Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

j. Pre-approved cloud computing services may include creating a user account, etc., to head off multiple requests for common cloud services, like Google Drive

9.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	IT HEAD	HOD
Agreement with Cloud vendor	I	R	A
Maintain Cloud Users	R	A	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	08 July 2022

10 E-Mail Security Policy

10.1 Objectives

Organizational E-mail Security Policy specifies mechanisms for the protection of information sent or retrieved through e-mail. In addition, the policy guides representatives of SUDARSHAN in the acceptable use of e-mail. For this policy, email is described as any computer-based messaging, including notes, memos, letters, and data files that may be sent as attachment.

10.2 Applicability

The E-mail Security Policy applies to all organizational employees, contractors, vendors, and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the IT Head.

10.3 Policy

Authorized users must comply with the following policies. Violators of any policy are subject to disciplinary actions including termination and/or civil and criminal legal action.

10.3.1 E-Mail Access:

a. All e-mail on organizational information systems, including personal e-mail, is the property of SUDARSHAN

b. The email ID is provided to the employees to assist in carrying out the business activities and is the official ID of the employee. The System Administrator can review the emails received/sent out from these IDs on business requirement.

c. User is not authorized to open or read the e-mail of another user.

d. E-mail is provided to the users and contractors of organization to enhance their ability to conduct organizational business.

e. The size of e-mail attachment shall be limited to 7 MB maximum which is necessary for a user to perform his or her function.

f. Group IDs should not be used to send or receive personal emails.

g. Users would be able to access email over the company provider Desktop/Laptop only. In case access to email is required over cell phone then approval of respective HOD at the level of Band 1/ 2 is required. Upon such an approved request IT Team would enable access over cell phone for the user using Mobile Device Management software.

10.3.2 E-Mail Contents:

a. Use of, inappropriate language, pornography, or misleading content in e-mail is prohibited.

b. Use of e-mail to spam (e.g. global send, mail barrage) is prohibited. This includes the forwarding of chain letters.

c. Use of e-mail for sexual or other harassment is prohibited. The mail from any user should not contain any words or phrases that may be construed as unprofessional or derogatory based on race, color, sex, age, disability, national origin, or any other category.

d. Forging of e-mail content (e.g., identification, addresses, etc.) is prohibited.

e. When forwarding or replying to a message, the content of the original message should not be altered.

f. Large files shall be transferred through official ftp server instead of as e-mail attachments or any external service (except approved service like one Drive)

10.3.3 E-Mail Usage:

a. Any e-mail activity that is in violation of the policy statements or that constitutes suspicious or threatening internal or external activity shall be reported.

b. When a user receives e-mail error messages that appear to be abnormal, they shall be reported to the System Administration Team.

c. When sending e-mail, users should verify all recipients to whom they are sending e-mail messages.

d. Users should understand that e-mail could be altered during transmission from the sender to the receiver, and the identities of the sender or receiver could be falsified. Users should carefully check when assessing whether e-mail is legitimate.

e. Emails should be used strictly for the business purpose, sending emails to other domains can be allowed as an exception as the business requirement.

f. Personal email ID should not be used for business purpose. Also, Business emails should not be forwarded to personal email Id.

10.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	IT Head	Employee	HR/HOD
Creating Email id	R	A	I	C
Email Policy	R	A	I	C
Email Control	R	A	I	C

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

11 Firewall Security Policy

11.1 Objectives

This Policy will document the procedures and mechanisms for requesting and applying changes to the firewall rule sets protecting the trust on its Internet Gateway

11.2 Applicability

The Firewall Policy applies to all employees, contractors, vendors of the organization and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the IT Head

11.3 Policy

a. A system designed to prevent unauthorized access to or from a private network through protecting and controlling both internal and external connections.

b. Firewall Security

The security of all the network devices may be addressed on two levels: the physical and the logical. These two aspects ensure that all devices are secure and that no unauthorized access is permitted.

c. Physical Security

The Firewall physical device is located in a secure area of the organization's premises. This location is restricted through the use of Lock and key. These areas may only be accessed by a restricted number of authorized staffs.

d. Logical Security

Access to the organization Firewall is governed by password authentication. Only the System Administrator is permitted access to the Firewall. Any changes to the device must be performed by system Administrator. No other member of staff is authorized or capable of accessing the Firewall.

e. Firewall Monitoring

Regular monitoring of the Firewall will occur so that the device is functioning properly. It will also ensure that the SUDARSHAN Network is being provided with the requisite protection.

f. Suspicious Activity Monitoring

The Firewall will be continually monitored for occurrence of any suspicious activity. This monitoring will enable the System Administrator to identify any potential threats arriving through the Firewall and enable a swift response to potential dangers.

g. Log File Monitoring

Due to the nature and size of log files, it is accepted that daily monitoring is not always feasible. As such, monitoring of Firewall logs will occur regularly at one-month interval & only under specific circumstances such as:

- An attempted intrusion
- Suspicious Inbound/Outbound activity
- On the request of the Management.

h. Security Monitoring

The System Administrator will perform regular auditing of the Firewall to ensure that the integrity of said devices has not been compromised. Examples of this auditing will take the form of regularly auditing access to the devices to ensure that only authorized users have gained access· monitoring the devices for any suspicious activity etc.

i. Analysis

Information gathered from the monitoring of the Firewall will be utilized to assess such areas as security. This will enable the System Administrator to efficiently assess the performance of the device and ensure that security is maintained.

j. Port Control

The Firewall will provide access to the trusted Network only through a restricted number of Ports. Any Port that is not used to provide a connection will be disabled to prevent unauthorized access and ensure the SUDARSHAN Network Security is maintained.

11.4 Roles, responsibilities and authorities

RACI Chart

Activities	System Admin	SDM IT	IT Head	Project Manager
Firewall Installation & Config	R	A	I	C
Port & Protocol Blocking/Disabling	R	A	I	C
Website Blocking/Disabling	R	A	I	C
Content Filtering	R	A	I	C

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

12 Incident Management Policy

12.1 Objectives

The purpose of this policy is to define the process for reporting security breaches within SUDARSHAN

12.2 Applicability

The Policy applies to all organizational employees, contractors, vendors, and entities identifying threats to information assets or information systems. Exceptions to this policy must be approved by the IT Head.

12.3 Policy

All employees, contractors and vendors, as well as anyone using or accessing organization's information assets shall comply with this policy. Violators of any policy are subject to disciplinary actions including termination and/or civil and criminal legal action.

a. Any event, incidence that is breaching the security of SCIL or violating the defined policies of SCIL shall be reported immediately to IT Department.

b. Any weakness observed in the security arrangements that challenge or compromise the security arrangements of SCIL shall be reported immediately to IT Department.

c. Immediately after the incident/weakness is known, a security incident can be raised through email. Email shall be sent to the IT Department at securityforum@sudarshan.com. This e-mail shall have details of whatever is known at the time the breach is discovered.

d. In case of unavailability of an e-mail, Security Forum Member shall be contacted immediately by any other suitable means of communication.

e. All the information regarding security incidents / weaknesses shall be maintained in a NC tracker by IT Head giving the details and the action taken.

f. If required the IT Head shall ensure that the department heads are contacting the relevant authorities such as law enforcement, fire department etc.

g. The IT Department members shall review, assess and analyze all reported incidents and provide a management summary to the Managing Director every six months.

h. Specific incidents of a more serious nature or with a potential for further negative impact on SCIL shall be addressed specifically with the Director.

i. Where a follow-up action against a person or organization after an information security incident involves a legal action, evidence shall be collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction by Security Forum.

j. Appropriate disciplinary action shall be taken against an entity or person believed to have been involved in the security incident.

k. Security forum shall take appropriate corrective & preventive action to reduce / eliminate occurrences of such incidences.

12.4 Roles, responsibilities and authorities

RACI Chart

Activities	Employee	IT Head	CIO	Security Forum
Incident raise	R	A	I	C
Change in Policy	I	A	C	R
Incident Action	I	A	C	R

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

13 Internet & Intranet Acceptable Usage Policy

13.1 Objectives

Internet / Intranet access is provided to organizational employees to conduct organizational business. While these resources are to be used primarily for company business, the company realizes that users may occasionally use them for personal work. Given that, users should use good judgment and be considerate of the needs of others when using these resources.

This policy outlines the acceptable use of internet/intranet facilities.

13.2 Applicability

The Policy applies to all company employees of company employees, contractors, vendors, and any other person using or accessing company's information or information systems. Exceptions to this policy must be approved by the IT Head.

13.3 Policy

a. Internet / intranet activities that can be attributed to the organizational domain address (such as posting news to newsgroups, use of chat facilities, and participation in mail lists) must not bring disrepute to organization or associate organization with controversial issues (such as objectionable or sexually explicit materials).

b. Internet / Intranet usage shall not have a negative effect on Organizational operations.

c. Internet / Intranet users shall not make unauthorized purchase or business commitments through the Internet.

d. Internet / Intranet services shall not be used for personal gain.

e. No unauthorized software shall be downloaded and installed on end user machines via the Internet without approval by the IT Head.

f. All Internet / Intranet users shall immediately notify the System Administration Team of any suspicious activity.

g. Access to various categories of internet sites such as but not limited to, malicious, phishing, gaming / adult etc. are blocked.

h. Company is authorized to poll reports & monitor internet usages.

13.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	IT Head	Employee
Policy change	R	A	I
Policy Implement/Monitor	R	A	R/I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

14 Licensing Policy

14.1 Objectives

The purpose of this policy is to define roles and responsibilities on the licensing of software within SUDARSHAN's Centrally managing licenses assists the SUDARSHAN to take full advantage of bulk or volume license pricing and reduces the possibility of redundant purchasing of Software Licenses. Incorrectly licensed software could lead to legal action being taken against the SUDARSHAN

14.2 Applicability

The Licensing Policy applies to all employees, contractors, vendors of the organization and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the IT Head

14.3 Policy

a. Users are required to conform to all SUDARSHAN policy and regulations on software licensing including, but not limited to, this policy and the Information Systems Statute. Breaches of this policy, may constitute misconduct or serious misconduct, and may result in disciplinary action

b. Users are required to conform with the Copyright Act 1994 and amendments, IT Act 2000 and amendments including but not limited to the copying, duplication, loading and use of licensed software

c. Users are required to conform to the terms and conditions of all license agreements for software loaded on to any Information System owned or administered by the SUDARSHAN.

d. Users of SUDARSHAN's licensed software are required to conform with the terms of all license agreements between the SUDARSHAN and any third party, including SUDARSHAN's licensed software installed or used on any system, computer, or device

e. Software must not be installed or used on SUDARSHAN owned Information Systems in any way that is in violation of the license agreement

f. SUDARSHAN's licensed Software must not be installed or used on any system, computer, or device in any way that is in violation of the license agreement

g. Software installed or used on SUDARSHAN's owned Information Systems in violation of its license must be uninstalled

h. SUDARSHAN licensed Software installed or used on any system, computer, or device in violation of its license must be uninstalled.

i. The party responsible for the software and the party responsible for the license must ensure

that they fully understand the implication s of any licensing agreement before acquiring or purchasing the software. For example:

1. Do not commit to license agreements that prevent the SUDARSHAN from removing any software; and
2. Exercise due care with any nested agreements allowing the automatic installation of additional software without authorization from the User

j. Adequate records must be kept by those responsible for management of any software, to ensure licensing information is available at all times.

14.4 Central Management of Software Licenses

IT Dept. will maintain an up to date list of SUDARSHAN managed Software Licenses.

a. Software Licenses to be used by SUDARSHAN must be purchased and managed by IT Dept./System Administrator Group

b. Software to be used by SUDARSHAN may be managed and installed by or third parties as delegated by IT Dept.

c. Users must inform and consult with IT Department prior to the purchase of any software to ensure the SUDARSHAN can take full advantage of any existing licenses, volume or bulk license pricing

d. Any installation of software by third parties as delegated by IT Dept. must be registered with IT Dept.

e. Ensuring compliance with the licensing agreement

f. Maintenance and renewal of the license agreement

g. Storing and retaining license documentation

h. Storing and retaining the documentation and media

14.5 Roles, responsibilities and authorities

RACI Chart

Activities	User	System Admin	SDM IT	Project Leader
Software Installation	I	R	A	C
Software License Compliance/Purchase	---	R	A	C
Software License Renewal	---	R	A	C
Software License Maintenance	---	R	A	C

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

15 Log Management Policy

15.1 Objectives

This document details the steps required to review the security logs of all system components within the Company environment periodically and following a security incident. Any exceptions identified are followed up and reported to Management. Employees of SUDARSHAN or any other third party authorized to monitor / handle / access the logs should familiarize themselves with this procedure.

15.2 Applicability

This policy applies to employees, contractors, consultants, temporaries, and other workers at SUDARSHAN, including all personnel affiliated with third parties, who use SUDARSHAN owned / rented Devices & assets.

15.3 Policy

Logs should be reviewed as per the requirement of the business as per the following manner.

a. Firewall Logs – Monthly

b. Antivirus Logs – Weekly and as per the incident

c. Operating System Logs (Server) – Weekly

d. Server Logs, Backup Logs, Application Logs - Monthly

Review of Firewall Log Procedure

The following Firewall Events are configured for logging, and are monitored by the System Administrator

a. ACL violations.

b. Invalid user authentication attempts.

c. Logon and actions taken by any individual

d. Configuration changes made to firewall

Review of Operating Systems Log Procedure

Any additions, modifications or deletions of user accounts

a. Any failed or unauthorized attempt at user logon.

b. Any modification to system files.

c. Any access to the server, or application running on the server

d. Actions taken by any individual with Administrative privileges.

e. Any user access to audit trails.

f. Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain System Administrator access to system)

Review of Antivirus Log Procedure

a. Alerts generated by antivirus software

b. Quarantine folder/ files

c. Whitelist of folders

Reporting

Any Deviations should be reported to SDM IT immediately.

Log Retention – Logs should be maintained/ retained for the period of one year on individual applications. Logs should be backed up while refreshing applications.

15.4 Roles, responsibilities and authorities

RACI Chart

Activities	System Admin	SDM IT	Sec. Forum
Firewall Log Review	R	A	C
Antivirus Log Review	R	A	C
Datacenter CCTV Log Review	R	A	C
Operating System Log Review	R	A	C
Backup Logs Review	R	A	C
Access control devices logs	R	A	C

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

Log Retention Period

Sr.	Activity	Period
1	Firewall Logs	90 Days
2	SAP Archive redo Logs	60 days
3	AD Server Logs	90 days
4	CCTV Footage	60 Days
5	Antivirus Logs	90 Days

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

16 Media Handling and Labeling Policy

16.1 Objectives

This policy ensures proper handling of electronic media containing business / personal and other data. Due to the diverse nature of the data stored on hard drives, removable media, and other Storage Devices, it is necessary to ensure proper media disposal to prevent unauthorized use after removal from service.

16.2 Applicability

The Policy applies to all organizational employees, contractors, vendors, and entities identifying threats to information assets or information systems. Exceptions to this policy must be approved by the SDM IT.

16.3 Policy

a. User shall not have access to CD/DVD drives, USB ports etc. unless it is authorized by respective Department Heads.

b. Bad/Old (unused) Tapes/Hard disks shall be labeled and kept in safe place in custody of System Administration Team.

c. Before a computer system or workstation is reallocated the hard drive shall be formatted, if required and software shall be installed as per Asset Transfer Process.

d. IT team is responsible to make sure that the all the sensitive / confidential information is completely erased or made unreadable from hard drive / any other storage media before the workstation / removable media is transferred, sold, salvaged, donated, disposed of, or otherwise sent outside of SUDARSHAN.

e. Damaged and unusable CDs/DVDs shall be broken and disposed with the help of shredding machine and an entry to this effect is made in the register.

f. A data cartridge tape/CD/DVD required to be taken outside the office building, its movement should be with the prior approval. A record of movement indicating full details like date/time of its being taken out with quantity etc., name of the person taking it out, purpose, date and time of its return, etc. shall be maintained by IT team. Administration head is responsible for reviewing material in-out register.

g. Whenever licensed software is resident on any computer media being, transferred, and traded-in, disposed of, or the hard drive is replaced the terms of the license agreement shall be followed by securely erasing degaussing or overwriting the media.

h. The media containing information should be protected against unauthorized access, misuse,

corruption, etc. during the transportation of data

16.4 Roles, responsibilities and authorities

RACI Chart

Activities	CIO	SDM IT/IT Head	Sys Admin	Admin	Employee
Policy enforce and Awareness	C	A	R	R	I
Disposal of Media	C	A	R	R	I
Media custody	I	R	A	R	I
Media handling & Labeling	I	A	R	R	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

17 Mobile / Laptop Device Policy

17.1 Objectives

All SUDARSHAN computer systems face information security risks. Laptop computers are an essential business tool but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside SUDARSHAN's premises increases the threats from people who do not work for the SUDARSHAN and may not have its interests at heart.

Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

Objective of laptop policy is to define guidelines and procedure that an employee has to follow if he/she has been allotted a laptop/notebook computer by SUDARSHAN.

This policy describes the controls necessary to minimize information security risks affecting SUDARSHAN's laptops.

17.2 Applicability

This policy applies to employees, contractors, consultants, temporaries, and other workers at SUDARSHAN including all personnel affiliated with third parties, who use SUDARSHAN's Laptops/Notebook Computers

17.3 Policy

Physical security controls for laptops

a. The physical security of 'your' laptop is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.

b. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

c. Keep a note of the make, model, serial number and the SUDARSHAN's asset label of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform the IT department as soon as practicable (within hours not days, please).

d. Use Laptops with approved OS with all relevant patches and updates applied as and when available, for ensuring the security of the information residing on the laptop.

e. Provide power on password as per SUDARSHAN's password policy.

f. To add a layer of protection to the laptop, a personal firewall product or IDS shall beinstalled.

g. Provide password for Folders containing confidential restricted or highly restricted information.

Virus protection of laptops

a. Viruses are a major threat to all and laptops are particularly vulnerable if its anti-virus software is not kept up-to-date. The anti-virus software **MUST** be updated daily. The easiest way of doing this is simply to log on to the SUDARSHAN 's network so that automatic update process will take place. If you cannot log on for some reason, contact the IT helpdesk for advice on obtaining and installing anti-virus updates.

b. Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.

c. Always scan all files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically but if it doesn't contact the IT Help/Service Desk to initiate manual scans if you wish to be certain.

d. Report any security incidents (such as virus infections) promptly to the IT Help desk in order to minimize the damage

e. Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Help desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

f. Be especially careful to virus-scan your system before you send any files outside the SUDARSHAN. This includes EMAIL attachments and CD-ROMs that you create.

g. Controls against unauthorized access to laptop data

h. You must use approved encryption software on all corporate laptops, choose a long, strong encryption password/phrase and keep it secure. Contact the IT Helpdesk for further information on laptop encryption. If your laptop is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.

i. You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.

j. Corporate laptops are provided for official use to authorized employees. Do not loan your laptop or allow it to be used by others such as family, friends & Personal Use.

k. Avoid leaving your laptop unattended and logged-on. Always Lock your device, log off or activate a password-protected screensaver before walking away from the machine.

17.3.1 Unauthorized software

Do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the SUDARSHAN's networks as well as affecting the working of your laptop. Software packages that permit the computer to be

'remote controlled' (e.g. PC anywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on SUDARSHAN equipment unless they have been explicitly pre-authorized by IT Department for legitimate business pur poses.

17.3.2 Unlicensed software

Be careful about software licenses. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate license fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and SUDARSHAN into disrepute by breaking the law.

17.3.3 Backups

You must take your own backups of data on your laptop. The simplest way to do this is to logon and upload a data from the laptop to the provided shared Drive on a regular basis – ideally daily, but weekly at least.

17.3.4 Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet).

17.3.5 Inappropriate materials

Be sensible! SUDARSHAN will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely audit the network and systems for such materials and use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, call IT Help desk to investigate further.

17.3.6 Health and safety aspects of using laptops

Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Balancing the laptop on your knees hardly helps the situation! Limit the amount of time you spend using your laptop. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. Stop using the portable and consult Health and Safety for assistance if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the portable.

17.3.7 Guide Lines

<u>When Traveling</u>

IT & Cyber Security Policy

a. Take care not to forget / misplace the laptop and thus prevent loss.

b. Don't keep your laptop kept unattended or out of sight, even during a security check at an airport.

c. Don't check in your laptop as baggage.

d. Always carry proper documentation with you when travelling.

17.4 Roles, responsibilities and authorities

RACI Chart

Activities	System Admin	SDM IT	User	Team Leader
Laptop/Mobile Allotment	R	A	I	I
Laptop/Mobile Return	R	A	I	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

18 Network Security Policy

18.1 Objectives

The purpose of this policy is to establish a comprehensive set of network security standards as SUDARSHAN Network security is crucial for maintaining the integrity of the data that organization relies on for everyday operations. Organizational network administrators have the primary responsibility for implementing and ensuring adherence to this policy, however all employees have a responsibility to protect the integrity of organizational network.

18.2 Applicability

The Network Security Policy applies to all organization employees, contractors, vendors, and any other person using or accessing organizational information or information systems. Exceptions to this policy must be approved by the SDM IT

18.3 Policy

18.3.1 General Network Security

General network security covers the protection of networks and their services that the network performs its critical functions correctly and there are no harms or side effects. It also provides information accuracy.

a. Accounts shall be considered inactive after 30 day(s) without a valid login. Inactive accounts are disabled and/or deleted.

b. No unauthorized user login scripts shall be used on the network. Only group and profile login scripts shall be used.

c. Vendor default passwords shall not be used and the administrator and supervisor accounts shall not be for general use. Network/System administrators shall use their own login accounts whenever possible.

d. Account rights and privileges shall be limited to what is necessary for a user to perform his or her function.

e. Files stored in a user's local hard disk cannot be accessed or viewed by another user without the originating user's permission.

f. Rights to file systems should be assigned on as-needed basis. Only the minimum rights necessary to accomplish a task should be issued.

g. The accesses to the user shall be granted as per the Joining / Resource reallocation form.

h. Terminated personnel shall not be provided access to any of organizational network assets

any time after termination.

i. Sensitive information shall be isolated and provided with restrictive access, on advice from respective data owners.

j. All Organizational Server and Network systems must be protected with appropriate protection mechanisms. Auditing to be enabled and logs to be retained as per log management policy.

k. System Administration Team shall review any privileged access rights assigned to special users once in a quarter.

l. Suitable test shall be carried out and proper approval shall be taken prior to installation of up-gradated versions, new servers etc.

m. System Administration Team shall take appropriate action on the information received from special interest groups or other specialist security forums like CERT.

n. All the Servers and Network devices should have time synchronization.

18.3.2 External Network Security

The intent of this policy is to protect organizational information assets and reputation by providing security requirements to any host connected to an external network of SUDARSHAN

a. System Administration Team must receive proper authorization from IT Head to allow users to connect to an external network

b. Services and trust extended from external networks shall be limited to the minimum necessary to accomplish the task requiring the connection

c. Both parties to an external network may audit the security of the connection

d. Questionable or unusual activities shall be immediately reported to the System Administration Team

e. Organizational sensitive or proprietary information shall not be stored on an external network

18.3.3 Internet Access/Firewall Security

Organizational firewall is a gateway that limits access between networks in accordance with Organizational Internet Access/Firewall Security Policy. This system, or combination of systems, enforces a boundary between two or more networks. All traffic from the inside out and outside in must pass through it, and only authorized traffic is allowed to communicate.

a. The network is divided into different sub-nets as appropriate to the requirements. The sub-nets are protected using appropriate firewall protection.

b. Any suspicious activity should be immediately notified to System Administration Team.

c. All Internet access shall be accomplished through approved firewalls and security processes.

d. Firewalls shall be placed between organizational network and the Internet to prevent unauthorized access to organization network.

e. Firewalls shall always perform security checks before routing packet from one network

interface to another.

f. Firewall shall not accept traffic on their external interface that appears to be from internal network addresses.

g. Firewalls shall audit the network traffic. Both approved and unapproved connections shall be audited.

h. Firewall audit logs shall be stored in a secure manner, such that only authorized personnel may access them.

i. Firewalls shall be configured to deny all inbound connections except those that have been previously approved.

j. Appropriate firewall documentation shall be maintained offline all times.

k. Firewall configurations shall be tested offline and verified before placed into service.

l. The System Administration team shall evaluate new releases of patches for firewall software, before implementation.

m. New releases of patches for firewall software shall only be obtained from the vendor or another trusted source.

n. The System Administration Team shall monitor available news sources from information about vulnerabilities in firewall software and how to patch or work around those vulnerabilities.

o. The System Administration head shall approve firewall configuration changes before being implemented.

p. Details of Organizational internal network should not be visible from outside the firewall.

q. Firewalls shall run on dedicated Server/Appliance, only software or services essential to firewall operation shall be installed or run.

r. Physical access to firewall shall be limited to members of the System Administrator Team.

s. Physical and Logical accesses to diagnostic ports shall be given only with proper authorization**.** The port shall be disabled after the use.

18.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	IT Head	SDM IT	Employee
Network Policy Awareness/Change	R	C	A	I
Access approvals	R	I	A	
Configuration change	R	I	A	
Access control	R	C	A	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

19 Password Policy

19.1 Objectives

SUDARSHAN recognizes that Passwordsare an important aspect of computer security. Poorly selected password represents one of the most vulnerable aspects of information security. Users must comply policies to minimize risk to corporate information assets. Policy outlines the password construct, usability, reset frequency.

19.2 Applicability

Policy applies to all company employees, contractors, vendors, and any other person using or accessing Company's Information or Information Systems. Exceptions to this policy must be approved by the SDM IT.

19.3 Policy

a. All system accounts must be assigned a unique user ID and password that are protected in accordance with company password policy statements.

b. All initial system user accounts shall be setup by the System Administration Team as per the Joining form.

c. First time users shall login to their account with the password provided to them by the system administrator and shall be required to change their password to a new password that complies with the corporate password policy.

d. Sharing of passwords is prohibited.

e. Copy of all critical passwords as per access control policy shall be kept with the IT Head, in a sealed envelope and contents shall immediately updated on any changes.

f. Any queries regarding passwords shall be reported to the System Administration team.

g. Accounts shall be locked out after 3 failed attempts. Account can be reactivated by contacting the System Administration Team.

h. Password shall be protected as organizational proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.

i. Using programs or scripts that include system passwords is prohibited.

j. Users shall change their passwords every 60 days.

k. User may reuse passwords only after 3 different passwords have been used

l. System Administration Team shall enforce required password changes out of cycle for certain security events that have the potential for security compromises (i.e. employee relocation, intrusion attempt, or employee termination).

m. If an user leaving the organization is a privileged user, system passwords shall be changed on his/her last working day.

n. Password expiration warnings shall be provided at least 15 day(s) prior to the password expiration.

o. The password should contain,

   a. Minimum of 8 character(s).

   b. At least 1 special character

   c. (!, @, #, $, %, ^, &, *, (,), _, -, +, =, |, \, <, >, , , ., ?, /, ;, :, ‘, “, [, {, },])

   d. At least one number (0 to 9)

   e. At least one capital letter (A to Z)

   f. At least one small letter (a to z)

Please note: As far as possible above password policy shall be implemented. In case application/product/OS/DB doesn’t support the above policy, then the supported password policy by application/product/OS/DB will be implemented.

19.4 Roles, responsibilities, and authorities

RACI Chart

Activities	End User	SYS Admin	SDM IT	IT Head
Password Policy change	I	C	A	C
Password implementation	I	R	A	I
Policy Awareness	R	I	A	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

20 Patch Management Policy

20.1 Objectives

SUDARSHAN's computers must be properly patched with the latest appropriate updates in order to reduce system vulnerability and to enhance and repair application functionality. The purpose of this policy is to establish standard procedures for the identification of vulnerabilities, potential areas of functionality enhancements as well as the safe and timely installation of patches.

20.2 Applicability

This policy applies to all software, servers, Cloud Servers, desktops, and laptop computers & Networking Devices owned and operated by SUDARSHAN

20.3 Policy

a. Vulnerability assessment and system patching will only be performed by System Administration Team

b. All server, desktop, and laptop systems, including all hardware and software components, must be accurately listed in the IT Department asset inventory to aid in patching efforts.

c. Vulnerability scanning of systems will take place at least once in a year. SUDARSHAN Shall use the organization authorized tools to scan its systems for security vulnerabilities: SUDARSHAN's systems will be scanned for vulnerabilities with the following frequency:

    a. Servers will be scanned once in a year.

    b. Desktops will be scanned once in a year.

    c. Laptops will be scanned once in a year.

d. The following information sources will be taken as primary authorities on existing and new system vulnerabilities. These sources must be monitored by assigned System Administration Team on an ongoing basis.

    a. Open Source Tools available in Public Domain

e. Each vulnerability alert and patch release must be checked against existing SUDARSHAN's systems and services prior to taking any action in order to avoid unnecessary patching. Read all alerts very carefully – not all patches are related to issues or actual system versions

present at SUDARSHAN

f. The decision to apply a patch, and within what timeframe, must be done following the guidelines presented in the Patch Priority Matrix.

g. All patches must be downloaded from the relevant system vendor or other trusted sources. Each patch's source must be authenticated, and the integrity of the patch verified. All patches must be submitted to an anti-virus scan upon download.

h. New servers and desktops must be fully patched before coming online in order to limit the introduction of risk.

i. New software must be fully patched when installed on SUDARSHAN's resources to limit the introduction of risk.

j. All patches must be tested prior to full implementation since patches may have unforeseen side effects. Describe testing procedure using either a dedicated test network or non-critical machines.

k. A back out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in the event that the patch has unforeseen effects.

l. Patches will be applied according to the following schedule: Describe patching schedule such that it provides minimal disruption to business activities.

m. Rollout of tested patches will adhere to the following procedure: Describe tiered rollout procedure, including all automated systems used.

n. All configuration and inventory documentation must be immediately updated in order to reflect applied patches. This includes the following documents: List the documents that must be regularly updated to reflect patch installations.

o. Audits will be performed yearly to ensure that patches have been applied as required and are functioning as expected.

20.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	SDM IT	USER	IT Head
WSUS Server Installation, configuration n maintenance	R	A	I	C
Patch Authorization	R	A	I	C
Patch Removal	R	A	I	C
Firm ware Updation	R	A	--	C

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

Patch Priority Matrix

Patch	Critical	Security
OS	Immediate	Quarterly
Applications	Immediate	

Note: Critical = Immediate, **Security** = Immediate

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

21 Remote Access Policy

21.1 Objectives

Mobile Computing, Teleworking, and Remote Access policies shall be put in place to ensure information security when using mobile computing and teleworking facilities.

21.2 Applicability

The Policy applies to all organizational employees of SUDARSHAN, contractors, vendors, and any other person using or accessing Organizational information or information systems. Exceptions to this policy must be approved by the SDM IT.

21.3 Policy

21.3.1 Mobile Computing, Teleworking, and Remote Access

Mobile Computing, Teleworking, and Remote Access policies shall be put in place to ensure information security when using mobile computing and teleworking facilities.

21.3.2 Mobile Computing and Communications - Remote Access

A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

21.3.3 Remote Access to SUDARSHAN Email

As a Communications and Operations Security Policy, necessary controls shall be in place

21.3.4 Allowed Technologies for Remote Access Capabilities

Allowed Remote Access Technologies

a. Tunneling based VPN (allowed only for SUDARSHAN devices)
b. SUDARSHAN-approved wireless email devices (Smartphones, etc.)
c. True SSL VPN that checks for malware and antivirus on the source machine

Technology Implementation Requirements for Remote Access

a. Multi-factor authentication
b. Split tunneling is not allowed when connected to the SUDARSHAN network
c. Remote access connections must have a 30-minute inactivity timeout
d. VPN sessions must be re-authenticated every 8 hours
e. Multiple VPN sessions are not permitted

IT & Cyber Security Policy

System Requirements

Only corporate-approved security products and services must be used to connect and authenticate to SUDARSHAN networks.

21.4 Roles, responsibilities and authorities

RACI Chart

Activities	CIO	SDM IT/IT Head	Sys Admin	Employee
Policy enforce / Change	C	A	R	I
Adhere to policy	R	A	R	R
Monitor & Review controls	A	R	R	I
Configuration Security	C	A	R	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	11 February 2019

22 Software Installation Policy

22.1 Objectives

The purpose of this policy is to outline the requirements around installation software on

SUDARSHAN's computing devices to minimize the risk of loss of program functionality, the exposureof sensitive information contained within SUDARSHAN's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

22.2 Applicability

This policy applies to all SUDARSHAN employees, contractors, vendors and agents with an SUDARSHAN owned devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within SUDARSHAN

22.3 Policy

a. Employees shall not install software on SUDARSHAN's computing devices operated within the SUDARSHAN's network without prior approval.

b. Software requests must first be approved by the Team Leader/System Administrator and then be made to the Information Technology department or Help Desk in writing or via email.

c. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need

d. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation/removal depending on the result.

22.4 Roles, responsibilities and authorities

RACI Chart

Activities	IT Head	System Admin	SDM IT	Team Leader
Software Installation	I	R	A	C
Software Removal	I	R	A	C
Software Testing	--	R	A	C
Periodical review of system	I	R	A	C

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

23 Third Party Service Delivery Policy

23.1 Objectives

The purpose of this policy is to maintain appropriate service delivery in line with third party service delivery agreements

23.2 Applicability

The Policy applies to all third-party contractors using or accessing company's information or information systems. Exceptions to this policy must be approved by SDM IT

23.3 Policy

All third-party contractors, using or accessing company's information assets shall comply with this policy.

Following are third-party contractors, such as:

1. Outsourced support services
2. Hardware and software maintenance vendors
3. Other short-term engagement with vendors

a. Scope of the services shall be included in the contract with third party service providers

b. Access to third-party contractors, to company's information or information systems shall be provided to the extent of service coverage

c. Third parties who require access to the Company's infrastructure/ information assets are bound by a contract that defines Company's security requirements. Prior to being granted any access, they are required to sign a non-disclosure agreement.

d. The services provided by third party contractors shall be supervised regularly

   a. Any change at third-party contractors end, with regards to security, infrastructure, etc. shall require approval to be obtained from SDM IT. If required, re-assessment of the risk shall be done considering the criticality of the services.

23.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	IT Head	Employee
3rd Party Contractors NDA/Contract signing	C	R/A	I
3rd Party Contractor Service Enablement	R/A	C	I
3rd Party Contractor Service Monitoring	R	R/A	I

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform

SUDARSHAN

Document No.	Issue No.	Effective Date
SCIL/IT Policy/3.0	3.0	06 October 2022

24 Anti-Virus Policy

24.1 Objective

The intent of this policy is to better protect SUDARSHAN's assets against attack from destructive or malicious programs.

24.2 Applicability

The Policy applies to all SUDARSHAN's employees, contractors, vendors, and any other person using or accessing Organizational information or information systems. Exceptions to this policy must be approved by the SDM IT.

24.3 Policy

a. All SUDARSHAN's systems shall be protected by a standard Anti-virus software.

b. Virus protection engines and/or versions shall be updated as and when they are released.

c. Upon release of upgrades/update, all computer systems get updated automatically.

d. Anti-virus software shall scan all files introduced into its environment for virus, hostile, and malicious code before they are used.

e. All Internet file transfer shall be scanned for virus, hostile, and malicious code.

f. System users shall not execute programs of unknown origin because they may contain malicious logic.

g. Only licensed and approved software shall be used on company's computing resources.

h. All external storage media introduced to SUDARSHAN's environment, such as removable disks and CD-ROM, shall be scanned for potential threats.

i. The unauthorized development, transfer, or execution of virus, hostile, and malicious code is prohibited.

j. All users shall report any suspicious occurrences to their Business Technology immediately.

24.4 Roles, responsibilities and authorities

RACI Chart

Activities	Sys Admin	IT Head	SDM IT	Employee
Antivirus/Antimalware installation and updation	R	C	A	I
Response to reported malware/ suspicious Activity	R	C	A	R

Note: R = Responsible, **A** = Accountable, **C** = Consult, **I** = Inform