SUDARSHAN

Information Security Policy

Version No: 1.0
Effective Date: 18/10/2024

Contents

1 Document Control

Version No.	Effective Date	Created By	Approved By	Reason of Change
1	18th Oct 2024	Mr. Manish Pawar	MRC (Management Review Committee)	Initial Document

2 Introduction

Sudarshan Chemical Industries Ltd. (hereafter referred to as Sudarshan) shall implement adequate security policies, procedures, and controls to protect confidentiality, maintain integrity, and ensure the availability of all information stored, processed, and transmitted through its information systems. This includes electronic data, physical records, intellectual property, customer and employee information, and other business-critical assets.

Sudarshan recognizes the critical importance of safeguarding its information assets to ensure the confidentiality, integrity, and availability of information throughout Sudarshan. As such, the Information Security Policy serves as the foundational document outlining Sudarshan's commitment to protecting its information assets.

The Information Security Policy establishes a comprehensive framework for managing information security within Sudarshan, encompassing all aspects of information handling, storage, processing, and transmission. All employees, contractors, sub-contractors, and vendors are expected to adhere to this policy and associated procedures in order to maintain a secure information environment.

3 Purpose

The purpose of the Information Security Policy is to:

- Communicate management's commitment to information security and its importance to Sudarshan’s overall mission and objectives.
- Provide a framework for establishing, implementing, maintaining, and continually improving the Information Security Management System (ISMS) in alignment with ISO 27001:2022 standard.
- Ensure the protection of information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

- Ensure compliance with relevant legal, regulatory, and contractual obligations related to information security. Promote a culture of security awareness among all employees, contractors, and stakeholders involved in handling Sudarshan's information assets.
- Implement controls and monitor measures for all hardware and software assets used throughout Sudarshan.
- Protect critical information from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional. Ensure the confidentiality, integrity, and availability of information whether permanently acquired, in transit, provided, or created.
- Protect Sudarshan's information, and assets from threats that could potentially disrupt business and damage Sudarshan's brand and reputation.
- Ensure that all business heads/department heads are directly responsible for compliance within their respective business departments.
- Ensure that all breaches of information security, actual or suspected, are reported, investigated by designated personnel, and appropriate corrective and preventive actions are initiated.

4 Scope

This Information Security Policy applies to:

- All stakeholders who access Sudarshan's information or networks, including full-time employees, off-roll employees (including subsidiary staff), contractors, consultants, temporary staff affiliated with third parties, system vendors, and staff from outsourcing companies.
- All information assets owned, controlled, or processed by Sudarshan, regardless of their form or medium, including but not limited to:
  - Electronic data and information systems
  - Physical records and documents
  - Intellectual property
  - Customer and employee information
  - Business processes and procedures
  - Voice and data communications
- All locations where Sudarshan conducts its business activities include offices, manufacturing facilities, remote sites, and mobile workplaces.
- All systems and networks used in processing, storing, and transmitting information, whether managed internally or by third-party service providers.

- All information assets (physical, informational, paper, people, services, site, and software) and underlying IT technologies and services (storage, backup, server hosting services, application services, etc.).
- All external/third-party companies/personnel (vendors, third-party resources, consultants, interns/trainees, contractors employed with Sudarshan, and clients/customers visiting Sudarshan’s office) who engage in work and have access to Sudarshan’s information or information processing facilities.

5 Information Security Policies

Information is an asset like other important business assets, holds significant value to Sudarshan and consequently requires protection from unauthorized use while being accessible to authorized personnel as needed. Sudarshan recognizes its information assets as a critical and valuable resource.

This Information Security Policy provides management direction and support to ensure the protection of Sudarshan's information assets and to facilitate access, use, and disclosure of such information by appropriate standards and laws. The Information Security Policy essentially describes the Annex A controls of the ISO 27001:2022 Standard, ensuring alignment with international best practices.

Information Security Objectives:

a. Develop and maintain an effective Information Security Management System (ISMS) consisting of an information security policy, supporting procedures, standards, guidelines, and a risk assessment procedure.
b. Identify all assets that directly or indirectly impact business operations and understand their vulnerabilities and threats through appropriate risk assessments.
c. Comply with applicable laws and contractual obligations related to information security and data privacy.
d. Raise awareness of information security risks within Sudarshan and foster a security-conscious culture, ensuring that all breaches of information security and suspected weaknesses are reported, investigated, and adequate actions are taken.

Policy Framework:

The Information Security Policy is supported by detailed Information Security Procedures and guidelines. These procedures are derived from business requirements and ensure effective implementation of the policy.

Policy Owner:

The ownership of the Information Security Policy lies with the MRC (Management Review Committee) (MRC). Any changes or updates to this document shall be made by the MRC based upon the recommendations from the Head of Business Technology or as deemed necessary by the MRC to meet changing business needs. These changes shall be incorporated into the document, and the details about the revision number, issue date, effective date, and associated changes shall be updated accordingly.

Policy Distribution:

The Information Security Policy shall be accessible to all employees of Sudarshan. All employees are required to read the policy, understand their responsibilities, confirm acceptance, and ensure information security within Sudarshan.

This policy is an internal document and shall be made available only to Directors, employees of Sudarshan, and business partners who have signed a Non-Disclosure Agreement (NDA). The Information Security Policy may be made available to external auditors, consultants, and regulatory bodies after signing confidentiality and non-disclosure agreements.

Policy Review and Approval:

The Information Security Policy shall be reviewed annually and as needed to address changes in information assets, organizational structures, technological advancements, legal requirements, or other relevant factors. The revision number indicates the number of times the document has been modified. The policy shall be reviewed and approved by the MRC, and all changes shall be communicated to all employees and third-party personnel through appropriate forums and channels.

Compliance:

All employees, stakeholders, and third-party vendors, contractors, interns, trainees, and consultants having access to Sudarshan's information and supporting processes of information processing facilities shall comply with the Information Security Policy. Any violation or attempted violation shall result in disciplinary action by the MRC in consultation with Human Resources, consistent with the severity of the incident.

Any violation of the Information Security Policy shall be reported to BTG & CISO keeping respective heads in loop.as per the below reporting matrix.

Name	Email-id	Role	Contact details
BTG	securityforum@sudarshan.com	Team	NA
Manish Pawar	mspawar@sudarshan.com	CISO	7350017227

Exceptions:

Approval for exceptions or deviations from the policy shall be granted only after an appropriate risk assessment by the CISO. Exceptions are not universal but approved on a case-by-case basis upon official request.

All exceptions during implementation shall be submitted by the CISO to the MRC. Ad-hoc exceptions required by a user shall be formally requested and approved by the User Department Head.

Management Direction for Information Security:

The management, including CISO, and MRC (Management Review Committee), is accountable for implementing the Information Security Policy. Location/department heads, along with the MRC (Management Review Committee), are responsible for managing overall information security within Sudarshan.

All employees shall read, understand, and adhere to the Information Security Policy.

The Information Security Policy should be reviewed at least annually or when significant changes occur that impact policies and procedures. This review assesses the impact of changes in information assets, deployed technology architecture, legal requirements, and the emerging threat landscape.

6 Information Security Governance

6.1 Policies for Information Security

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.1

Purpose

The purpose of this policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Policy

Sudarshan shall establish and maintain an information security policy that:

- Is approved by MRC (Management Review Committee) and communicated to all employees and relevant external parties.
- Aligns with organizational objectives, business needs, and applicable legal and regulatory requirements.
- Is reviewed at least annually or upon significant changes to ensure continued suitability and effectiveness.

Procedures

- The Information Security Policy shall be documented and made accessible to all employees and relevant external parties.
- Management shall ensure that the policy is communicated and understood throughout Sudarshan.
- The policy shall be reviewed and updated as necessary by the MRC (Management Review Committee), which includes the CISO and the Executive Management.

6.2 Information Security Roles & Responsibilities

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.2

Purpose

The purpose of this is to define and allocate information security responsibilities to ensure proper management of information security within Sudarshan.

Policy

Sudarshan shall define and allocate information security roles and responsibilities, ensuring they are clearly communicated and understood throughout Sudarshan.

- The MRC (Management Review Committee) shall be responsible for overseeing the development, implementation, and maintenance of the information security program.
- Specific roles and responsibilities for information security shall be defined and documented, including but not limited to:
  - **MRC:** Overall responsibility for monitoring, reviewing and approving the Information Security Program
  - **CISO**: Overall responsibility for the information security strategy and program.
  - **Business Technology Group**: Implementing and managing technical security controls.
  - **HR Team**: Ensuring personnel-related security measures are in place.
  - **Admin Team**: Ensuring physical-related security measures are in place.
  - **All Employees**: Adhering to information security policies and procedures.

- Roles and responsibilities shall be reviewed and updated as necessary to reflect changes in Sudarshan or its operations.

6.3 Segregation of Duties

This section covers compliance with the following ISO Standards Clause & Control requirements:

ISO 27001:2022 - Control No. 5.3

Purpose

The purpose of this is to reduce the risk of unauthorized or unintentional modification or misuse of Sudarshan's assets.

Policy

- Sudarshan shall implement segregation of duties to ensure that no single individual has the capability to execute all critical aspects of a process.
- Critical tasks and processes shall be identified and analyzed for potential conflicts of interest.
- Duties and responsibilities shall be divided among different individuals to ensure that no single individual has control over all aspects of any critical process.

- Access controls and monitoring mechanisms shall be implemented to enforce segregation of duties.
- The segregation of duties shall be reviewed periodically and adjusted as necessary to address changes in Sudarshan structure or processes.

6.4 Management Responsibilities

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.4

Purpose

The purpose of this is to ensure that management supports information security through clear direction, demonstrated commitment, and visible support.

Policy

Management at Sudarshan shall provide clear direction and visible support for information security initiatives, ensuring that sufficient resources and support are allocated to maintain Sudarshan's information security posture.

- Management shall demonstrate commitment to information security by endorsing policies, allocating resources, and supporting security initiatives.
- Information security objectives and expectations shall be clearly communicated to all employees.
- Management shall ensure that information security responsibilities are included in job descriptions and performance evaluations.
- Regular CISO / MRC meetings shall be held to review information security performance and address any issues or concerns.

6.5 Contact with Authorities

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.5

Purpose

The purpose of this is to ensure appropriate and timely contact with relevant authorities in the event of security incidents or other significant events.

Policy

Sudarshan has established and maintained contact with relevant authorities to ensure timely and appropriate responses to security incidents and compliance with legal and regulatory requirements.

A list of relevant authorities and contact information are maintained.

- Procedures are established for reporting security incidents to relevant authorities as required.
- The CISO is responsible for managing relationships with authorities and ensuring timely communication in the event of a security incident.
- Records of all communications with authorities are maintained and reviewed as part of the incident management process.

6.6 Contact with Special Interest Groups

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.6

Purpose

The purpose of this is to ensure that Sudarshan is aware of and complies with relevant information security developments, threats, and regulatory requirements.

Policy

Sudarshan is maintaining contact with special interest groups, industry associations, and other relevant organizations to stay informed about information security trends, threats, and best practices.

- The CISO has to identify and establish relationships with relevant special interest groups, industry associations, and other organizations.
- Regular participation in meetings, conferences, and other events organized by these groups are encouraged.
- Information gathered from these groups shall be communicated to relevant stakeholders within Sudarshan.
- Participation in special interest groups is to be reviewed periodically to ensure continued relevance and value.

6.7 Threat Intelligence

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.7

Purpose

The purpose of this Threat Intelligence Policy is to establish an effective framework for the collection, analysis, and dissemination of threat intelligence information to ensure the protection of Sudarshan against cyber threats and vulnerabilities. This also defines the steps for the effective collection, analysis, and dissemination of threat intelligence to protect Sudarshan's assets and operations.

Scope

This policy applies to all employees, contractors, and third-party service providers involved in the information security operations of Sudarshan. It covers all threat intelligence activities, including data collection, analysis, and response.

Responsibility

- **Chief Information Security Officer (CISO)**: Overall responsibility for threat intelligence program.
- **Business Technology Group**: Responsible for gathering, analyzing, and disseminating threat intelligence, along with implementing and responding to threat intelligence information.

Policy

Sudarshan recognizes the importance of threat intelligence in maintaining a robust security posture. To this end, the following principles shall guide the threat intelligence program:

- Threat intelligence shall be gathered from multiple sources, including Sentinel One Managed Services, industry reports, government advisories, threat-sharing communities, and internal monitoring tools.
- Collected threat intelligence shall be analyzed to identify potential threats, vulnerabilities, and trends.
- Information related to Threat Intelligence shall be collected from following Sources:
    - Sentinel One Managed Services
    - Industry reports and publications
    - Government advisories and alerts
    - Threat-sharing communities and forums
    - Internal monitoring tools and systems

- This policy shall be reviewed annually and updated as necessary to reflect changes in the threat landscape and organizational needs. All threat intelligence activities, including collection, analysis, and dissemination, shall be documented.
- Regular reports shall be generated and shared with relevant stakeholders.

Procedure

- **Threat Intelligence Collection**

Activity	Responsibility
Establish a threat intelligence team	Business Technology Group
Identify and subscribe to relevant threat intelligence sources (E.g., Sentinel One Managed Services, industry reports, government advisories)	Business Technology Group
Integrate automated feeds from threat intelligence sources into monitoring systems	Business Technology Group

- **Threat Intelligence Analysis**

Activity	Responsibility
Analyze collected threat intelligence to identify potential threats and vulnerabilities	Business Technology Group
Prioritize threats based on potential impact and likelihood	Business Technology Group
Document findings in threat intelligence reports	Business Technology Group

- **Threat Intelligence Dissemination**

Activity	Responsibility
Share relevant threat intelligence with management, IT, and security teams	Business Technology Group
Provide regular threat intelligence updates and reports	Business Technology Group

Use dashboards and email alerts to disseminate critical threat information	Business Technology Group

- **Threat Response**

Activity	Responsibility
Develop and maintain incident response playbooks	Business Technology Group
Conduct regular drills and simulations to test response procedures	Business Technology Group
Implement response actions based on threat intelligence (e.g., patching, reconfiguration)	Business Technology Group

- **Integration with Sentinel One**

Activity	Responsibility
Configure and monitor Sentinel One's automated threat detection and response features	Business Technology Group
Regularly review Sentinel One threat intelligence feeds and alerts	Business Technology Group

- **Collaboration with External Entities**

Activity	Responsibility
Participate in threat-sharing communities and special interest groups	Business Technology Group
Maintain regular contact with industry peers, government authorities, and managed service providers (e.g., Sentinel One)	Business Technology Group

- **Periodic Review & Update**

Activity	Responsibility
Conduct periodic reviews of the threat intelligence program	Business Technology Group

Update procedures based on changes in the threat landscape and lessons learned	Business Technology Group
Incorporate feedback from drills, simulations, and real incidents	Business Technology Group

6.8 Information Security in Project Management

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.8

Purpose

The purpose of this document is to establish a comprehensive framework for integrating information security into project management activities at Sudarshan. This ensures that all projects are managed with due consideration to the security of information assets, compliance with security standards, and effective risk management throughout the project lifecycle.

Scope

This policy and procedure apply to all employees, contractors, and third-party service providers involved in project management activities. It covers all projects, regardless of size or complexity, and includes all stages of the project lifecycle from initiation to closure.

Responsibility

- **Chief Information Security Officer (CISO)**: Has overall responsibility for ensuring the integration of information security in project management.
- **Project Managers**: Are responsible for incorporating information security requirements into project plans and ensuring compliance throughout the project lifecycle.
- **Business Technology Group**: Provides guidance and support to project teams on information security matters.

Policy

- Information security considerations shall be integrated into the project management framework from the initiation phase through to project closure.

- Risk assessments shall be conducted for all projects to identify potential threats and vulnerabilities and to determine appropriate controls.
- Information assets involved in projects shall be classified according to Sudarshan's Data classification scheme.
- Appropriate security controls should be implemented and maintained throughout the project lifecycle.
- Project teams shall receive adequate training and awareness on information security principles and practices.
- Information security in projects shall be reviewed and monitored regularly to ensure compliance and effectiveness.
- All information security activities within projects shall be documented, and regular reports shall be generated and shared with relevant stakeholders.
- This policy shall be reviewed annually and updated as necessary to reflect changes in the project management framework and information security requirements.

Procedure

- **Project Initiation**

Activity	Responsibility
Identify and classify information assets involved in the project	Project Manager
Conduct a preliminary risk assessment to identify potential security threats	Project Manager with Business Technology Group
Define information security requirements and include them in the project plan	Project Manager

- **Project Planning**

Activity	Responsibility
Develop a detailed risk assessment and identify appropriate security controls	Project Manager with Business Technology Group
Incorporate security controls into the project plan and schedule	Project Manager

Assign roles and responsibilities for implementing security controls	Project Manager

- **Project Execution**

Activity	Responsibility
Implement security controls as defined in the project plan	Project Team
Monitor and manage risks throughout the project lifecycle	Project Manager with Business Technology Group

- **Project Monitoring and Control**

Activity	Responsibility
Regularly review and update risk assessments	Project Manager with Business Technology Group
Monitor compliance with information security requirements	Business Technology Group

- **Project Closure**

Activity	Responsibility
Conduct a final risk assessment and review security controls	Project Manager with Business Technology Group
Document lessons learned and best practices for information security in projects	Project Manager
Ensure all information assets are securely archived or disposed of according to Sudarshan's data retention policy	Project Manager

- **Review and Monitoring**

Activity	Responsibility

Conduct regular reviews of the information security in project management policy and procedures	Business Technology Group
Monitor the effectiveness of information security controls in projects	Business Technology Group
Update policies and procedures based on lessons learned and changes in the threat landscape	Business Technology Group

7 ASSET MANAGEMENT

7.1 Asset Management Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.9, 5.11, 5.12, 5.13

Purpose

The purpose of this document is to establish a framework for the effective management and protection of all assets owned and managed by Sudarshan. This includes implementing suitable controls to safeguard information security assets, ensuring compliance with legal and regulatory requirements, and supporting Sudarshan's business objectives.

Scope

This policy applies to all assets owned and managed by Sudarshan, including physical assets, information assets, IT, software, and services. It is applicable to all users, including employees, contractors, third-party service providers, and any other individuals who have access to Sudarshan’s assets. It also covers all computers, network, voice, and data communication systems owned by and/or administered by Sudarshan.

Responsibility

- **Chief Information Security Officer (CISO)**: Oversees the implementation of the asset management policy and procedures, ensuring compliance with security standards and regulatory requirements.
- **Business Technology Group**: Manages the asset register, coordinates asset allocation and deallocation, and ensures the security of IT assets.

- **Admin Team**: Responsible for the physical security of assets, tracking asset movement, and managing asset procurement and disposal.
- **HR Team**: Coordinates the allocation and deallocation of assets for new hires and departing employees.
- **Asset Owners**: Responsible for the security and management of assigned assets, including ensuring proper use and reporting any changes or incidents.
- **Users**: Ensure the proper use and protection of assigned assets and report any issues or changes promptly.

Policy

- All information security assets shall be formally defined, identified, classified, and baselined.
- Assets include information, software assets, physical assets, services, people, and intangibles.
- An IT asset register shall be developed and maintained, updated to reflect any changes in asset status.
- All IT assets associated with information processing facilities, systems, or services shall have a designated owner responsible for their management.
- Exception: Common assets that are mapped with the respective department heads.
- Asset Tagging and Labeling shall be allocated to the following teams:
    - **IT Assets**: Labelled with an asset code by the BTG Team.
- Asset management procedures are implemented to secure and support business requirements, considering storage, classification, secure disposal, and record-keeping as per the above-mentioned procedure.
- Only approved software and products shall be installed within Sudarshan. Additions to the approved list require approval from the Head of BTG and the CISO.
- The asset management policy and procedures should be reviewed and updated annually to ensure continued relevance and effectiveness.

Procedure

- **Information Classification**

Activity	Responsibility
Identify and classify information based on sensitivity and business importance: • **Restricted**: Sensitive and business-critical information; unauthorized access could cause significant financial loss or customer dissatisfaction. Examples include top management	All Employees

strategic documents, company-developed software code, and passwords. • **Confidential**: Business-sensitive information or personally identifiable information (PII) intended for specific groups. Examples include salaries, personnel data, and financial reports. • **Internal**: Information approved for internal circulation and approved third-party vendors. Examples include training materials, policies, procedures, and records. • **Public**: Non-confidential information that can be made public. Examples include brochures and product information.	

- **Information Labelling**

Activity	Responsibility
Label information clearly as per the classification when acquired or created. Documents must be labeled in the footer for Word files.	All Employees
Store information in cloud storage based on classification and sensitivity: • **Restricted**: Store in a designated shared folder with strictly restricted access. • **Confidential**: Store in a shared folder with permission on a need-to-know basis. • **Internal**: Store in a shared folder accessible by anyone within Sudarshan. • **Public**: Public information may be disclosed on the Internet or in brochures only by designated personnel and with approvals.	All Employees
Dispose of information according to classification: • **Restricted**: Destruction requires approval from the CISO/Admin Team. • **Confidential**: Destruction requires approval from the information owner and CISO/Admin Team. • **Internal/Public**: Destruction requires approval from the information owner. Hard copies should be shredded, and soft copies should be deleted securely.	All Employees
Consider unlabeled information as "Internal" and do not share it externally without an NDA.	All Employees

- **Asset Classification & Grouping**

Activity	Responsibility
Classify and group assets into the following categories: • **Paper Documents**: Hard copy documents. • **Digital Information**: Soft copy documents such as files and folders. • **IT Hardware**: Computer equipment, servers, workstations, network devices, media, virtual machines, and cloud environments. • **Non-IT Hardware**: Hardware such as keys, locks, ID cards, biometrics, etc. • **Services**: Operational services offered to customers. • **Software**: Applications and tools used by Sudarshan.	Asset Owner

- **Asset Register**

Activity	Responsibility
Maintain an asset register.	BTG
Update the asset register with any additions, deletions, or modifications: • New assets commissioned. • Assets decommissioned or replaced.	BTG
Track changes to the asset register and maintain version and revision history.	BTG
Reconcile the asset register at least annually.	BTG

- **Asset Tracking**

Activity	Responsibility
Track all IT assets allocated to users, such as laptops and Desktop.	BTG
Update system records for any changes in asset allocation or reallocation.	BTG
Ensure users are responsible for their assigned assets and protect them.	Users
Verify the condition of returned/replaced assets, report damages to HR for recovery of charges.	HR / Business Technology Group

- **Asset Management**

Activity	Responsibility
Protect all assets, including media devices, from unauthorized access by securing them in appropriate locations.	Users / Asset Owner
Store media in locked cabinets placed in controlled access locations.	Users / Asset Owner
Track all assets entering or leaving the premises using an inward/outward register maintained at the reception.	Users / Asset Owner

- **Secure Disposal of Asset**

Activity	Responsibility
Dispose of various types of media using the following methods: • **Printed Material**: Dispose of by shredding. • **Hard Disk**: Format the hard disk of PCs or laptops before disposal. Physically destroy damaged hard disks and remove magnetic media. • **IT Asset Hardware**: Dispose of as E-Waste.	Asset Owner

- **Asset Allocation**

Activity	Responsibility
HR informs the BTG of new joiners for the week.	HR Team
BTG prepares assets based on HR details, ensuring systems meet the hardening guide.	BTG
Create and configure user IDs and email IDs on the day the user joins.	BTG

- **Asset De-Allocation**

Activity	Responsibility
HR informs IT of employee departures for the week.	HR Team
Departing employees obtain clearance from all departments using the clearance checklist.	User
BTG verify access on different systems and disables accounts on the last working day.	BTG
BTG backs up user data to cloud storage and deletes accounts. The physical system remains until reassigned.	BTG

- **Movement of IT Assets Outside Premises**

Activity	Responsibility
Systems sent to vendors require a gate pass and must be tracked via register.	BTG

- **Asset Procurement**

Activity	Responsibility
Users request assets based on job needs, with approval from their reporting manager.	User / Reporting Manager
BTG reviews and approves requests.	BTG
CISO reviews requests for high-priced items, with BTG Head approval.	BTG Head/ CISO
Raise a purchase order (PO) based on approval and share with the vendor.	BTG
Vendor sends material, which is verified against the PO; invoices are sent to Accounts for payment.	BTG

7.2 Data Classification Policy

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Clause 7.5, Control 5.12, 5.13, 5.14

Purpose

The purpose of this Data Classification Policy is to establish a consistent approach to classifying data based on its level of sensitivity, value, and criticality to Sudarshan. This classification will assist in applying the appropriate security controls and managing risks associated with data handling.

Scope

This policy applies to all data generated, collected, or maintained by Sudarshan. It encompasses electronic, physical, and verbal data, as well as any form of communication, whether stored on premises or in the cloud.

Data Classification Levels

Data shall be classified into the following four levels based on sensitivity:

1. Public Data

- Description: Data that is intended for public disclosure. Its unauthorized disclosure, alteration, or destruction poses little to no risk to Sudarshan.
- Examples: Press releases, marketing materials, public web content.

- Handling Requirements: No restrictions. Public data can be freely shared internally and externally.

2. Internal Data

- Description: Data intended for use within Sudarshan. Unauthorized access may cause minor inconvenience but poses minimal risk.
- Examples: Internal memos, employee directories, operational procedures.
- Handling Requirements: Share only with authorized employees and partners. Do not disclose externally without permission.

3. Confidential Data

- Description: Data that is sensitive in nature. Unauthorized disclosure could have a significant negative impact on Sudarshan's operations, reputation, or compliance.
- Examples: Financial data, customer information, internal strategy documents.
- Handling Requirements: Limit access to authorized personnel only. Strong access controls are required for storage and transmission.

4. Restricted Data

- Description: Highly sensitive data that, if disclosed, could lead to severe consequences for Sudarshan, including legal liability, severe reputational damage, or major operational disruptions.
- Examples: Trade secrets, personal identifiable information (PII), intellectual property, cybersecurity incident reports.
- Handling Requirements: Access is strictly limited on a need-to-know basis.

Roles and Responsibilities

- Data Owners: Responsible for the classification of data they generate or control and ensuring appropriate security measures are applied.
- BTG Group: Implements technical controls for data protection and assistance in the enforcement of the Data Classification Policy.
- Employees and Contractors: Adhere to the data handling requirements specified by the classification level and report any incidents or breaches promptly.

Data Labeling and Marking

Each data type should be clearly labeled with its classification level.

Data Protection and Security Measures

Depending on the classification level, appropriate security measures, such as access control, and data loss prevention tools, will be applied to protect Sudarshan's data.

Training and Awareness

All employees will receive training on this Data Classification Policy and will be required to comply with its terms. Regular updates will be provided to reinforce the best practices for data handling.

Compliance and Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment. Sudarshan reserves the right to audit and monitor compliance with this policy.

8 ACCEPTABLE USE OF INFORMATION & ASSOCIATED ASSETS

Acceptable Usage Policy

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.10

Purpose

The purpose of this policy is to:

- Outline the acceptable use of information and information processing assets.
- Protect the information and information processing assets of Sudarshan and its customers.
- Prevent exposure to risks including virus attacks, compromise of network systems, services, and legal issues.

Scope

This Acceptable Use Policy applies to all employees, contractors, vendors, and external parties of Sudarshan. It covers all information and information processing assets owned or leased by Sudarshan.

Responsibility

- **Chief Information Security Officer (CISO)**: Shall approve, review, and update the Acceptable Use Policy. The CISO is accountable for ensuring the policy aligns with Sudarshan's goals and legal requirements.

- **Employees and External Parties**: Shall understand and adhere to the guidelines outlined in this policy. Employees and external parties are accountable for their actions and compliance.
- **Business Technology Group**: Shall enforce technical aspects of the policy, including monitoring network traffic and ensuring compliance with security measures.
- **HR Department**: Shall incorporate the Acceptable Use Policy into employee onboarding and training programs.
- **Management**: Shall set a tone of compliance with the policy and provide support to ensure its effective implementation. Management is accountable for promoting a culture of security awareness and accountability among employees.

Policy

- **General Policy:**
  - All employees, contractors, vendors, and anyone using or accessing Sudarshan's information assets shall comply with this policy. Violators are subject to disciplinary action.
  - All information assets and systems within Sudarshan are property of Sudarshan and shall be used in compliance with Sudarshan's policy statements.
  - Any information placed on Sudarshan's information system resources and cloud resources shall be property of Sudarshan.
  - Copyright and licensing agreements shall not be violated.
  - Any attempt to circumvent Sudarshan's security procedures shall be strictly prohibited.
  - Unauthorized use, destruction, modification, and/or distribution of Sudarshan's information assets or information systems shall be prohibited.
  - All employees shall acknowledge understanding and acceptance by signing the appointment letter/client-specific NDA prior to using Sudarshan's Information Assets and Information Systems.
  - 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.
  - All users shall report any suspicious activity about Information Assets to the BTG Head/ CISO immediately.
  - Sudarshan's Information Systems and Information shall be subject to monitoring at all times.
  - All policy statements shall be reviewed annually and updated as required.
  - Sudarshan shall cooperate with law enforcement authorities regarding information security and related incidents.

- Sudarshan shall protect the data and privacy of personal information.
- 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.
- Release of information shall be in accordance with Sudarshan's policy statement.
- Users shall not attach their own or any third-party computer or test equipment to Sudarshan's computers or networks without prior approval of the BTG Head.

- **General Use & Ownership:**
  - While Sudarshan desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Sudarshan.
  - Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
  - For security and network maintenance purposes, authorized individuals within Sudarshan may monitor equipment, systems, and network traffic.
  - Users shall only use the information and information processing assets they are entitled to and follow the specified instructions.

    Do's:

    - Use strong passwords and do not share them with anyone.
    - Be careful about what websites you visit and what files you download.
    - Do not open emails or attachments from unknown senders.
    - Report any suspicious activity to the BTG department immediately.
    - Place your critical data on centralized repository and OneDrive.
    - Use the network for authorized purposes only.
    - Respect the privacy of others.
    - Comply with all applicable laws and regulations.

    Don'ts:

    - Use the network for illegal activities, such as downloading pirated software or sharing prohibited content.
    - Spam or send unsolicited emails.
    - Use the network for personal use, such as shopping or browsing social media, during work hours.
    - Share your passwords with anyone.
    - Install unauthorized software on the network.
    - Access or download sensitive data without authorization.
    - Disrupt or disable the network or any of its components.
    - Violate the privacy of others.
    - Engage in any other activity that is prohibited by law or by Sudarshan's policies.

- **Security and Proprietary Information:**
  - The user interface for information contained on the Internet/Intranet/Extranet-related systems shall be classified as either confidential or not confidential. Employees shall take all necessary steps to prevent unauthorized access to this information.
  - Keep passwords secure and do not share authentication information. Authorized users are responsible for the security of their passwords and accounts.
  - All PCs, laptops, and workstations are secured with automatic activation feature set at 10 minutes or less.
  - Employees must use extreme caution when opening email attachments received from unknown senders.
- **Unacceptable Use:**
  - The following activities are prohibited:
    - Engaging in illegal activities under local, state, federal, or international law while using Sudarshan-owned resources.
    - Using personal computers or laptops and associated peripherals within Sudarshan premises without authorization from the department head and CISO.
    - Unauthorized copying of copyrighted material and the installation of any unlicensed software.
    - Introducing malicious programs into the network or server.
    - Revealing account passwords or allowing use of your account by others.
    - Using Sudarshan's computing assets to procure or transmit material that violates sexual harassment or hostile workplace laws.
    - Making fraudulent offers of products, items, or services.
    - Effecting security breaches or disruptions of network communication, including but not limited to network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
    - Port scanning or security scanning unless permitted by and with prior notification to the concerned authority of Sudarshan.
    - Circumventing user authentication or security of any host, network, or account.
    - Using any program/script/command to interfere with or disable a user's terminal session.
    - Providing information about our lists of employees to parties outside Sudarshan.
- **System and Network Activities:**
  - The following activities are strictly prohibited:
    - Violations of intellectual property rights, including installing or distributing pirated or unlicensed software.
    - Unauthorized copying of copyrighted material.

- Introducing malicious programs into the network or server.
- Revealing account passwords or allowing use of your account by others.
- Using Sudarshan's computing assets for unlawful activities.
- Making fraudulent offers of products, items, or services.
- Security breaches or network disruptions.
- Port scanning or security scanning without authorization.
- Circumventing user authentication or security measures.
- Interfering with or disabling a user's terminal session.
- Providing information about our lists of employees to external parties.

- **Email and Communication Activities:**
  - The following activities are strictly prohibited:
    - Sending unsolicited email messages, including "junk mail" or spam.
    - Harassing others via email, telephone, or paging.
    - Forging email header information.
    - Soliciting email for harassment purposes.
    - Creating or forwarding "chain letters."
    - Posting non-business-related messages to large numbers of Usenet newsgroups.

9 ACCESS CONTROL

Access Control Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.14, 5.15, 5.16, 5.17, 5.18

Purpose

The purpose of this document is to govern the appropriate access granting and usage mechanism at Sudarshan and to outline the steps for managing user accounts across various IT systems used within Sudarshan. These steps include creating user accounts, granting specific privileges or equipment, revoking privileges, and disabling/removing user accounts.

Sudarshan recognizes that user access control is crucial for safeguarding information and computing resources from unauthorized access. This policy provides guidance on the development, communication, and implementation of procedures for access control.

Scope

The scope of this policy is bound to the BTG team and their responsibilities pertaining to access management, including user creation and deactivation, privilege access mapping, and revoking rights. 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 BTG Head.

Responsibility

The responsibility of this policy lies with the BTG team.

Policy

The BTG team shall adhere to the following points related to access:

- All sensitive computer-resident information shall be protected via logical access controls to ensure that unauthorized access, disclosure, modification, and deletion of information is prevented.
- Access to Sudarshan's information systems and computing resources shall be based on each user's access privileges. This applies to all employees as well as all contractors, consultants, temporary workers, outsourcing firms, etc.
- Access privileges shall be granted based on specific business needs (i.e., on a "need to know" basis) and default access privileges shall be set to "deny-all" prior to any specific permissions being granted.
- Addition, change, or deletion of access shall be done using a formal approval process.
- For access to all systems, users shall be authenticated using a unique login ID and a secret password assigned to them.
- A list of all access and privilege access given to the users shall be reviewed on a periodic basis.

User Access Management

- **User Registration and De-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:
        - **Unique ID**: Each user shall be uniquely identified when authenticating to any Sudarshan system to ensure users can be accountable for their actions. Generic or multi-user usernames and passwords are prohibited, except as specifically authorized by the BTG Head.

  - **User Registration Process**: A documented process for providing and approving user access to applications, systems, databases, and networks shall be implemented.
  - **User De-Registration/Terminations Process**: A documented termination process, to be administered by Human Resources, shall be established to ensure all application, system, and network access is immediately removed.
  - **Role Changes**: As a user moves into a new role, a process shall exist to revise the user's new access requirements. This process shall be well documented and retained for audit and compliance purposes.

- **Privilege Management**
  - User access privileges shall be based on predefined user roles and follow the principle of the least privilege, which mandates providing minimum access to perform assigned duties and responsibilities. Privileged credentials shall be limited to a small number of trusted employees.
- **Emergency Access**
  - Emergency access must be pre-approved by the BTG Head and reviewed monthly. The process for obtaining emergency access credentials shall include documented justification, specific individual access, and a validity timeframe not exceeding 48 hours.
- **Segregation of Duties**
  - Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Sudarshan's assets.
- **User Password Management**
  - The allocation of passwords shall be controlled through a formal management process. Accounts shall be activated securely, and the account administrator shall not know the password assigned to an account. User credentials shall be communicated through secure channels.
- **Review of User Access Rights**
  - Management shall review user access rights at regular intervals using a formal process. All user accounts inactive for 90 days shall be disabled or deleted after confirmation from HR.
- **Network Access Control**

  Users shall only be provided with access to the services that they have been specifically authorized to use. Web content filtering policies from firewall shall be used to manage the internet traffic of all employees.

Procedure

- **Access Required**

Sr.#	To Access	Role	Type of Access	Approval Needed	How
1	Laptop/Desktop	All Users	General	Functional Head	Email
2	File Server	Business Technology Group	General	BTG Head	Email
3	Production Server	Business Technology Group	Privilege	BTG Head	Email
4	AD Server	Business Technology Group	Privilege	BTG Head/ CISO	Email
5	Cloud Storage	Business Technology Group	Privilege	BTG Head/ CISO	Automated
6	QA/Replica Servers	Business Technology Group	Privilege	BTG Head	Email
7	Monitoring Tool	Business Technology Group	Privilege	BTG Head	Email
8	VPN – Admin	Business Technology Group	Privilege	BTG Head	Email
9	VPN	All Users	General	Functional Head	Email
10	Firewall	Business Technology Group	Privilege	BTG Head	Email
11	Switch	Business Technology Group	Privilege	BTG Head	Email
12	Desktop Central, Antivirus Software, Device Drivers, Firewall, Network Monitoring Tools, etc.	Business Technology Group	Privilege	BTG Head	Email

13	Source Code	Business Technology Group	Privilege	BTG Head	Email

- **Procedure to be Followed for Managing Access**

Sr.#	Activity	Responsibility
1	**Creating User Accounts**	
1.1	Send request for creation of user ID for a new hire employee	HR Team
1.2	Upon receiving the access request form, create a user account in AD. The standard format for username is FirstNameInitailMiddleNameInitialLastName.	Business Technology Group
1.3	Share the user ID and temporary password with the employee in person or over the remote connection.	Business Technology Group
1.4	Users need to change the password after the first login	User
2	**Granting Privileges to a User**	
2.1	When a new user joins Sudarshan, the CISO authorizes the BTG team to create a folder with relevant privileges for the user on the cloud storage	CISO/Business Technology Group
2.2	The access to a user's folder is to be restricted to the user and the BTG team	Business Technology Group
2.3	Privileged access is reviewed once a month	CISO
3	**Revoking the User Access**	
3.1	Receive request from HR for revoking the access granted to the user with the date	HR
3.2	Revoke all access granted to the user on their last working day and acknowledge the Exit Clearance Form	Business Technology Group
3.3	The user's folders (of an employee leaving or being terminated) should be hand overed to the respective reporting manager and backed up on the network drive	Business Technology Group
3.5	Check that user privileges to their folders are removed	Business Technology Group
3.6	User account access rights should be disabled on all servers on exit	Business Technology Group
4	**Revoking the Privileged Access**	

4.1	If the user is leaving or being terminated, then their emails will be forwarded to respective managers or Department Heads.	Business Technology Group
4.2	Revoked access should be reviewed on a quarterly basis	HOD/CISO
5	**Movement of User from One Location to Another**	
5.1	Receive intimation from functional/HR team on the movement of an employee to another location	Business Technology Group
5.2	Take necessary steps to ensure the user can continue working from the new location	Business Technology Group

10 SUPPLIER RELATIONSHIPS

Third-Party Security Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.19, 5.20, 5.21, 5.22

Purpose

The purpose of this policy is to ensure that information security risks associated with supplier relationships are properly managed and mitigated. This policy outlines the requirements for establishing, maintaining, and terminating supplier relationships, focusing on information security considerations throughout the supplier lifecycle.

Scope

This policy applies to all supplier relationships at Sudarshan including all contractors, vendors, and third-party service providers who have access to Sudarshan’s information assets or who are involved in processing, storing, or transmitting information on behalf of Sudarshan.

Responsibility

The responsibility for implementing and maintaining this policy lies with the BTG, Procurement Department, and all relevant departmental heads involved in supplier management.

Policy

Information Security in Supplier Relationships

- **Supplier Risk Assessment**
  - Conduct an initial risk assessment for all suppliers to identify potential information security risks.
  - Classify suppliers based on the criticality and sensitivity of the information they handle.
  - Perform periodic re-assessments of supplier risks based on changes in the scope of services or identified incidents.
- **Supplier Selection**
  - Include information security criteria in the supplier selection process.
  - Evaluate supplier security controls and practices before finalizing any agreements.
  - Consider suppliers with industry-recognized security certifications (e.g., ISO 27001, SOC 2).
- **Supplier Onboarding**
  - Ensure that all new suppliers undergo a formal onboarding process that includes a review of information security requirements.
  - Provide suppliers with the necessary security policies and guidelines they must adhere to.
  - Establish clear communication channels for reporting security incidents or concerns.

Addressing Information Security Within Supplier Agreements

- **Contractual Requirements**
  - Include specific information security requirements in all supplier agreements, covering the protection of company data, compliance with relevant regulations, and adherence to security policies.
  - Define roles and responsibilities for information security within the contract, including the responsibility for reporting security incidents.
  - Specify the security controls and measures the supplier must implement and maintain.
- **Confidentiality and Data Protection**
  - Include confidentiality clauses to ensure suppliers protect sensitive information.
  - Require suppliers to comply with data protection laws and regulations applicable to Sudarshan.
  - Include provisions for data encryption, secure data transfer, and data breach notification.
- **Access Control and Audit Rights:**

- Define access controls for supplier personnel accessing company information systems or data.
- Reserve the right to audit the supplier's security practices and controls periodically.
- Require suppliers to provide access to relevant audit reports or certifications.

Managing Information Security in the ICT Supply Chain

- **Supply Chain Risk Management**
  - Identify and assess information security risks within the ICT supply chain.
  - Ensure that suppliers implement security measures to protect the integrity and confidentiality of information throughout the supply chain.
  - Require suppliers to manage their own supply chain risks and ensure that sub-suppliers comply with security requirements.
- **Security Incident Management**
  - Require suppliers to report security incidents promptly and provide a detailed incident response plan.
  - Define procedures for joint incident response activities and communication during a security incident.
  - Review and update incident response plans with suppliers regularly.
- **Continuity and Resilience**
  - Require suppliers to implement business continuity and disaster recovery plans to ensure the continuity of services.
  - Evaluate the resilience of supplier services, including the ability to recover from security incidents or disruptions.
  - Ensure suppliers participate in continuity testing and share the results with Sudarshan.

Monitoring, Review, and Change Management of Supplier Services

- **Supplier Performance Monitoring**
  - Implement a process for continuous monitoring of supplier performance against agreed-upon service levels and security requirements.
  - Conduct regular security reviews and audits of supplier services to identify potential weaknesses or vulnerabilities.
  - Establish key performance indicators (KPIs) to measure supplier compliance with security obligations.
- **Change Management**
  - Require suppliers to notify Sudarshan of any significant changes in services, personnel, or security practices.

   - Evaluate the impact of changes on information security and update agreements or controls as necessary.
   - Include change management procedures in supplier agreements, covering approval and testing processes.
- **Supplier Relationship Review**
   - Conduct periodic reviews of supplier relationships to ensure alignment with business objectives and security requirements.
   - Assess the effectiveness of supplier security controls and identify areas for improvement.
   - Consider termination or renegotiation of contracts if suppliers fail to meet security expectations.
- **Contract Termination**
   - Define procedures for the secure termination of supplier contracts, including the return or destruction of company data.
   - Revoke all access rights and privileges granted to the supplier upon contract termination.
   - Conduct a final review of the supplier's compliance with security requirements before contract closure.

Procedure

Supplier Onboarding and Risk Assessment

- **Initiate Supplier Onboarding**
   - The Procurement Department initiates the onboarding process for new suppliers.
   - The BTG conducts an initial risk assessment to identify potential security risks.
- **Conduct Security Evaluation**
   - The BTG evaluates the supplier's security controls, certifications, and practices.
   - Suppliers are classified based on risk levels and criticality.
- **Approve Supplier**
   - Based on the evaluation, the Procurement Department approves the supplier for engagement.
   - Suppliers with high-security risks may be rejected or required to improve controls before approval.

Supplier Agreement and Contract Management

- **Draft Supplier Agreement**
   - The Legal Department, in collaboration with the BTG, drafts the supplier agreement.

  - Information security requirements, roles, and responsibilities are included in the contract.
- **Negotiate Contract Terms**
  - The Procurement Department negotiates contract terms with the supplier, ensuring all security requirements are addressed.
  - The Legal Department finalizes the contract, and both parties sign the agreement.
- **Manage Contract Changes**
  - The Procurement Department manages contract changes and ensures security requirements are updated accordingly.
  - Significant changes are evaluated by the BTG for its impact on information security.

Supplier Monitoring and Review

- **Monitor Supplier Performance:**
  - The BTG monitors supplier performance against agreed-upon service levels and security requirements.
  - Regular audits and reviews are conducted to assess compliance with security obligations.
- **Review Supplier Relationship:**
  - The Procurement Department conducts periodic reviews of supplier relationships, focusing on security performance.
  - The BTG identifies areas for improvement and collaborates with suppliers to enhance security controls.

10.1 Information Security for Use of Cloud Services

Cloud Security Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.23

Purpose

The purpose of this document is to set out key control activities that enable Sudarshan to make use of public Cloud resources in a secure and sustainable manner that manages the risk to Sudarshan and its customers with regards to the use of these services, including having due regard to regulatory requirements. The guidelines ensure the secure use of cloud-based applications, preventing security incidents by clearly understanding the responsibility.

Scope

This policy applies to all cloud-based applications used by Sudarshan.

Responsibility

The responsibility for enforcing this policy lies with the BTG team.

Policy

- **Manage Access Control**
  - Implement role-based permissions & access controls for users accessing the cloud environment to reduce the risks of unauthorized access to vital information.
- **Data Ownership**
  - Verify that the cloud service providers do not reserve rights to use, disclose, or make public Sudarshan's information.
  - Ensure the intellectual property rights of data owned by Sudarshan remain intact.
  - Confirm that data can be permanently erased from the cloud, including any backup storage, when requested by Sudarshan.
- **Password Policies**
  - Set password lengths as per the guidelines of Cloud Service provider.
  - Enforce a password expiration period as per the cloud service provider guidelines.
- **Multi-Factor Authentication**
  - Implement multi-factor authentication (MFA) for accessing critical cloud-based applications as the availability.
  - Use Approved MFA methods as provided by Cloud Service provider.
- **Access & Permissions**
  - Control application permissions to the cloud accounts and restrict access to vulnerable applications.
- **Data Loss Prevention**
  - Implement systems, processes, and services to ensure data integrity and persistence.
  - Develop a data loss prevention strategy to protect sensitive information from accidental or malicious threats.
- **Business Continuity**
  - Cloud Service provider shall Ensure end-to-end service continuity for all cloud-based applications.

11 SECURITY INCIDENT RESPONSE AND HANDLING POLICY

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Clause 6.1.3, Control 5.25

Purpose

The purpose of this policy is to establish procedures for prompt detection, assessment, notification, containment, evidence collection, eradication and recovery, chain of custody, root cause analysis and corrective action, lessons learned, and reporting of security incidents within SUDARSHAN.

Scope

This policy applies to all employees, contractors, and third-party entities who have access to SUDARSHAN'S' information systems, data, and resources.

Definitions

- Security Incident: Any suspected or confirmed breach of security policy or event that compromises the confidentiality, integrity, or availability of SUDARSHAN'S' information assets.
- Incident Response Team (IRT): A designated group responsible for coordinating and executing incident response procedures.
- Chain of Custody: Procedures and documentation used to maintain the integrity and accountability of evidence throughout its handling and analysis.

Incident Response Process

1. Detection

- Continuous Monitoring: Utilize advanced monitoring tools and technologies to detect security incidents in real-time.
- Threat Intelligence: Incorporate threat intelligence feeds and sources to identify potential threats and vulnerabilities.
- Anomaly Detection: Monitor for unusual patterns or deviations from normal activities.

2. Assessment

- Initial Triage: Immediately assess and classify incidents based on severity and potential impact.

- Incident Prioritization: Prioritize incidents based on criticality and impact on business operations.
- Impact Analysis: Evaluate the extent of the incident and potential implications on systems, data, and clients.

3. Notification

- Internal Notification: Promptly notify the Incident Response Team (IRT), including designated stakeholders and management, upon confirmation of a security incident.
- External Notification: Comply with legal and regulatory requirements for reporting incidents to clients, regulatory authorities, or affected parties.

4. Containment

- Isolation: Isolate affected systems or networks to prevent further spread of the incident.
- Containment Strategy: Implement containment strategies and controls to minimize impact and prevent escalation.
- Temporary Mitigations: Apply temporary fixes or mitigations to stabilize the environment and protect critical assets.

5. Evidence Collection

- Documentation: Maintain detailed records of incident response activities, including timestamps, actions taken, and individuals involved.
- Forensic Imaging: Conduct forensic imaging of affected systems to preserve evidence for analysis.
- Chain of Custody: Adhere to rigorous chain of custody to ensure the integrity and admissibility of evidence.

6. Eradication and Recovery

- Remediation: Remove malicious code, unauthorized access points, or vulnerabilities identified during the incident.
- System Restoration: Restore affected systems and data to a secure state from trusted backups or clean sources.
- Validation: Verify the effectiveness of remediation actions and ensure systems are fully operational.

7. Chain of Custody

- Secure Handling: Maintain secure storage and handling procedures for all collected evidence.
- Documentation Control: Document the chain of custody from initial collection through analysis and retention.
- Integrity Assurance: Implement controls to preserve evidence integrity and prevent tampering or unauthorized access.

8. Root Cause Analysis and Corrective Action

- Investigation: Conduct a thorough root cause analysis to determine how the incident occurred and identify vulnerabilities or weaknesses.
- Corrective Actions: Develop and implement corrective actions to address underlying causes and prevent recurrence.
- Documentation: Document findings, recommendations, and action plans for management review and approval.

9. Lessons Learned

- Post-Incident Review: Conduct a comprehensive review with stakeholders to analyze incident response effectiveness and identify areas for improvement.
- Knowledge Sharing: Share lessons learned and best practices across the organization to enhance incident response capabilities.
- Training and Awareness: Provide training and awareness programs based on lessons learned to enhance staff readiness and resilience.

10. Reporting

- Internal Reporting: Prepare detailed incident reports documenting incident details, response actions, and outcomes for internal records and analysis.
- External Reporting: Comply with contractual obligations and regulatory requirements for incident reporting to clients, regulators, or other relevant parties.

Data Privacy

- Data Protection: Ensure that personal data is handled in compliance with applicable data protection laws and regulations during all phases of the incident response process.
- Privacy Impact Assessment: Conduct privacy impact assessments to evaluate the potential impact of the incident on personal data.

- Data Minimization: Limit the collection and retention of personal data to what is necessary for incident response and investigation.
- Confidentiality: Maintain confidentiality of personal data and implement appropriate safeguards to prevent unauthorized access or disclosure.

Responsibilities

- Incident Response Team (IRT): Responsible for coordinating incident response efforts, executing response procedures, and ensuring compliance with this policy.
- Employees: Promptly report security incidents and comply with incident response procedures as outlined.

Compliance

- Policy Review: Regularly review and update this policy to align with changes in technology, business operations, and regulatory requirements.
- Training and Awareness: Provide ongoing training and awareness programs to ensure understanding and compliance with incident response procedures.

Enforcement

- Non-Compliance: Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

12 BUSINESS CONTINUITY MANAGEMENT

Business Continuity Policy

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.29, 5.30, 8.14

Purpose

The objective of this policy is to ensure the continued operation of critical business functions and the rapid recovery from disruptions at Sudarshan

Scope

This policy applies to all critical business functions and supporting IT systems.

Responsibility

The responsibility for enforcing this policy lies with the Business Continuity Management Team.

Policy

The following guidelines shall be followed to ensure business continuity and disaster recovery:

- Sudarshan shall develop, test, and maintain business continuity and disaster recovery plans.
- Sudarshan shall document and implement Business Continuity Plan (BCP) and procedures to maintain or restore operations and ensure the continuity of information security in the event of a short-term disruption or a disaster.
- Critical business functions and IT systems should be identified and protected.
- Business Impact Analysis (BIA) and Recovery Time Objectives (RTOs), as well as the roles and responsibilities of personnel, shall be taken into account for business continuity planning.
- The BCP shall be reviewed at least once a year to confirm the incorporation of all changes since the previous review.
- To ensure awareness about the evacuation process and response to an emergency, an evacuation simulation shall be conducted once a year.
- In the event of a disaster affecting Sudarshan or its resources, the Business Continuity Management Team shall respond in accordance with the Disaster Recovery Plan (DRP) and initiate specific actions for recovery.
- Application systems and business processes that are critical to the business shall be planned for continuity of operations in the event of business disruptions.
- The cost-effectiveness and fitness for the purpose of countermeasures to be implemented should be considered and continually reviewed as part of normal management responsibility.
- It shall be ensured that critical services needed for meeting business requirements, Sudarshan’s property, and information security are maintained with minimal interruption in the event of disasters and failures.
- Major business continuity risks that threaten the continuation of the delivery of services and security shall be identified, tested, and maintained.
- The respective department heads and support teams shall be responsible for assessing the potential impact on their business processes.
- The Business Continuity Management Team (BCMT) shall oversee the implementation, maintenance, and testing of the BCP and DRP.
- This policy shall be reviewed and approved by the Business Continuity Management Team (BCMT) annually or as required due to changes in the business environment or operations.

Business Continuity

- Sudarshan's respective department heads and support teams are responsible for assessing the potential impact on their business processes.
- The plans shall include provisions for business continuity of critical business processes and recovery in the event of disaster and failures.
- The plan shall contain considerations of backups of critical information supporting these business operations based on Risk Assessment.
- Based on the business need, a paper-based walkthrough or an actual test of all business continuity plan/disaster recovery plans shall be conducted as appropriate.
- Sudarshan shall ensure that ICT readiness is planned, implemented, maintained, and tested in accordance with business continuity objectives.

Planning Information Security in Business Continuity

- The scope of the Business Continuity Plan shall consider applicable factors including customer requirements, legal regulations, and industry requirements. The following shall be considered while implementing any DR/BCP program:
- Identify critical business functions, applications, and supporting technologies.
- Develop an appropriate cost-effective recovery strategy.
- Identify alternate backup locations with the necessary infrastructure to support the recovery needs.
- Identify the SPOCs for the disaster response and recovery teams.
- Train the SPOCs for conducting BCP tests.
- Identify the vendors that are required for recovery support.
- A thorough risk assessment shall be carried out for all assets required for business continuity, considering all the events that can disrupt the business processes. The considered events shall include but are not limited to, man-made error, natural disasters, technical failure, etc.

Business and Information Security Continuity

- Pune, Global Head Office Inaccessible
  - In case of a disaster/failure, where users are not able to work/connect to the Pune, India office, the Pune team will communicate to R&D Center (Sutarwadi), Manufacturing Units (Mahad & Roha) team to intimate all the clients about the nonfunctioning of the Pune, India office and that there could be a potential delay in work deliverables.
  - All customer requests shall be routed to Mahad, Roha, or Sutarwadi office.
  - To maintain information security, user authentication requests shall be done via domain controllers hosted in Mahad, Roha, or Sutarwadi.

- Users shall connect via VPN to access critical systems from outside network.

- **Mahad, Roha Manufacturing Unit Inaccessible**
  - In case of a disaster/failure, where users are not able to work/connect to the Roha, Mahad office, the Roha team will communicate to Pune, India (Global Head Office) team to intimate all the clients about the nonfunctioning of the Roha, Mahad office and that there could be a potential delay in work deliverables.
  - All customer requests will be routed to Pune or the Sutarwadi office.
  - To maintain information security, user authentication requests will be done via domain controllers hosted in Pune, India.
  - Users shall connect via VPN to access critical systems from Outside Network.

Test Calendar

Sr. No.	Test Type	Frequency	Owner
1	Fire Drill Evacuation	Annually	Admin Team
2	DR Drill – Key Users to login from Mahad	Annually	Business Technology Group
4	Work From Home Testing	Regularly	Business Technology Group
5	Backup Restoration Testing	Annually	Business Technology Group

Disaster Recovery Plan
RPO (Recovery point Objective) & RTO (recovery Time objective)

	Recovery Site	
Criticality	Primary (Hrs)	Secondary (Hrs)
High	14	53
Medium	8	59
Low	20	151

Detailed describe Plan mentioned in **IT - Disaster Recovery Plan** document.

13 LEGAL AND REGULATORY COMPLIANCE

14.1 Legal, Statutory, Regulatory & Contractual Requirements

Legal & Regulatory Compliance Policy

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.31

Purpose

The objective of this policy is to ensure that Sudarshan complies with all relevant laws, regulations, and standards related to information security. It aims to avoid breaches of any criminal and civil law, statutory, regulatory, or contractual obligations, and security requirements. The policy also seeks to maximize the effectiveness of, and minimize interference with, the system audit process, thus ensuring compliance with organizational security policies and standards.

Scope

This policy applies to all employees, contractors, and third-party service providers.

Responsibility

The responsibility for enforcing this policy lies with the Legal & Compliance Team.

Policy

The following guidelines shall be followed to ensure compliance:

- All activities shall comply with applicable laws, regulations, and standards.
- Regular audits and assessments shall be conducted to ensure compliance.
- Specific legal advice should be sought from suitably qualified legal practitioners, as applicable.
- All relevant statutory, regulatory, and contractual requirements should be explicitly defined and documented for each information system.
- Specific controls and individual responsibilities to meet these requirements should be defined and documented.
- Information systems should be regularly reviewed against appropriate security policies and technical platforms and audited for compliance with security implementation standards.
- All required licenses should be purchased, and an inventory of all software installed on Sudarshan's computers should be maintained and regularly checked

for compliance. Original copies of media, licenses, and manuals should be preserved.

- The retention period of all important records required as per statutory/regulatory requirements should be defined and mentioned on the record. All such records should be protected from loss, destruction, and falsification until the retention period ends.
- Personal identifiable information shall only be collected and used for business purposes, in line with relevant legislation, regulations, and contractual clauses.

Procedure

- **Legal and Regulatory Requirements**
  - Identify all relevant laws, regulations, and standards that apply to Sudarshan.
  - Develop and maintain a compliance matrix to track requirements and ensure adherence.
- **Internal Policies**
  - Develop internal policies and procedures to address compliance requirements.
  - Enforce compliance policies through regular training and awareness programs.
  - Ensure all employees are aware of and understand the compliance policy.
- **Audits and Assessments**
  - Conduct regular internal audits to assess compliance with internal policies and external requirements.
  - Facilitate external audits by regulatory bodies and third-party auditors as required.
  - Information systems should be audited for compliance with security implementation standards.
- **Reporting and Documentation**
  - Prepare and submit compliance reports to senior management and regulatory bodies as required.
  - Maintain thorough documentation of compliance activities, including audit findings and corrective actions.
  - Define and document the retention period for all important records required as per statutory/regulatory requirements and ensure these records are protected until the retention period ends.
- **Continuous Improvement**
  - Perform regular gap analyses to identify areas of non-compliance and opportunities for improvement.
  - Develop and implement action plans to address identified gaps and enhance compliance efforts.

  - Take immediate action to remediate any compliance violations and prevent recurrence.
  - Collect and use personal identifiable information only for business purposes and in accordance with relevant legislation, regulations, and contractual clauses.

14.2 Intellectual Property, Record Protection, and Data Privacy Policy

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.32, 5.33, 5.34

Purpose

The purpose of this policy is to ensure that Sudarshan effectively manages and protects its intellectual property rights, maintains the integrity and confidentiality of its records, and safeguards the privacy of personally identifiable information (PII) in compliance with applicable laws, regulations, and standards.

Scope

This policy applies to all employees, contractors, vendors, and third-party service providers who have access to Sudarshan's information systems, data, and intellectual property.

Responsibility

The following responsibilities are defined under this policy:

- **Legal & Compliance Team**: Oversee the implementation and enforcement of this policy, provide guidance on legal and regulatory requirements, and manage compliance audits.
- **Business Technology Group**: Implement technical controls and procedures to protect intellectual property, records, and PII, and ensure adherence to this policy.
- **HR Department**: Ensure employee awareness and training on intellectual property, data protection, and privacy practices.
- **All Employees**: Adhere to the policies and procedures outlined and report any breaches or potential breaches to the appropriate department.

Policy

- **Intellectual Property Rights**

Sudarshan is committed to protecting its intellectual property (IP) and respecting the intellectual property rights of others.

- Identification and Protection:
  - Identify and document all intellectual property assets, including patents, trademarks, copyrights, trade secrets, and proprietary information.
  - Implement appropriate technical, administrative, and physical controls to protect Sudarshan's intellectual property from unauthorized access, use, disclosure, or infringement.
- Usage and Licensing:
  - Ensure that all software, content, and materials used within Sudarshan are appropriately licensed and comply with licensing agreements.
  - Obtain legal approval before using any third-party intellectual property to ensure compliance with relevant laws and agreements.
- Employee and Third-Party Compliance:
  - Train employees and third parties on their obligations regarding intellectual property protection and provide clear guidelines on acceptable use.
  - Include IP protection clauses in contracts with third-party vendors and partners to ensure compliance with Sudarshan's IP policies.
- Monitoring and Enforcement:
  - Regularly monitor compliance with intellectual property laws and this policy.
  - Take appropriate action against any infringement of Sudarshan's intellectual property rights, including legal action if necessary.

- **Protection of Records**
  - Sudarshan is committed to ensuring the integrity, confidentiality, and availability of its records in compliance with statutory and regulatory requirements.
- Record Management:
  - Identify and classify records based on their importance and sensitivity.
  - Define retention periods for each type of record in accordance with legal, regulatory, and business requirements.
- Record Protection:
  - Implement access controls to ensure that only authorized personnel have access to records.
  - Use encryption, backup, and disaster recovery solutions to protect records from loss, destruction, and unauthorized access.
- Record Disposal:

  - Develop and implement procedures for the secure disposal of records that are no longer required, ensuring that records are destroyed in a manner that prevents unauthorized access or reconstruction.

- **Privacy and Protection of Personally Identifiable Information (PII)**
  Sudarshan is committed to protecting the privacy of individuals and ensuring the confidentiality of personally identifiable information (PII).
  - PII Collection and Use:
  - Collect and use PII only for legitimate business purposes and in compliance with applicable laws and regulations.
  - Obtain consent from individuals before collecting, using, or disclosing their PII, except where otherwise permitted by law.
- PII Protection:
  - Implement appropriate security measures to protect PII from unauthorized access, use, disclosure, alteration, or destruction.
  - Regularly review and update security measures to address new threats and vulnerabilities.
- Data Subject Rights:
  - Inform individuals of their rights regarding their PII, including the right to access, correct, and delete their data.
  - Respond promptly to requests from individuals to exercise their rights and ensure compliance with applicable legal requirements.
- Breach Notification:
  - Develop and implement procedures for responding to data breaches, including notifying affected individuals and regulatory authorities as required by law.
  - Investigate breaches and take corrective actions to prevent recurrence.

Procedure

- **Intellectual Property Rights Procedure**
- IP Inventory:
  - Maintain a centralized inventory of all intellectual property assets.
  - Regularly update the inventory to reflect new IP assets and changes in status.
- IP Compliance Checks:
  - Conduct periodic reviews to ensure compliance with IP licensing agreements.
  - Verify that all third-party content and software are appropriately licensed and used in accordance with agreements.

- IP Incident Management:
  - Report any suspected IP infringement to the Legal & Compliance Team immediately.
  - Investigate IP incidents and take corrective actions to prevent recurrence.

- **Protection of Records Procedure**
- Record Access Control:
  - Implement role-based access controls to limit access to records based on job responsibilities.
  - Review access permissions regularly and update them as needed.
- Record Backup and Recovery:
  - Schedule regular backups of critical records and store them securely.
  - Test disaster recovery procedures periodically to ensure effective data restoration.
- Record Disposal:
  - Follow secure disposal procedures for physical and electronic records, including shredding or permanently deleting sensitive information.

- **Privacy and Protection of PII Procedure**
- PII Collection and Consent:
  - Obtain explicit consent from individuals before collecting their PII, unless otherwise permitted by law.
  - Maintain records of consent and ensure they are easily accessible for audit purposes.
- PII Access and Correction:
  - Provide individuals with access to their PII upon request and facilitate corrections as needed.
  - Implement procedures for verifying the identity of individuals requesting access or correction of their data.
- PII Breach Response:
  - Develop a data breach response plan outlining steps for identifying, containing, and mitigating breaches.
  - Notify affected individuals and regulatory authorities of breaches as required by law.
- Employee Training:
  - Conduct regular training sessions on data protection and privacy practices.
  - Update training materials to reflect changes in laws, regulations, and company policies.

- **Monitoring and Review**
  - Conduct regular reviews of this policy to ensure it remains current and effective.
  - Monitor compliance with this policy through audits, assessments, and feedback from stakeholders.
  - Update the policy as needed to address new threats, vulnerabilities, and regulatory changes.

14 MONITORING AND REVIEW OF ISMS

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 5.35, 5.36, 5.37

Purpose

The purpose of this policy is to ensure that Sudarshan maintains a robust information security management system (ISMS) that is regularly reviewed, complies with relevant policies, rules, and standards, and is supported by well-documented operating procedures. This policy is designed to enhance Sudarshan's overall security posture by ensuring continuous improvement and adherence to best practices.

Scope

This policy applies to all employees, contractors, vendors, and third-party service providers who have access to Sudarshan information systems, data, and resources.

Responsibility

The responsibility for enforcing this policy lies with the Management Review Committee(MRC), which includes representatives from BTG, Legal & Compliance, and relevant business units.

Policy

- **Independent Review of Information Security**

  Ensure that Sudarshan's information security practices are regularly reviewed by independent parties to provide an objective assessment of the effectiveness and compliance of the ISMS.
  - The organization shall engage qualified external auditors to perform independent reviews of the ISMS at least annually. These audits will assess the adequacy and

effectiveness of information security controls, identify gaps, and recommend improvements.
  - In addition to external audits, internal audits shall be conducted periodically by the internal audit team or designated personnel. These audits will cover all aspects of the ISMS and provide insights into areas requiring attention.
  - Senior management should review the results of independent and internal audits to assess the overall security posture and make informed decisions regarding security improvements and resource allocation.
  - Audit findings and recommendations shall be documented and communicated to relevant stakeholders. Action plans shall be developed to address identified issues, and progress shall be monitored to ensure timely resolution.

- **Compliance with Policies, Rules, and Standards for Information Security**
  Ensure that all information security policies, rules, and standards are effectively implemented, communicated, and adhered to across Sudarshan.
  - The CISO shall develop and maintain comprehensive information security policies, rules, and standards that align with industry best practices and regulatory requirements.
  - All employees, contractors, vendors, and third-party service providers shall be made aware of the information security policies, rules, and standards. This shall be achieved through regular training, awareness programs, and easy access to policy documents.
  - Compliance with information security policies shall be mandatory for all personnel. Non-compliance shall result in disciplinary action, which may include termination of employment or contract.
  - Information security policies, rules, and standards shall be reviewed and updated at least annually or as needed to reflect changes in the threat landscape, technology, or regulatory requirements.

- **Documented Operating Procedures**
  Ensure that all information security-related activities are supported by documented operating procedures to promote consistency, reliability, and accountability.
  - The CISO shall develop and maintain documented operating procedures for all critical information security activities, including access control, incident response, data protection, and system configuration.
  - Documented procedures shall be easily accessible to authorized personnel who need them to perform their duties. Access to procedures shall be restricted to those with a legitimate need to know.

  - Documented procedures shall be reviewed and updated regularly to reflect changes in technology, processes, and security requirements. Feedback from users and audit findings should be considered when updating procedures.
  - All personnel responsible for executing documented procedures shall receive appropriate training to ensure they understand their roles and responsibilities. Training records should be maintained for audit purposes.

Procedure

- **Independent Review of Information Security**
- Planning and Scheduling Audits
  - External Audits:
    - Engage qualified external auditors with expertise in information security.
    - Schedule audits annually, considering business cycles and critical periods.
  - Internal Audits:
    - Designate internal audit personnel or teams with the necessary skills.
    - Develop an audit plan covering all ISMS components, including policies, controls, and procedures.
- Conducting Audits
  - Provide auditors with access to relevant documents, records, and systems.
  - Ensure auditors understand the scope and objectives of the audit.
  - Conduct audits objectively, thoroughly examining policies, controls, and procedures.
  - Identify strengths, weaknesses, and opportunities for improvement.
- Reporting and Action Plans
  - Prepare detailed audit reports with findings, recommendations, and risk assessments.
  - Present reports to senior management for review and decision-making.
  - Develop action plans to address audit findings and recommendations.
  - Assign responsibilities, set deadlines, and track progress.
- **Compliance with Policies, Rules, and Standards for Information Security**
- Policy Development and Maintenance
  - Policy Creation:
    - Develop comprehensive information security policies that align with industry standards and regulatory requirements.
    - Include input from relevant stakeholders, including legal, BTG, and business units.
  - Policy Approval:
    - Submit policies for approval by senior management and the MRC.

        - Ensure policies are formally documented and version controlled.

- Policy Communication and Training
    - Conduct regular training sessions and awareness programs for employees, contractors, and vendors.
    - Provide easy access to policy documents through Sudarshan's intranet or document management system.
    - Implement mechanisms to monitor and enforce policy compliance.
    - Conduct periodic assessments to ensure adherence to policies.
- **Documented Operating Procedures**
- Procedure Development and Maintenance
    - Develop documented operating procedures for all critical information security activities.
    - Ensure procedures are detailed, clear, and aligned with policies.
    - Submit procedures for approval by the MRC and relevant stakeholders.
    - Maintain a centralized repository for all approved procedures.
- Procedure Training and Compliance
    - Provide training to personnel responsible for executing documented procedures.
    - Maintain training records and update training materials as needed.
    - Regularly review and update documented procedures to reflect changes in technology, processes, and security requirements.
    - Solicit feedback from users and incorporate lessons learned from audits and incidents.

15 BUSINESS TECHNOLOGY GROUPREMOTE WORKING

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 6.7

Purpose

The primary purpose of this document is to provide a secure framework for the use of mobility devices of Sudarshan.

Scope

The Work from Anywhere (WFA) Policy applies to Sudarshan stakeholders/employees who have access to Sudarshan information and associated processing facilities and assets.

Definitions

- **Mobile Computing**: Working from a non-fixed location using mobility devices.

- **Work From Anywhere**: Work carried out away from normal places of work, such as offices, performed in a fixed location, e.g., at home or any public place.
- **Teleworking**: Work carried out away from normal places of work, such as offices, performed in a fixed location, e.g., at home.
- **Mobility Devices**: Computing devices are small enough to hold and operate in hand, e.g., laptops.

Roles and Responsibilities

- **Chief Information Security Officer (CISO)**: Responsible for overseeing the implementation and enforcement of the policy. Accountable for ensuring compliance and handling exceptions.
- **Business Technology Group**: Responsible for providing technical support and implementing security measures. Accountable for maintaining the security of mobility devices and responding to incidents of loss or theft.
- **Heads of Departments (HODs)**: Responsible for ensuring employees under their supervision comply with the policy. Accountable for notifying IT immediately upon termination of employees using mobility devices.

Policy

- Safe and secure use of Mobility equipment in support of operational work of the Sudarshan shall be ensured.
- Secure working practice for personnel/employees who intend to use and transfer manual and computer files between home, the office and the community shall be provided.
- It shall be ensured that Sudarshan resources provided to staff are not misused.
- The security of computer systems and the information they contain shall not be compromised in any way.
- Employees working from remote locations shall route all maintenance requests through IT and not directly approach the vendors.

- **Work from Anywhere**
  - As a policy, Sudarshan allows Work from Anywhere.
  - Any employee that needs to work from a remote location shall connect to the application directly from the internet as most of the applications are web-based, no VPN is required.
  - Management authorizes all the users to work remotely since it is a business requirement.

- The physical and logical controls implemented within the Sudarshan network and physical environment shall not be automatically available when working outside of that environment.
- Users shall take necessary measures to protect sensitive information in these circumstances. Unauthorized access and tampering to a mobility device, particularly if there are repeated opportunities for access, shall:
  - Lead to continuing (and undetected) compromise of information on the device itself undermine security measures, intended to protect information on the device in the event of loss or theft; and
  - All Information Security Policies and Procedures applicable at Sudarshan shall still hold good for Work from Anywhere.
- Due care shall be exercised by employees working from anywhere to ensure confidentiality of Sudarshan's information and security of its assets.
- Any compromise of Sudarshan's information or assets shall be immediately reported to the IT / CISO by the employees working from anywhere.
- Sudarshan shall initiate punitive action against a Work from Anywhere employee in case of any compromise of its information while working from anywhere and reserves the right to recover a proportionate amount of financial loss arising from the same, subject to it being proved that the said compromise resulted from lack of due care by the employees working from anywhere.
- When undertaking Mobile computing/Work from Anywhere the following guidelines shall be followed:
  - When travelling, equipment (and media) shall not be left unattended in public places.
  - Laptops shall be carried as hand luggage when travelling.
  - When using a laptop, employees shall not process personal or sensitive data in public places, e.g., on public transport.
  - General access to the laptop for use by immediate household members is not permitted. The employee shall bear the responsibility for the consequences should access be misused.
- Passwords used for access to the Sudarshan systems shall never be stored on Mobility devices where they may be stolen or permit unauthorized access to the information assets.
- Security risks (e.g., of damage, loss or theft) may vary considerably between locations and this should be considered when determining the most appropriate security measures.
- Sensitive data, including that relating to clients, stored on a hardened laptop shall be kept to the minimum required for its effective business use in order to minimize the risks and impacts.

- **Mobility Devices Policy**
  - Only authorized Mobility devices shall be used for business within the Sudarshan by the authorized employees of the Sudarshan.
  - Mobility devices should be kept secure at all times. Each individual is responsible for their physical protection against loss, damage, abuse or misuse. This includes when it is used, where it is stored, and how it is protected in transit.
  - Mobility devices should regularly be updated, e.g., Anti-Malware and Windows updates, etc.
  - Mobility devices shall always be kept with you or locked away when not in use.
  - Mobility devices use shall be kept to a minimum when used in public areas.
  - Personal identifiable information shall be saved on Mobility devices in a separate folder.
  - All Mobile computing Devices shall be tagged.
  - Users shall immediately notify the BTG team if the device is suspected to be lost or stolen by utilizing the Incident Reporting Form.
  - HODs shall notify BTG team immediately upon termination of employees using Mobility devices.

- **Teleworking Policy**
  - The physical and logical controls that are available within the Sudarshan network and physical environment shall not automatically be available when working outside of that environment, as a result, there is an increased risk of information being subject to unauthorized access.
  - Mobile computing / Teleworking users shall take necessary measures to protect sensitive information in these circumstances. Unauthorized access and tampering to a Mobile computing / Teleworking device, particularly if there are repeated opportunities for access, may:
    - Lead to continuing (and undetected) compromise of information on the device itself undermine security measures, intended to protect information on the device in the event of loss or theft; and
    - All Information Security Policies and Procedures applicable at Sudarshan still hold good for telework.
  - Due care shall be expected to be exercised by teleworking employees to ensure the confidentiality of Sudarshan’s information and the security of its assets.
  - Any compromise of Sudarshan’s information or assets shall be immediately reported to the IT / ISO by the teleworking employee.

- The Sudarshan shall initiate punitive action against a teleworking employee in case of any compromise of its Information while teleworking and reserves the right to recover a proportionate amount of financial loss arising from the same, subject to it being proved that the said compromise resulted from lack of due care by the teleworking employee.
- The impact of a breach of Mobile computing / Teleworking security shall extend far more widely than the device itself. When undertaking Mobile computing / Teleworking the following guidelines must be followed:
  - When traveling, equipment (and media) shall not be left unattended in public places. Portable computers are to be carried as hand luggage when traveling. When using a laptop, do not process personal or sensitive data in public places e.g. on public transport.
  - General access to the laptop for use by immediate household members shall not be permitted. The employee bears responsibility for the consequences shall the access be misused.
  - Passwords should be used for accessing the Sudarshan systems and never to be stored on mobile devices where they may be stolen or permit unauthorized access to the information assets.
  - Security risks (e.g. of damage, loss, or theft) may vary considerably between locations and this should be considered when determining the most appropriate security measures.
  - Sensitive data, including that relating to clients, stored on a Trusted/Protected laptop shall be kept to the minimum required for its effective business use to minimize the risks and impacts.

- **Remote Access Policy**
  - Mobile computing, teleworking, and remote access policies should be put in place to ensure information security when using mobile computing and teleworking facilities.
  - A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
  - As a communications and operations security policy, necessary controls shall be in place.
  - Allowed Technologies for Remote Access Capabilities are as follows:
    - Tunneling based VPN (allowed only for Sudarshan devices) shall be used.
    - Sudarshan-approved wireless email devices (smartphones, etc.) shall be used.
    - True SSL VPN that checks for malware and antivirus on the source machine shall be used.
  - Technology Implementation Requirements for Remote Access are as follows:

    - Multi-factor authentication shall be used.
    - Split tunneling shall not be allowed when connected to the Sudarshan network.
    - Remote access connections should have a 30-minute inactivity timeout.
    - VPN sessions shall be re-authenticated every 8 hours.
    - Multiple VPN sessions shall not be permitted.
  - Only corporate-approved security products and services shall be used to connect and authenticate to Sudarshan networks.

16 CLEAR DESK AND CLEAR SCREEN

Clear Desk & Clear Screen Policy

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 7.7

Purpose

The primary purpose of this document is to define a systematic policy to establish and maintain a system for the security of Sudarshan.

Scope

The Clear Desk and Clear Screen Policy applies to all employees of Sudarshan.

Responsibility

- **Employees**: Responsible for ensuring compliance with the Clear Desk and Clear Screen Policy. Accountable for maintaining clear desks and screens, securing confidential information, and following proper information handling policies and procedures.
- **Department Heads**: Responsible for enforcing the policy within their respective departments. Accountable for conducting periodic checks to ensure compliance and addressing any non-compliance issues.
- **CISO**: Responsible for approving and maintaining the policy. Accountable for ensuring that all staff receive annual training on the policy and for overseeing internal audits to monitor compliance.

Policy

- No important information assets shall be left unprotected on desks after Sudarshan working hours.
- Confidential, sensitive or critical business information, on paper or on electronic storage media, shall be locked away when not required, especially when the office is vacated.
- Users shall log off / lock their machines when they are not at their desk. Personal computers and computing terminals shall be attended to when in a 'logged on' condition

and shall be protected with screen saver passwords or by locking it using Ctrl+Alt+Del keys option or Windows Key + L when the host is unattended.

- The user end points shall have Account lockout activated after 10 minutes of inactivity.
- All confidential/internal use information or media shall be locked in the desk when the workstation is unattended.
- All information should be handled responsibly, and it is the responsibility of each employee to protect the information they have access to.
- All desks shall be clear of any papers holding confidential information related to Sudarshan as well as clients. No confidential information shall be displayed on pin-up boards.
- All aspects and related roles and responsibilities of managing, reviewing, and updating the Clear Desk and Clear Screen Policy shall be approved by the CISO.
- All staff are trained annually on the Clear Desk and Clear Screen Policy, and random checks are performed periodically to ensure compliance. All documents shall be tracked during internal audits.

17 Operational Security

17.1 User Endpoint Devices

User Endpoint Devices Security Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.1

Purpose

The objective of the User Endpoint Devices Policy is to ensure the secure management and use of endpoint devices at Sudarshan.

Scope

This policy applies to all personnel using endpoint devices (desktops, laptops) that connect to Sudarshan's network or handle company information.

Responsibility

The responsibility for enforcing this policy lies with the Business Technology Group.

Policy

The following guidelines shall be followed to ensure the security of endpoint devices:

- All endpoint devices shall be configured according to Sudarshan's security standards.
- Endpoint devices should be encrypted to protect sensitive data for supported devices.
- Antivirus and anti-malware software should be installed and regularly updated.
- Users shall report any loss or theft of endpoint devices immediately.

Procedure

- **Configuration of Devices**
  - BTG team shall configure endpoint devices according to Sudarshan's security baselines before deployment.
  - All devices must have the following settings enabled:
    - Firewall
    - Disk encryption (e.g., BitLocker for Windows)
  - Software Installation: Only approved software should be installed on endpoint devices.

- **Encryption**
  - BTG must ensure that all endpoint devices have disk encryption enabled.
  - Regular checks must be conducted to verify that encryption is active on all devices.

- **Antivirus and Anti-Malware**
  - BTG must install approved antivirus and anti-malware software on all endpoint devices.
  - BTG must ensure that antivirus definitions and software updates are applied regularly, at least daily.
  - Scheduled scans must be configured to run weekly.

- **Incident Reporting**
  - Users must report the loss or theft of any endpoint device to the Business Technology Group immediately.
  - BTG shall follow the incident response plan.

17.2 Privileged Access Rights

Privileged Access Rights Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO **27001**:2022 - Control No. 8.2

Purpose

The objective of this policy is to control and monitor the use of privileged access to systems and data at Sudarshan.

Scope

This policy applies to all personnel with privileged access to Sudarshan's systems and data.

Responsibility

The responsibility for enforcing this policy lies with the CISO.

Policy

The following guidelines shall be followed to ensure secure management of privileged access:

- Privileged access shall be granted only to authorized personnel.
- Privileged accounts shall be reviewed bi-annually.
- Use of privileged access shall be logged and monitored.
- The allocation of access rights to information systems and services shall be managed comprehensively across all stages of the user access life cycle. This includes the processes of initial registration, modification, and final de-registration of users.

Procedure

- **Access Request and Approval**
  - Requests for privileged access must be documented using Email (HoD) or Ticketing tool. (End User)
  - Requests must be approved by the relevant Department Heads or Managers.

- **Account Management**
  - Each privileged user must have a unique account.
  - Privileged accounts must adhere to the Password Policy with additional complexity requirements.
  - Privileged accounts must be reviewed half yearly to ensure they are still required and appropriately assigned.

- **Logging and Monitoring**
  - All activities performed using privileged accounts must be logged.
  - Logs must be reviewed weekly by the BTG Security Team for any suspicious activity.
  - Alerts must be set up for unusual activities, such as access outside normal working hours or access to sensitive data.

- **Privileged Session Management**
  - Privileged sessions must be recorded where possible for audit purposes.
  - Privileged sessions must automatically time out after 15 minutes of inactivity.

17.3 Information Access Restriction

Information Access Restriction Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.3

Purpose

The objective of this policy is to ensure that access to information systems is restricted to authorized users at Sudarshan.

Scope

This policy applies to all personnel with access to Sudarshan's information systems.

Responsibility

The responsibility for enforcing this policy lies with the Business Technology Group and the CISO.

Policy

The following guidelines shall be followed to ensure secure access control:

- Access shall be based on the principle of least privilege.
- Access rights shall be reviewed biannually.

Procedure

- **Access Control Implementation**
  - Access must be assigned based on job roles and description shared by the HR Team over Email.

  - Access requests must be submitted by the HR Team and approved by the relevant Department Head/Manager.
  - BTG must provide access based on the approved request and ensure it aligns with the Job roles and description shared by the HR.

- **Access Review and Revocation**
  - BTG team must review access rights on a half yearly basis.
  - Access rights must be revoked immediately upon termination of employment or a change in role. The Business Technology Group must be notified immediately.

- **Access Monitoring**
  - Access to critical systems must be logged and reviewed periodically.
  - Automated alerts must be set up for unauthorized access attempts through a VPN and PAM 360.

17.4 Secure authentication

Password Management Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.5

Purpose

The objective of this policy is to ensure secure authentication mechanisms are in place at Sudarshan to protect the integrity, confidentiality, and availability of information systems and data. This policy governs the appropriate password assignment and management mechanisms to ensure that all passwords are created, used, and managed in a secure manner, preventing unauthorized access to information systems and data.

Scope

This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that has access to Sudarshan's network or stores any non-public organization information. It includes all employees, contractors, consultants, temporary workers, and other workers at Sudarshan, including all personnel affiliated with third parties.

Responsibility

The responsibility for enforcing this policy lies with the CISO.

Policy

- All system accounts shall be assigned a unique user ID and password that are protected in accordance with Sudarshan's password policy statements.
- All initial system user accounts shall be set up by the System Administration Team as per the Joining form.
- First-time users shall log in to their accounts with the password provided by the System Administrator and shall be required to change their password to a new password that complies with the corporate password policy.
- Sharing passwords shall be prohibited.
- A copy of all critical passwords as per the access control policy shall be kept with the BTG Head, in a sealed envelope, and the contents shall be updated immediately upon any changes.
- Any queries regarding passwords shall be reported to the System Administration Team.
- Passwords shall be protected as organizational proprietary information. Writing them down or storing them in open area shall be prohibited.
- Using programs or scripts that include system passwords shall be prohibited.
- The System Administration Team shall enforce required password changes out of cycle for certain security events that have the potential for security compromises (e.g., employee relocation, intrusion attempt, or employee termination).
- If a user leaving Sudarshan is a privileged user, system passwords shall be changed on his/her last working day.
- Password expiration warnings shall be provided at least 15 days prior to the password expiration.

To ensure secure authentication and password protection, the following guidelines must be followed:

- MFA should be used for accessing critical systems.
- All user-level and system-level passwords shall conform to the password construction guidelines mentioned below.
- Passwords shall comply with complex requirements:
  - Passwords shall be at least 8 characters long.
  - Passwords shall consist of alphanumeric and special characters.
  - Passwords shall be a combination of all the following four elements:
    - One upper case letter (A – Z).
    - One lower case letter (a – z).
    - One digit (0 – 9).

  - One special character (@, ~, !, etc.).

.

- Password changes shall follow a formal request by raising a ticket for a password change.
- Accounts shall be locked out after 3 incorrect password attempts for 10 minutes.
- Users shall adhere to the following password guidelines for laptops and desktops:
  - Maximum minutes of inactivity until screen locks: 10 minutes.
  - Password expiration: 60 days.
  - Prevent reuse of previous passwords: 3.
  - Preferred Microsoft Entra tenant domain: sudarshan.com.

Procedure

- **Multi-Factor Authentication (MFA):**
  - BTG team shall configure MFA for all critical systems.
  - Approved methods include one-time passwords (OTP), mobile authenticator apps, and hardware tokens.
- **Password Complexity and Management:**
  - Passwords must be at least 8 characters long and include a mix of uppercase letters, lowercase letters, digits, and special characters.
  - Users must change their passwords every 60 days.
  - Accounts must be locked out after 3 unsuccessful login attempts for 10 minutes.
  - Prevent reuse of the last 3 passwords.

- **Password Management for Servers:**
  - Server admin username must be renamed, and the password must be kept with the BTG Head.
  - When the admin user ID needs to be accessed, the BTG Head/CISO should change the password immediately.
  - Each BTG System admin will have their own unique user ID and password.
  - Follow the password policy as defined in the above section.

- **Password Management for Desktops & Laptops:**
  - Raise a ticket for the Business Technology Group to change the system password.
  - In case of a forgotten system password, raise ticket in ticketing tool.

  - Once the password reset is done by System Admin, the employee must verify whether the password was changed successfully when they receive the password change confirmation from the Admin.
  - New passwords are auto generated by the system, and a password change prompt is given to the users.

- **Password Management for Network Devices:**
  - Create a unique ID for Firewall and switches.
  - Configure the password policy for all Network Admins with appropriate entitlements.
  - When the admin user ID needs to be accessed, the BTG Head/CISO should change the password immediately.

- **Password Management for E-mail:**
  - Self-service is available in Email Office 365 through which users can change the password.
  - Users will get the link to change/reset the password on the alternate email address/mobile number and by following the on-screen instructions, users can change the password.

- All user-level and system-level passwords shall conform to these guidelines.

17.5 Capacity Management

Capacity Management Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.6

Purpose

The purpose of the Capacity Management Policy is to establish guidelines and procedures for managing information system capacity within Sudarshan, ensuring that resources are effectively and efficiently utilized to meet business demands while maintaining the integrity and availability of information. This plan ensures that IT resources are sufficient to meet business demands at Sudarshan.

Scope

This policy applies to all information systems and services within Sudarshan, encompassing hardware, software, networks, and associated resources. It applies to all employees, contractors, and third parties who have access to or are responsible for managing information system capacity, including all BTG resources such as hardware, software, network infrastructure, and personnel. Exceptions to this policy shall be approved by the BTG Head.

Responsibilities

The Business Technology Group and CISO are responsible for conducting regular capacity assessments, forecasting future capacity requirements, and planning for necessary enhancements. BTG is accountable for providing accurate and timely information related to the systems' capacity needs. The BTG will ensure that capacity management practices align with ISO 27001:2022 standards and that relevant controls are implemented and monitored. The responsibility for enforcing this plan lies with the Business Technology Group and CISO.

Policy

The Business Technology Group shall conduct periodic assessments of system capacity to identify and address potential bottlenecks or performance issues.

Capacity planning activities shall be conducted to anticipate future requirements based on business growth and technological advancements. Adequate resources, including hardware, software, and network bandwidth, shall be allocated to meet current and future capacity demands.

Continuous monitoring of system performance and capacity usage shall be conducted, with regular reporting to the head of BTG.

All capacity management activities, assessments, and plans shall be documented, including records of changes made to enhance capacity.

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

Plan

- **Capacity Planning**
  - Business Technology shall conduct capacity planning assessments annually to forecast future resource needs.
  - Key performance metrics shall be identified and monitored to assess current capacity and predict future requirements.

- **Monitoring and Reporting**
  - Business Technology should use monitoring tools to track system performance and utilization.
  - Quarterly capacity reports shall be generated and reviewed by BTG Management.

- **Resource Allocation**
  - Business Technology shall allocate resources based on the capacity planning assessments and monitoring reports.
  - Systems shall be scalable to accommodate increasing demands without compromising performance.

- **Capacity Management Review**
  - Every alternate week review meetings shall be conducted to discuss capacity management issues and update the plan as necessary.
  - The capacity management process shall be continuously improved based on feedback and changing business needs.

Procedure

- **Business Technology Operations Management**
  - A stable IT infrastructure must be designed and maintained. The following areas must be managed at a minimum:
    - Server environments
    - Networks
    - Storage and archiving
    - Databases
    - Desktops / Laptops
    - Backups
    - ISP Bandwidth
- **Server Environment**
  - Server equipment must be documented, and the following information must be maintained at a minimum:
    - Host contact information and location of server equipment.
    - Server hardware and operating system version and serial numbers.
    - Purpose/function of server equipment and applications.
    - Configuration information (server name, IP Address, and application-specific information).

All critical and security-related patches/hot-fixes released by vendors must be installed in accordance with Sudarshan's Patch Management Policy. Remote system administration (through privileged access) must be conducted using approved VPN secure solutions in accordance with Sudarshan's Remote Access Policy. All server event logs must be kept as per the log management policy.

- **Server Performance and Capacity Management**
  - Ensure that controlled processes are in place in the server environment and that equipment remains current with appropriate patches/hot fixes.
  - Disable all services and applications that are unused or are not serving business requirements, except when approved by the Administrator.
  - The Administrator must complete the Daily Operations Tasks Checklist.

- **Monthly Performance and Capacity Management Checklist**
  - Retain evidence of the completed and approved checklist(s).
  - Ensure server equipment configuration is documented, including host contact information, server hardware and operating system/version, purpose/function of server equipment and applications, configuration change management processes, backup requirements, Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and escalation procedures.
  - Ensure servers are named consistently according to the server and device naming conventions.

- **Monitor IT Infrastructure**
  - The Administrator must ensure monitoring for system alerts and failures capture the following details:
    - Alerts or messages from consoles.
    - Exceptions in system logs.
    - Alarms generated by network management devices.
    - Centralized logging system.

  - The Administrator must ensure monitoring for system access captures the following details:
    - The ID of the user.
    - The date/time of key events.
    - The type of event.
    - The files accessed and their type.
    - The programs or utilities used during access.

- **IT Infrastructure Capacity Planning Elements**
  - **Server CPU Utilization**: Monitor if CPUs are running at full capacity or being under-utilized to improve response time for applications.
  - **Server Disk Utilization**: Ensure critical processes on the server have sufficient system resources.
  - **Server Process Utilization**: Monitor memory and CPU utilization of processes to identify high resource usage.
  - **Network Availability**: Identify data bottlenecks or specific devices using more resources than expected.
  - **Network Traffic and Bandwidth Usage**: Monitor network interface traffic on the server.
  - **Network Devices (routers, switches, etc.)**: Ensure network devices are functioning as required.
  - **Event Logs and Key Indicators for Critical Systems and Applications**: Must be monitored by the Administrator using the Daily Operations Task Checklist.

- **Scheduled Capacity Assessments**
  - The Business Technology Group will schedule periodic capacity assessments based on the criticality and usage of information systems.
  - Assessments will include the evaluation of current resource utilization, performance metrics, and identification of potential bottlenecks.
  - The Business Technology Group will collaborate with department heads and system owners to gather information on anticipated business growth, technological advancements, and changes in information system usage.
  - Based on data gathered, the Business Technology Group will forecast future capacity requirements.
  - The Business Technology Group, in coordination with relevant stakeholders, will allocate adequate resources, including hardware, software, and network bandwidth, to meet current and future capacity demands.
  - Resource allocation decisions will be based on the findings from capacity assessments and forecasting activities.
  - Continuous monitoring tools will be employed to track system performance and capacity usage in real-time.
  - Quarterly reports summarizing capacity metrics, potential issues, and recommended actions will be generated and shared with BTG Head.

- All capacity management activities, including assessments, forecasts, and resource allocation decisions, will be documented.
- Records of changes made to enhance capacity, along with the rationale for those changes, will be maintained for auditing and review purposes.
- The Business Technology Group will conduct regular reviews of the capacity management process to identify areas for improvement.
- Based on reviews and feedback, adjustments to the capacity management procedure will be made to enhance its effectiveness.

17.6 Protection against malware

Anti-Virus / Anti-Malware Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.7

Purpose

The purpose of this policy is to establish guidelines and procedures for protecting Sudarshan's assets against attacks from destructive or malicious programs.

Scope

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

Policy

- All Sudarshan systems shall be protected by Sentinel One Anti-Virus with Managed Detection & Response (MDR) Service 24*7*365.
- Virus protection engines and/or versions shall be updated as and when they are released.
- Upon the release of upgrades/updates, all computer systems must get updated automatically.
- Anti-virus software shall scan all files introduced into its environment for viruses, hostile, and malicious code before they are used.
- All internet file transfers shall be scanned for viruses, hostile, and malicious code.
- System users shall not execute programs of unknown origin because they may contain malicious logic.
- Only licensed and approved software shall be used on Sudarshan's computing resources.

- All external storage media introduced to Sudarshan’s environment, such as removable disks and CD-ROMs, shall be scanned for potential threats (if any).
- The unauthorized development, transfer, or execution of viruses, hostile, and malicious code is prohibited.
- All users shall report any suspicious occurrences to the Business Technology Group immediately.

Procedures

- The Business Technology Group must install approved anti-malware software on all devices.
- Anti-malware software must be updated daily with the latest definitions.
- BTG must configure devices to perform full system scans weekly.
- Real-time scanning must be enabled to detect and block malware immediately.
- If malware is detected, BTG must isolate the affected system to prevent the spread.
- BTG must use anti-malware tools to remove the malware and restore the system to a secure state.

Guidelines for Anti-Virus Deployment

- **Enterprise-Wide Protection**
  - The organization shall have an enterprise-wide antivirus/malware protection to scan all assets within its infrastructure on a real-time basis and generate reports on a prescribed basis.
  - Proactive antivirus/malware protection shall be supported for all Windows operating systems installed on all BTG systems.
  - The requirements for an effective protection mechanism against malicious codes in all assets shall be addressed from the design to the installation stage.
  - The Business Technology Group shall be responsible for the design, implementation, management, and monitoring of antivirus protection mechanisms at the corporate and end-user levels.
  - The Business Technology Group shall take care of the license management of antivirus solutions within Sudarshan.

- **Installation and Configuration**
  - The antivirus/malware software shall be installed on Sudarshan's BTG assets, and users shall not be able to uninstall programs, change the configurations, or disable the scheduled scan on the system.

- Configuration parameters and auto-update settings are set correctly and not modified.
- Any external media devices are scanned by the BTG team before being given to the respective team.

- **Business Technology Group Responsibilities**
    - Endpoint protection client is installed on all individual machines and antivirus is installed on all production servers.
    - The endpoint protection client is configured to automatically update with the latest virus definitions from the cloud consol.
    - Endpoint protection is set to fully scan the system once a week.
    - Endpoint protection will have inbuilt protection against malware.
    - Antivirus uses a central mechanism to push the virus definitions on production-servers.
    - All systems are updated with the latest antivirus updates automatically.
    - The status of antivirus updates is monitored, and all systems are up to date.
    - A security incident is raised to identify the root cause and take corrective action in case of any virus or malware attack.
    - When a virus or malware is found in an incoming email, the email needs to be deleted and not notified either the sender or recipient. Instead, a notification is to be sent to the Business Technology Group for necessary action.

17.7 Management of technical vulnerabilities

Patch Management Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.8

Purpose

The purpose of this policy is to establish standard procedures for identifying, evaluating, mitigating vulnerabilities, and managing patches in the BTG environment at Sudarshan. This policy aims to enhance system security and repair application functionality.

Scope

This policy applies to all software, servers, desktops, laptops, IT systems, applications, network infrastructure, and network devices owned and operated by

Sudarshan. It is applicable to all employees, consultants, vendors, and other stakeholders.

Responsibility
The responsibility for enforcing these procedures lies with the BTG and CISO.

Policy

- **Vulnerability Management**
  - **Vulnerability Scanning:**
  - Regular scans shall be performed on all critical systems on a yearly basis using approved vulnerability scanning tools.
  - The Business Technology Group shall maintain an asset inventory to aid in patching efforts.
  - **Vulnerability Assessment:**
  - Identified vulnerabilities shall be evaluated based on their severity and impact.
  - A risk assessment shall be conducted to determine the potential impact on Sudarshan.
  - **Remediation:**
  - Patches shall be applied promptly to remediate identified vulnerabilities.
  - For vulnerabilities that cannot be immediately patched, mitigation steps shall be implemented to reduce risk.
  - **Reporting and Documentation:**
  - Detailed reports of identified vulnerabilities and remediation actions shall be documented.
  - A high-level summary shall be presented to senior management Annually.
- **Patch Management**

  General Guidelines:
  - All digital assets, systems, or services shall be patched and updated against security vulnerabilities.
  - The scope includes operating systems, applications, and program components.
  - Patches shall be checked for compatibility with all systems components prior to being applied.
  - Patches shall be successfully tested on non-production systems prior to being loaded on production systems.
  - All patches shall obtain the appropriate change control approval prior to deployment on a production system.

- Patching shall be performed during an authorized maintenance time window unless there is an urgent security requirement, and stakeholders should be notified accordingly.
- Critical system data shall be backed up prior to the installation of new patches.
- Depending on the severity of risk/vulnerability, the Business Technology Group will decide to shorten the tolerance time to reduce the risk.
- System patching shall only be performed by the System Administration Team.
- All server, desktop, and laptop systems, including all hardware and software components, shall be accurately listed in the Business Technology Group asset inventory to aid in patching efforts.
- Vulnerability scanning of systems shall take place at least once a year. Sudarshan shall use authorized tools to scan its systems for security vulnerabilities. Sudarshan's systems shall be scanned for vulnerabilities with the following frequency:
  - Servers shall be scanned once a year.
- Each vulnerability alert and patch release shall be checked against existing Sudarshan systems and services prior to taking any action to avoid unnecessary patching. All alerts shall be read very carefully – not all patches are related to issues or actual system versions present at Sudarshan.
- The decision to apply a patch and within what timeframe shall be done following the guidelines presented in the Patch Priority Matrix.
- All patches shall be downloaded from the relevant system vendor or other trusted sources. Each patch's source shall be authenticated, and the integrity of the patch shall be verified. All patches shall be submitted to an anti-virus scan upon download.
- New servers and desktops shall be fully patched before coming online to limit the introduction of risk.
- New software should be fully patched when installed on Sudarshan's resources to limit the introduction of risk.
- All patches shall be tested prior to full implementation since patches may have unforeseen side effects. Testing procedures shall be described using either a dedicated test network or non-critical machines.
- A back-out plan that allows safe restoration of systems to their pre-patch state shall be devised prior to any patch rollout in the event that the patch has unforeseen effects.
- Audits shall be performed yearly to ensure that patches have been applied as required and are functioning as expected.

Windows Patch Management:

- Desktop central server manages patches for desktops and laptops.
- Deployment of patches is scheduled twice a week for desktops and laptops and for server monthly basis.
- The Business Technology Group monitors the deployment of patches as per the schedule.
- In case of deployment failures, the BTG team deploys the patches manually.

Application Patches:

- The vendor application team is responsible for managing application patches, such as Tally on the cloud and the website.
- The website vendor provides feedback and test results to the Business Technology Group.

Procedures

- All server, desktop, and laptop systems, including hardware and software components, must be accurately listed in the Business Technology Group asset inventory.
- New servers and desktops must be fully patched before coming online to limit the introduction of risk.
- New software must be fully patched when installed on Sudarshan’s resources.
- All patches must be downloaded from relevant system vendors or other trusted sources, authenticated, and their integrity verified.
- All patches must be submitted to an anti-virus scan upon download.
- Patches must be tested prior to full implementation using either a dedicated test network or non-critical machines.
- A back-out plan must be devised before any patch rollout to allow safe restoration of systems to their pre-patch state in case of unforeseen effects.
- The rollout of tested patches will adhere to a tiered procedure, including all automated systems used.
- All configuration and inventory documentation must be immediately updated to reflect applied patches.
- Yearly audits will be performed to ensure patches have been applied as required and are functioning as expected.

17.8 Storage Media Policy

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 – Control 5.15, 5.18, 5.9, 5.10, 5.11

Purpose

The purpose of this policy is to ensure the secure handling, storage, and disposal of storage media that contain sensitive or confidential company data. This policy aims to prevent unauthorized access, data breaches, and loss of data.

Scope

This policy applies to all employees, contractors, and third-party vendors who handle any form of storage media including, but not limited to, hard drives, USB drives, CDs, DVDs, magnetic tapes, cloud storage services, and mobile devices.

Definitions

- Storage Media: Devices or locations used to store digital information (e.g., hard drives, USB sticks, optical discs, cloud storage).
- Sensitive Data: Information classified as confidential, proprietary, or sensitive to Sudarshan or its clients.
- Authorized Users: Individuals granted access to sensitive data stored on company storage media.

Policy Statements

1. Usage Guidelines

- Only authorized personnel are allowed to access, copy, or distribute sensitive data from storage media.
- Sensitive data should be stored only on company-approved devices or cloud services. Personal devices should not be used for company data storage unless explicitly authorized.

2. Access Control

- Access to storage media must be restricted based on user roles and responsibilities.

- Physical storage media must be kept in a secure, locked environment when not in use, with access limited to authorized personnel.

3. Data Transfer

- Sensitive data should not be transferred via unapproved storage media or channels.
- For data transfers, only secure methods (e.g., email, OneDrive) should be used.

4. Disposal of Storage Media

- When storage media are no longer in use or are being decommissioned, they must be securely erased or physically destroyed to prevent data recovery.
- A log must be maintained by all disposed storage media, including the method of disposal.

Cloud Storage

- Only authorized OneDrive cloud services should be used for storing company data.
- Access to cloud storage must be managed with strong passwords and multi-factor authentication (MFA).

Incident Reporting

- Any loss, theft, or unauthorized access to storage media must be reported immediately to the BTG Team.
- Incidents will be investigated to determine if a data breach has occurred, and appropriate measures will be taken to mitigate any impact.

Policy Compliance

- Non-compliance with this policy may result in disciplinary action, including termination of employment or contract, depending on the severity of the violation.
- Regular Review will be conducted to ensure compliance with this policy.

Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in technology, regulations, or company practices.

17.9 Information Deletion

Information Deletion Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.10

Purpose

The purpose of this policy is to ensure that information and data are securely deleted from Sudarshan’s systems and storage devices to prevent unauthorized access and ensure compliance with data protection regulations.

Scope

This policy applies to all data and information stored on company-owned devices, servers, and storage media. It includes data managed by employees, contractors, and third-party service providers.

Responsibility

The responsibility for enforcing this policy lies with the Business Technology Group, under the oversight of the Chief Information Security Officer (CISO).

Policy

- Data that needs to be deleted shall be identified and classified based on retention schedules and business requirements.
- The Business Technology Group shall identify and classify data according to Sudarshan's data classification policy.
- Data owners shall review and confirm the classification and retention schedules of their data.
- Secure deletion methods, such as data wiping or degaussing, shall be utilized for electronic data.
- The Business Technology Group shall utilize industry-standard secure deletion methods, such as data wiping or degaussing, for electronic data.
- Verification of the deletion process shall be conducted and recorded.
- Physical media shall be destroyed when no longer needed.
- Physical media containing sensitive information shall be shredded, incinerated, or destroyed using other secure methods.
- Documentation of the destruction process shall be maintained.

- All data shall be securely deleted from equipment before disposal or reassignment.
- The Business Technology Group shall ensure all data is securely deleted from equipment before it is disposed of or reassigned. A certificate of e-waste shall be obtained and filed for record-keeping.
- Third-party service providers should follow secure data deletion practices and provide proof of deletion when required. Third-party service providers handling company data shall be required to follow secure deletion practices.
- Proof of deletion should be provided by third-party service providers and retained for auditing purposes.
- The Compliance Team shall ensure adherence to all legal, regulatory, and contractual data deletion requirements.

Procedure

- **Data Identification and Classification**
  - Identify data eligible for deletion based on the business requirements.
  - Classify data according to sensitivity and confidentiality.
- **Secure Deletion Process**
  - For electronic data, use data wiping software that meets industry standards.
  - For physical media, we use shredding or degaussing methods for destruction.
- **Documentation and Reporting**
  - Document the deletion process and retain records for auditing purposes.
  - Report on completion of data deletion to the BTG Head and CISO.
- **Verification**
  - Verify that deleted data is unrecoverable using appropriate tools and techniques.
  - Review and update procedures annually or as needed.

17.10 Information Backup

Backup & Restoration Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.13

Purpose

The purpose of this policy is to maintain the integrity and availability of information and information processing facilities at Sudarshan to ensure that all essential business information and software can be recovered in the event of an application failure/malfunction, data corruption, media failure, or disaster. This policy is intended to provide guidelines for data backup and retrieval operations, ensuring Sudarshan meets business objectives and maintains the viability of its IT & IS assets.

Scope

This policy applies to all users, including those affiliated with third parties and outsourced parties who own and have access to Sudarshan's IT and IS assets.

Responsibility

- **Business Technology Group**: Responsible for implementing and managing the backup processes, ensuring that all data backups are conducted as per the defined schedule, and regularly testing restoration procedures.
- **Backup Administrator**: Responsible for managing backup operations, monitoring backup logs, troubleshooting issues, and ensuring successful data recovery during tests and actual events.
- **Data Owners**: Responsible for identifying critical data that needs to be backed up.
- **CISO**: Responsible for providing support and resources for effective backup management and ensuring compliance with this policy across Sudarshan.

Policy

Sudarshan recognizes that the backup and maintenance of data are critical to the viability and operations of IT & IS assets in meeting business objectives.

The following policies must be adhered to:

- All business essential data shall be included in the backup process. Business essential data include, but are not limited to:
  - Project Data
  - Financial Data
  - HR Data
  - Admin Data
  - IT Support Data
  - Email Data
  - Production Data
  - SAP Data

  - Third-Party Software
- Backups shall be conducted according to an approved schedule, including daily email backups and monthly backups stored off-site for disaster recovery.
- Backups shall be stored on approved media in a safe and controlled environment, accessible only to authorized personnel.
- All backed-up devices shall be labelled and stored securely. Off-site storage shall be used to ensure availability in case on-site backups become inaccessible.
- Non-SAP Backups shall be tested half yearly, and SAP Backups shall be tested annually for reliability and data integrity.
- Backup logs shall be maintained as per the log management policy, and backup restoration tests shall be performed periodically according to the criticality of the data.
- Full backups shall be retained as per the approved retention period. Backup data shall be deleted when no longer needed, following secure disposal procedures.
- The retention periods for backups are defined as follows:

Backup Type	Retention Period
Daily Backup	7 days

- A data restore request shall be raised by authorized personnel (Data Owner/Management) via the ticketing system.
- Backup restoration shall be completed in accordance with the approved recovery time objectives (RTO) and recovery point objectives (RPO).
- The Backup Policy does not apply to Cloud Applications, as these are managed under separate service agreements with third-party providers.

Procedure

- **General**
  - All application and operating systems software, data (including databases), configuration information (like hardware configuration information where applicable), and log files/logs that need to be backed up shall be identified and documented.
  - The frequency of backup, medium of backup, and storage of the backup shall be identified and documented. This must be in accordance with the importance of the information and the acceptable risk as determined by the BTG.
  - The team involved shall ensure that all backups are completed successfully, and periodic reviews of the backup process shall be conducted for all in-scope assets.
  - Logs shall be maintained to verify the amount of data backed up and record any failed backup occurrences.

  - The Business Technology Group, including the backup administrator, shall be responsible for performing backup management of in-scope IT assets.
  - The team shall identify problems and take corrective actions to reduce any risks associated with failed backups. They should maintain records demonstrating the review of logs and test restores.

- **Backup Scope**
  - The scope of the backup shall include all critical systems, applications, and data necessary for Sudarshan's operations.
  - The backup scope should be reviewed and updated regularly to ensure that any changes in the IT environment or data requirements are addressed promptly.

- **Backup Scheduling**
  - Backup schedules shall be established to minimize disruptions to business operations and ensure data integrity.
  - Backups shall occur every day after regular business hours, following the defined schedule.

- **Backup Schedule**
  - Daily incremental or differential backups of all application and operating systems software, data (including databases), configuration information (like hardware configuration information where applicable), and log files/logs shall be conducted.
  - Weekly full backups shall be taken. Full backups shall also be conducted before and soon after any major changes to hardware, operating systems, applications, or configurations, including the following scenarios:
    - Upgrade of operating systems, applications, or critical patches.
    - Installation of new application components.
    - Before and after the execution of a critical process.

- **Backup Restoration**
  - Backup restoration procedures shall be developed and tested to ensure timely and reliable recovery of data in the event of a failure or disaster.
  - Restoration tests shall be conducted periodically to validate the effectiveness of backup processes and identify areas for improvement.
  - Documentation of successful and unsuccessful restoration attempts shall be maintained and reviewed regularly to ensure the continuous improvement of the backup process.

17.11 Logging

Log Management Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.15

Purpose

The purpose of this policy is to ensure that all logs generated by Sudarshan's information systems and infrastructure are collected, managed, and analyzed to support security monitoring, troubleshooting, and compliance efforts.

Scope

This policy applies to all information systems, applications, network devices, and other infrastructure components that generate logs at Sudarshan.

Responsibility

- **Business Technology Group**: Responsible for implementing and maintaining the log management infrastructure, monitoring and analyzing log data for security incidents and compliance, and for ensuring that logs are generated and properly forwarded to the log management system.

Policy

- All critical systems, applications, and network devices shall generate logs for security, operational, and compliance purposes.
- Logs shall be collected in a centralized log management system to ensure availability for analysis and compliance.
- Logs shall be stored securely to prevent unauthorized access, modification, or deletion.
- Retention periods for log data shall be defined based on business, legal, and regulatory requirements.
- Logs shall be monitored and analyzed regularly to detect security incidents, operational issues, and compliance violations.
- SIEM tools shall be used to automate log analysis and generate alerts for suspicious activities.
- Access to log data shall be restricted to authorized personnel only.

- Log management practices shall comply with all applicable legal, regulatory, and contractual requirements.
- All log management activities, including configuration, storage, analysis, and incident response, shall be documented.
- Documentation of log management procedures shall be maintained for audit and review purposes.
- Updates to the policy shall be documented and communicated to all relevant stakeholders.

- Logs shall be reviewed as per the requirement of the business in the following manner:
  - Firewall Logs – Monthly
  - Antivirus Logs – Weekly and as per the incident
  - Operating System Logs (Server) – Weekly
  - Server Logs, Backup Logs, Application Logs – Monthly

- The following Firewall Events shall be configured for logging and monitored by the System Administrator:
  - ACL violations
  - Invalid user authentication attempts
  - Logon and actions taken by any individual.
  - Configuration changes made to the firewall.

- The following Operating System Logs shall be reviewed:
  - Any additions, modifications, or deletions of user accounts
  - Any failed or unauthorized attempt at user logon
  - Any modification to system files
  - Any access to the server or application running on the server.
  - Actions taken by any individual with administrative privileges.
  - Any user access to audit trails
  - Any creation or deletion of system-level objects installed by Windows.

- The following Antivirus Logs shall be reviewed:
  - Alerts generated by antivirus software.
  - Quarantine folder/files.
  - Whitelist of folders

- Any deviations shall be reported to the Business Technology Group or CISO immediately.
- Logs shall be maintained or retained for the period of one year on individual applications. Logs shall be backed up while refreshing applications.

Procedure

- **Log Generation and Collection:**
  - Identify critical systems, applications, and network devices that need to generate logs.
  - Configure these systems to generate logs and forward them to the centralized log management system.

- **Log Storage:**
  - The store logs in a centralized log management system.
  - Implement access controls and encryption to secure stored logs.
  - Define and implement retention periods for different types of log data based on business, legal, and regulatory requirements.

- **Log Analysis and Monitoring:**
  - Set up regular monitoring and analysis schedules.
  - Configure SIEM tools to generate alerts for suspicious activities and potential security incidents.
  - Establish a process for responding to alerts and security incidents identified through log analysis.
- **Access Control:**
  - Restrict access to log data to authorized personnel only.
  - Maintain audit trails of access to log data.
  - Review and update the log management policy and procedures annually or as needed.

- **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	30 Days
5	Antivirus Logs	90 Days

17.12 Monitoring Activities

Monitoring Management Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.16

Purpose

The purpose of this policy is to ensure that monitoring activities are effectively implemented to detect and respond to security incidents, compliance violations, and operational issues within Sudarshan's information systems and infrastructure.

Scope

This policy applies to all information systems, applications, network devices, and other infrastructure components within Sudarshan.

Responsibility

- **Business Technology Group**: Responsible for implementing and maintaining monitoring tools and systems, for monitoring, analyzing, and responding to security incidents and compliance violations, and for ensuring that monitoring configurations are correctly implemented and maintained.

Policy

- Monitoring tools and systems shall be implemented to continuously observe information systems, applications, network devices, and other infrastructure components.
- Logs from critical systems and applications shall be collected and analyzed using SIEM tools to detect suspicious activities and potential security incidents.
- Access to monitoring data and tools shall be restricted to authorized personnel only.
- Monitoring activities shall support the identification and response to security incidents in a timely manner.
- Monitoring practices shall be reviewed and updated regularly to ensure their effectiveness and to incorporate new threats and technologies.

Procedure

- **Monitoring Implementation:**
  - Identify critical systems, applications, and network devices that require monitoring.
  - Configure monitoring tools and systems to continuously observe identified components.

- **Log Collection and Analysis:**
  - Aggregate logs from critical systems and applications in a centralized SIEM system.
  - Analyze collected logs for suspicious activities, potential security incidents, and compliance violations.
  - Configure the SIEM system to generate alerts for detected anomalies and incidents.

- **Access Control:**
  - Restrict access to monitoring data and tools to authorized personnel only.
  - Maintain audit trails of access to and usage of monitoring data.

- **Incident Response:**
  - Use monitoring data to detect security incidents and compliance violations.
  - Follow established incident response procedures to address detected incidents promptly.
  - Document all detected incidents and the corresponding response actions taken.
  - Maintain documentation of monitoring configurations, detected incidents, response actions, and audit results.

17.13 Installation of Software on Operational Systems

Software Installation Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.18, 8.19

Purpose

The purpose of this policy shall be to outline the requirements around installing software on Sudarshan's computing devices to minimize the risk of loss of program functionality, exposure of sensitive information contained within Sudarshan's computing network, the risk of introducing malware, and legal exposure from running unlicensed software.

Scope

This policy applies to all Sudarshan employees, contractors, vendors, and agents with Sudarshan-owned devices. This policy should cover all computers, servers, and other computing devices operating within Sudarshan.

Policy

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

Software requests shall first be approved by the Team Leader/System Administrator and then be made to the BTG or Help Desk in writing or via email.

Software shall be selected from an approved software list, maintained by the BTG, unless no selection on the list meets the requester's need.

The BTG will obtain and track the licenses, test new software for conflicts and compatibility, and perform the installation/removal depending on the result.

17.14 Networks Security

Network Security Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.20, 8.21, 8.22

Purpose

The purpose of this policy is to ensure the security and integrity of Sudarshan's network infrastructure by implementing robust security measures and practices.

Scope

This policy applies to all network infrastructure components, including but not limited to routers, switches, firewalls, and wireless access points, within Sudarshan.

Responsibility

- **Business Technology Group**: Responsible for implementing and maintaining network security measures, for configuring and managing network security devices and protocols, and for monitoring network security and responding to incidents.

Policy

- All network infrastructure components shall be configured and maintained to ensure the highest level of security.
- Network security measures shall include, but are not limited to, firewalls, intrusion detection/prevention systems (IDS/IPS), and secure access controls.
- Network services shall be protected against unauthorized access, misuse, and disruption.
- Access to network services shall be restricted to authorized personnel only.
- Network segments shall be created to separate sensitive information and systems from less critical or public areas.
- Virtual LANs (VLANs) and other segmentation techniques shall be used to enforce segregation.
- Access controls should be implemented to restrict traffic between network segments based on security policies.
- Maintain documentation of network configurations, security policies, detected incidents, and audit results.
- This policy and procedure shall be reviewed annually or as needed to ensure relevance and effectiveness.
- Updates to the policy shall be documented and communicated to all relevant stakeholders.

Procedure

- **Networks Security:**
  - **Configuration**: Configure firewalls, IDS/IPS, and other network security devices to protect the network perimeter and internal segments.
  - **Access Control**: Implement strong access control measures, including multi-factor authentication and role-based access controls, for network devices.
  - **Monitoring**: Continuously monitor network traffic and security logs for signs of suspicious activity.
- **Security of Network Services:**
  - **Encryption**: Use encryption protocols such as SSL/TLS to protect data transmitted over the network wherever applicable.

  - **Authentication**: Require secure authentication methods for access to network services.
  - **Patching**: Regularly update and patch network services to protect against known vulnerabilities.
- **Segregation of Networks:**
  - **Segmentation**: Implement VLANs and other network segmentation techniques to separate sensitive systems and data.
  - **Access Control Lists (ACLs)**: Use ACLs to control traffic flow between network segments based on security policies.
  - **Regular Review**: Regularly review and update network segmentation and access controls to ensure effectiveness.
- **Incident Response:**
  - **Detection**: Use monitoring tools to detect network security incidents.
  - **Response**: Follow established incident response procedures to address network security incidents promptly.
  - **Documentation**: Document all network security incidents and the corresponding response actions taken.

17.15 Web Filtering

Web Filtering Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.23

Purpose

The purpose of this policy is to ensure that web access within Sudarshan is controlled and monitored to protect against security threats and to ensure compliance with company policies and requirements.

Scope

This policy applies to all employees, contractors, and third-party service providers who access the internet using Sudarshan's network and devices.

Responsibility

- **Business Technology Group**: Responsible for implementing and managing web filtering technologies and monitoring web filtering logs and responding to security incidents.

- **Employees**: Responsible for adhering to web filtering policy and reporting any issues or violations.

Policy

- Sudarshan shall implement web filtering solutions to control access to websites and online content.
- Access to certain categories of websites, including malicious and inappropriate content, shall be restricted.
- Web usage shall be monitored, and access logs shall be reviewed regularly to ensure compliance with this policy.
- Exceptions to the web filtering policy shall be granted only with approval from the Business Technology Group head or CISO.
- This policy and procedure shall be reviewed annually or as needed to ensure relevance and effectiveness.
- Updates to the policy shall be documented and communicated to all relevant stakeholders.

Procedure

- **Web Filtering Implementation:**
  - **Selection of Web Filtering Solution**: Choose an appropriate web filtering solution that meets the security and operational requirements of Sudarshan.
  - **Configuration**: Configure the web filtering solution to block access to categories of websites that are deemed malicious or inappropriate.

- **Access Control:**
  - **Block Lists**: Maintain and regularly update block lists to prevent access to known malicious websites and inappropriate content.
  - **Allow Lists**: Create allow lists for websites that are essential for business operations and have been verified as safe.
  - **User Groups**: Define user groups and apply different web filtering policies based on job roles and responsibilities.

- **Monitoring and Reporting:**
  - **Web Usage Monitoring**: Monitor web usage logs to detect attempts to access blocked content or other suspicious activities.
  - **Regular Reviews**: Conduct regular reviews of web filtering logs to ensure compliance and identify any potential security threats.

  - **Incident Response**: Respond promptly to any detected security incidents or policy violations related to web filtering.

- **Exceptions:**
  - **Request Process**: Establish a formal process for requesting exceptions to the web filtering policy, including a justification for the request and necessary approvals.
  - **Approval**: Obtain written approval from the Business Technology Group or senior management for any exceptions granted.
  - **Documentation**: Document all granted exceptions and review them periodically to ensure continued relevance and necessity.

17.16 Use of Cryptography

Cryptographic Controls Policy & Procedure

This section covers compliance of following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.24

Purpose

The primary purpose of this document is to establish a system for the usage of cryptographic controls to be resilient against known attacks and sufficient to protect assets of Sudarshan. The use of encryption techniques is to protect sensitive data both at rest and in transit. This document defines the controls and related procedures for the various areas where encryption and other cryptographic techniques are employed.

Scope

Cryptographic controls are used to achieve different information security objectives:

- **Confidentiality**: Using encryption of information to protect sensitive or critical information either stored or transmitted.
- **Non-Repudiation**: Using cryptographic techniques to provide evidence of the occurrence of an event or action.
- **Authentication**: Using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities, and resources.

Responsibility

- **CISO**: Responsible for approving and maintaining the policy. Accountable for ensuring compliance with the policy and overseeing its implementation.
- **Business Technology Group**: Responsible for implementing and managing cryptographic controls according to the policy. Accountable for ensuring that encryption mechanisms are properly configured and maintained.
- **All Employees**: Responsible for adhering to the policy and using cryptographic controls appropriately. Accountable for safeguarding sensitive information and following encryption procedures outlined in the policy.

Policy

The policy followed at Sudarshan for cryptographic controls is:

- The use of encryption shall be considered whenever the confidentiality of an asset is important.
- Data encryption must be enabled where applicable.
- The use of digital signatures or hash functions shall be considered when considering encryption.
- Strong cryptographic algorithms shall be used.
- Key management shall be in place. Keys shall be generated securely, stored securely, and destroyed when no longer needed.
- All keys shall be randomly generated using a secure random number generator. Keys shall never be stored in source code.
- **Encryption for End Users**
  - Laptops
    - It is recommended that Bit locker be used for Encrypting Laptop Disk.
  - Application and Database Servers
    - IPSEC VPN is used to connect Data Center – Application & Database Server.
  - Use of Digital Signature Certificates
    - Sudarshan uses Digital signatures for statutory compliance.
    - The finance team is responsible for managing Digital signatures.
  - Encryption is used for.
    - The transport of sensitive files (secure FTP and VPN usage to encrypt sensitive data for network file access of unencrypted files).
    - The website is protected using HTTPS encryption.
    - SSH is used for remote access to the virtual environment through a VPN and PAM 360.

18 System Acquisition, Development, And Maintenance

18.1 Outsourced Development Policy

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Clause 6.1.2, Control 5.15, 6.6, 8.30, 8.31

Purpose

The purpose of this policy is to define the standards and procedures for engaging with external vendors for outsourced development projects. This policy ensures that all outsourced development is conducted securely, efficiently, and in alignment with Sudarshan's business goals and regulatory requirements.

Scope

This policy applies to all Sudarshan departments, employees, and project managers who engage with external vendors for the purpose of software development, system maintenance, quality assurance, or any other development-related activities. This policy covers all stages of the outsourced development lifecycle, from vendor selection to project completion and termination.

Vendor Selection Criteria

All vendors must meet the following criteria:

- Technical Competence: Vendors must have documented experience and expertise in the required technology stack and project domain.
- Compliance Standards: Vendors must comply with Sudarshan's data security policies and applicable industry regulations.
- Reputation and References: Vendors must provide verifiable references and demonstrate a positive reputation in the industry.
- Financial Stability: Vendors must provide evidence of financial stability to ensure continuity of service throughout the project lifecycle.
- All vendor selections must be approved by BTG Head following a thorough evaluation of these criteria.

Contractual Requirements

All outsourcing contracts must include the following provisions:

- Scope of Work (SOW): A detailed SOW, including deliverables, timelines, milestones, and quality standards.

- Intellectual Property (IP) Rights: Sudarshan retains full ownership of all IP developed during the project.
- Confidentiality: A Non-Disclosure Agreement (NDA) must be signed by the vendor before any project work commences.
- Termination Clause: Clear terms for contract termination, including conditions and procedures for handling incomplete work or assets, must be defined.

Security and Access Control

Vendors will only be granted access to the systems and data necessary for their tasks. Access levels will be defined by CISO. Vendors must adhere to Sudarshan's cybersecurity standards, including:

- Secure Access Protocols: All remote access must be secured using VPNs, multi-factor authentication, and strong password policies.
- Data Protection Compliance: Vendors must comply with all data protection regulations relevant to the project, including secure data storage requirements.

Project Management and Communication

- Project Manager Assignment: Sudarshan will assign an internal Project Manager to oversee vendor activities, monitor progress, and facilitate communication.
- Status Reporting: Vendors are required to provide weekly progress reports and attend scheduled meetings as defined by the Project Manager.
- Performance Metrics: Vendors will be evaluated based on established Key Performance Indicators (KPIs), including project timelines, quality of deliverables, and adherence to security protocols.

Quality Assurance and Testing

All development deliverables must meet Sudarshan's quality standards. The following quality assurance measures are mandatory:

- Code Review and Testing: Vendors must conduct unit testing, integration testing, and code reviews before submitting deliverables.
- Acceptance Testing: Sudarshan will perform final acceptance testing based on predefined criteria. Deliverables that fail to meet the acceptance criteria will be rejected until rectified.

Confidentiality and Data Handling

Vendors must adhere to the following confidentiality and data handling practices:

- Data Access and Storage: Vendors are prohibited from accessing or storing sensitive data beyond project requirements and must follow Sudarshan's data Storage Policy.
- Post-Project Data Disposal: Upon project completion or termination, vendors must securely delete all project-related data from their systems and provide a certificate of data destruction.

Dispute Resolution

In the event of a dispute, the following resolution process shall be followed:

- Initial Resolution: Disputes will first be addressed through direct negotiation between Sudarshan and the vendor.
- Mediation: If direct negotiation fails, the matter will be escalated to mediation as outlined in the contractual agreement.
- Jurisdiction: All legal proceedings will be conducted under the jurisdiction specified in the contract.

Termination and Exit Procedures

Upon termination of the vendor relationship, the following steps will be taken:

- Exit Plan: The Project Manager will oversee a structured exit plan, including knowledge transfer, documentation handover, and system access revocation.
- Post-termination Obligations: Vendors must provide post-termination support during the transition period as defined in the contract.

Policy Review and Compliance

This policy will be reviewed annually by CISO to ensure it remains up-to-date and in compliance with Sudarshan's objectives and regulatory requirements. Any violation of this policy may result in disciplinary actions, including termination of the vendor relationship.

18.2 Change Management

Change Management Policy & Procedure

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Control No. 8.32

Purpose

The purpose of this Change Management Policy and Procedure is to ensure that all changes to Sudarshan information systems, infrastructure, and business processes are conducted in a controlled and coordinated manner. This policy aims to minimize the risk of disruption, maintain service quality, and comply with relevant regulatory requirements.

Scope

This policy applies to all employees, contractors, and third-party service providers involved in the implementation, management, and support of changes to Sudarshan's IT systems and infrastructure. This policy is applicable to all functions at Sudarshan and shall be used by all functions/employees requesting changes within Sudarshan. This policy is applicable for changes in the production environment of IT applications and IT infrastructure owned and managed by Sudarshan including new application procurements / Application as a Service.

This policy does not apply to changes and releases at an operational level (e.g., repair to printers or other routine service components).

Definitions

- **Change:** Any modification to the IT infrastructure, systems, applications, or business processes.
- **Change Request (CR):** A formal proposal for a change to be made.
- **Emergency Change:** A change that shall be implemented immediately to resolve a critical issue.

Roles and Responsibilities

- **Change Requester:** Initiates the change request and provides necessary details.
- **Change Manager:** Oversees the change management process and ensures compliance with the policy.
- **Implementer:** Executes the approved change.
- **Tester:** Validates that the change has been implemented correctly and without issues.

Policy

Sudarshan is committed to managing changes in a structured manner to ensure that changes are planned, tested, approved, implemented, and reviewed efficiently and effectively. All changes shall be documented, reviewed, and authorized according to this policy.

The policy followed at Sudarshan for change management is:

- All changes to Sudarshan's IT infrastructure and applications shall undergo a formal change management process.
- Changes shall be initiated through a formal Change Request (CR) process, documented, reviewed, and authorized by the relevant approving authority, based on the requirement, inter-dependency, compliance, and potential impact on Sudarshan’s business operations.
- Major changes require approval from BTG Head.
- All changes affecting IT & IS assets and supporting processing facilities must be authorized by the relevant approving authority.
- A comprehensive impact analysis and rollback plan must be prepared for all changes.
- All changes shall be tested in a non-production environment before being implemented in the production environment to ensure their stability and effectiveness.
- All changes shall be documented, including impact and rollback analyses, and maintained in a formal change management log.
- Implementation scheduling information for approved changes shall be maintained and communicated to relevant stakeholders.
- The Change Request Form shall be used to document all requested changes, including those that are unscheduled or emergency changes.
- Provisions shall be made for emergency changes, enabling quick and controlled implementation of changes needed to resolve incidents.
- Emergency changes shall be documented, reviewed, and included in the change management log.
- Development/test and operational environments shall be kept separate to prevent unauthorized access or changes to information assets.
- Any unauthorized changes shall be reported to the CISO for appropriate action.

Procedure

The following guidelines are to be considered while raising a change request:

Step	Description	Responsibility
1.	Change Initiator to raise a CR by completing the CR form/tool.	Change Initiator
2.	The relevant stakeholder/HOD to verify the CR for completion	HOD

3.	HOD to verify: • Change urgency. • Change impact analysis. • Change priority	HOD
4.	CISO will approve CR and communicate to all stakeholders	CISO
5.	Change to be implemented as per the decided timelines	Business Technology Group
6.	If the change is not successful, the respective team would have to roll back or resolve the problem.	Business Technology Group
7.	Business Technology Group will conduct Post Implementation Review as per the criticality of the change if required	Business Technology Group

Emergency Change Process

- Emergency changes follow an expedited process due to their critical nature.
- The Change Manager or designated authority shall approve emergency changes.
- Emergency changes must be documented and reviewed by the MRC.

19 Cyber Crisis Management Plan

This section covers compliance with the following ISO Standards Clause & Control requirements:

- ISO 27001:2022 - Clause 6.1.3

Introduction

As a chemical manufacturing entity, Sudarshan’s is exposed to a range of cybersecurity threats that can affect production, safety, and compliance. Since cyber risks can disrupt business continuity in unique ways, this plan is designed to guide the company in managing any crisis arising from cyber threats. The CCMP will ensure that Sudarshan Chemicals promptly detects and responds to cyber incidents, minimizes business impacts, and recovers efficiently.

Purpose

The primary purpose of this plan is to:

- Detect any cyber intrusions swiftly.

- Respond effectively to cyber-attacks (e.g., malware, ransomware, and industrial espionage).
- Recover critical business operations, focusing on production, supply chains, and compliance.
- Contain the damage and prevent its spread across the organization.

Scope

The plan covers all operations of Sudarshan's, including production facilities, research labs, and administrative offices. A cyber crisis may result in serious harm to safety, production halts, environmental risks, and loss of sensitive data (formulas, intellectual property).

Cybersecurity Threats

Sudarshan is particularly vulnerable to:

- Industrial Espionage: Theft of formulas and R&D data.
- Phishing & Spear Phishing: Targeted attacks on employees.
- Ransomware: Locking critical systems, halting production.
- DDoS Attacks: Disruptions to plant operations and safety systems.
- SCADA System Attacks: Manipulating industrial control systems to disrupt manufacturing.
- Data Breaches: Unauthorized access to client and partner data.

Cyber Crisis Management Team (CCMT)

A Cyber Crisis Management Team is established, composed of:

- Crisis Coordinator: BTG Head or CISO
- Production Management: Ensure plant safety and continuity.
- Research & Development: Safeguard intellectual property.
- Compliance and Legal: Address any regulatory breaches or violations.
- BTG Department: Isolate and contain affected systems.
- HR Department: Handle internal communication and employee support.
- External Experts: Engage third-party cybersecurity consultants for specialized forensics or incident response.

Cyber Crisis Phases

1. Readiness and Detection

- 24/7 monitoring of systems.
- Employee training and awareness programs.
- Periodic security assessments of critical systems.

2. Response

- Immediate isolation of affected systems (disconnecting compromised networks or disabling user access).
- Coordination with external forensic experts for containment and analysis.
- Communication strategy to inform stakeholders without damaging the company's reputation.

3. Recovery

- Restore affected systems using clean backups.
- Rebuild compromised systems from scratch if needed.
- Review and strengthen the disaster recovery plan to ensure quick resumption of production.

4. Reporting

- Internal reports to the Board and external regulatory reports to government bodies (environmental safety, compliance).
- Customer and partner notification, especially if data breaches or delays in deliveries occur.

5. Prevention

- Implement lessons learned from each incident.
- Regularly update security policies and the CCMP.

Roles and Responsibilities

- BTG Head / Crisis Coordinator: Initiates the crisis response, coordinates efforts, and communicates with top management.
- Instrumentation Team: Ensures Cyber safety protocols are in place to prevent any harm in SCADA systems.
- Legal and Compliance: Ensures regulatory compliance and handles legal matters related to breaches.
- HR: Handles employee-related issues and ensures correct internal communication.

Escalation Matrix

- 0-30 minutes: BTG Head/CISO and Production Lead informed of the incident.
- 30-60 minutes: Crisis escalated to Top Management.

20 Additional Policy & Procedures

20.1 Bring Your Own Device (BYOD) Policy

Purpose

The primary purpose of this policy provides guidelines, standards, and rules of behavior for the use of personally owned smartphones, tablets, and laptops by Sudarshan employees to access Sudarshan's resources and services. Access to and continued use of these devices shall be granted on the condition that each user reads, signs, and complies with Sudarshan's policies concerning the use of these resources and services.

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

Scope

This Bring Your Own Device Policy shall be applicable to all employees of Sudarshan contractors, vendors, and any other person using or accessing information or information systems of Sudarshan. Exceptions to this policy shall be approved by the BTG Head.

Policy

- **Acceptable Use**
  - Sudarshan shall define acceptable business use as activities that directly or indirectly support the business of Sudarshan.
  - Sudarshan shall define acceptable personal use in company time as reasonable and limited personal communication or recreation, such as reading or game playing.
  - Devices shall not be used at any time to:
    - Store or transmit illicit materials.
    - Store or transmit proprietary information.
    - Harass others.
    - Engage in outside business activities.
  - Employees shall use their mobile devices to access the following company-owned resources:
    - Email
    - Teams
    - One Drive for Business

  - Sudarshan shall enforce a zero-tolerance policy for texting or emailing while driving; only hands-free talking while driving shall be permitted.

- **Devices and Support**
  - The following devices shall be supported:
    - iPhone version 17 and above
    - iPad version 15 and above
    - Android version 13 and above
  - Employees shall contact the device manufacturer or their carrier for operating system or hardware-related issues.

- **Security**
  - To prevent unauthorized access, devices shall be password protected using the features of the device, and a strong password shall be required to access Sudarshan network.
  - The device shall lock itself with a password or PIN.
  - Rooted (Android) or jailbroken (iOS) devices shall be strictly forbidden from accessing the network.
  - Smartphones and tablets that are not on Sudarshan's list of supported devices shall not be allowed to connect to the network.
  - Smartphones and tablets belonging to employees that are for personal use only shall not be allowed to connect to the network.
  - Employees shall be responsible for patch updates of these devices.
  - Employees' access to company data shall be limited based on user profiles defined by the Business Technology Group and automatically enforced by Mobile Device Management software.
  - All employees who are provided with access to company-owned resources through Mobile Device Management software shall access the resources through the profile created by Mobile Device Management software.
  - Accessing company-owned resources by any other means than mentioned above shall be strictly prohibited.

- **Risks/Liabilities/Disclaimers**
  - Sudarshan shall reserve the right to disconnect devices or disable services without notification.
  - Lost or stolen devices shall be reported to Sudarshan within 24 hours. Employees shall be responsible for notifying their mobile carrier immediately upon loss of a device.

- Employees shall use their devices in an ethical manner at all times and adhere to Sudarshan's acceptable use policy as outlined above.
- Employees shall be personally liable for all costs associated with their devices.
- Employees 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.
- Sudarshan shall reserve the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

20.2 E-Mail Security Policy

Purpose
The E-Mail Security Policy shall specify mechanisms for the protection of information sent or retrieved through e-mail. Additionally, the policy shall guide representatives of Sudarshan in the acceptable use of e-mail. For the purpose of this policy, e-mail shall be described as any computer-based messaging, including notes, memos, letters, and data files that may be sent as attachments.

Scope
The E-Mail Security Policy shall apply to all organizational employees, contractors, vendors, and any other person using or accessing organizational information or information systems. Exceptions to this policy shall be approved by the BTG Head.\

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

- **E-Mail Access**
  - All e-mail on organizational information systems, including personal e-mail, shall be the property of Sudarshan.
  - The email ID provided to employees shall assist in carrying out business activities and shall be considered the official ID of the employee. The System Administrator shall review the emails received/sent from these IDs as per business requirements.
  - Users shall not be authorized to open or read the e-mail of another user.
  - E-mail shall be provided to the users and contractors of Sudarshan to enhance their ability to conduct organizational business.

- The size of e-mail attachments shall be limited to a maximum of 35 MB, which shall be necessary for a user to perform his or her function.
- Group IDs should not be used to send or receive personal emails.
- Users shall be able to access email over Sudarshan-provided Desktop/Laptop only and personal mobile devices using Mobile Device Management software.

- **E-Mail Contents**
  - The use of inappropriate language, pornography, or misleading content in e-mail shall be prohibited.
  - The use of e-mail to spam (e.g., global send, mail barrage) shall be prohibited. This shall include the forwarding of chain letters.
  - The use of e-mail for sexual or other harassment shall be prohibited. Emails from any user shall 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.
  - Forging of e-mail content (e.g., identification, addresses, etc.) shall be prohibited.
  - When forwarding or replying to a message, the content of the original message shall not be altered.
  - Large files shall be transferred through the official FTP server instead of as e-mail attachments or any external service (except approved services like OneDrive).

- **E-Mail Usage**
  - 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.
  - When a user receives e-mail error messages that appear to be abnormal, they shall be reported to the BTG or CISO.
  - When sending e-mail, users shall verify all recipients to whom they are sending e-mail messages.
  - Users shall 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.
  - Emails shall be used strictly for business purposes; sending emails to other domains shall be allowed only as an exception based on business requirements.
  - Personal email IDs shall not be used for business purposes. Additionally, business emails shall not be forwarded to personal email IDs.

20.3 Firewall Security Policy

Purpose

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

Scope

The Firewall Security Policy shall apply to all employees, contractors, and vendors of Sudarshan, as well as any other person using or accessing organizational information or information systems. Exceptions to this policy shall be approved by the BTG Head.

Policy

- **Firewall System Design**
  A system designed to prevent unauthorized access to or from a private network shall protect and control both internal and external connections.

- **Firewall Security**
  The security of all network devices shall be addressed on two levels: physical and logical. These two aspects ensure that all devices are secure and that no unauthorized access is permitted.

- **Physical Security**
  The physical firewall device shall be located in a secure area of Sudarshan's premises. This location shall be restricted through the use of Biometric access. These areas shall only be accessed by a restricted number of authorized staff.

- **Logical Security**
  Access to Sudarshan's firewall shall be governed by password authentication. Only the System Administrator shall be permitted access to the firewall. Any changes to the device shall be performed by the System Administrator. No other member of staff shall be authorized or capable of accessing the firewall.

- **Firewall Monitoring**
  Regular monitoring of the firewall should occur to ensure that the device is functioning properly. This monitoring shall also ensure that the Sudarshan Network is being provided with the requisite protection.

- **Suspicious Activity Monitoring**
  The firewall shall be continually monitored for any suspicious activity. This monitoring shall enable the System Administrator to identify any potential threats arriving through the firewall and enable a swift response to potential dangers.

- **Log File Monitoring**
  Due to the nature and size of log files, daily monitoring may not always be feasible. As such, monitoring of firewall logs shall occur regularly at one-month intervals and under specific circumstances such as:
  - An attempted intrusion.
  - Suspicious inbound/outbound activity.
  - At the request of management.

- **Security Monitoring**
  The System Administrator shall perform regular auditing of the firewall to ensure that the integrity of said devices has not been compromised. Auditing shall include regularly reviewing access to the devices to ensure that only authorized users have gained access and monitoring the devices for any suspicious activity.

- **Analysis**
  Information gathered from the monitoring of the firewall shall be utilized to assess areas such as security. This should enable the System Administrator to efficiently assess the performance of the device and ensure that security is maintained.

- **Port Control**
  The firewall shall provide access to the trusted network only through a restricted number of ports. Any port that is not used to provide a connection shall be disabled to prevent unauthorized access and ensure the security of the Sudarshan Network.

Appendix

Sr. No.	Committees Involved	Members
1	Management Review Committee	
2	BTG Team	1. Sandeep Mhalgi 2. Manish Pawar 3. Anand Joshi 4. Sandeep Patil 5. Dhananjay Guldagad 6. Sanjeev Mhatre 7. Deepak Sankpal 8. Swati Shinde 9. Shweta Dalvi 10. Supriya Bhatmare 11. Hrishikesh Rajpathak
3	Incident Response Team	1. Business Technology Group 2. Safety Department 3. Admin Department 4. HR Department 5. Engineering Department 6. Legal Department
4	Business Continuity Management Team	1. Business Technology Group 2. Safety Department 3. Admin Department 4. HR Department 5. Engineering Department 6. Legal Department