IT Security and Management Policy

Document Statistics

Type of Information	Document Data
Document Title	IT Security and Management Policy
Date of Release	31.12.2024
Document Version No	1.0
Security Classification	Internal
Document Status	Draft

Document Approval History

Ver. No.	Date	Author	Approved by
1.0	30.03.2025		Nitish Jain (DGM IT)
1.0	31.01.2026		Saurabh Sharma (IT Head)

Document Revision History

Ver. No.	Date	Change Description	Author	Approved By
1.0			Akshat Jain	Nitish Jain

Review Summary

S. No.	Review Date	Reviewed By
1	**31.12.2024**	**Suraj Kumar (Chief Finance Officer)**
2	**31.01.2026**	**Saurabh Sharma (IT Head)**
3		

Table of Contents

1. Introduction

The IT security and management policy requires that the SG MART IT application and infrastructure reliably deliver the appropriate IT services when they are needed and provides the framework for SG MART to establish guidelines and procedures necessary to ensure security, confidentiality, integrity, availability and privacy of the information and data.

SG MART recognizes the vital role IT plays in supporting business operations and the importance of protecting information available in SG MART's IT applications and infrastructure. IT policy exists to maintain, secure, and ensure appropriate use of Information technology infrastructure established by the organization.

1.1 Purpose

The purpose of this document is to provide the IT policy framework for all its employees. The document defines guidelines towards good IT practices and adherence from employees on proper IT application and infrastructure usage. It also provides general guidance for employees of SG MART to prevent IT application and infrastructure related security incidents.

The overall purpose of this policy is as follows.

i. Establish controls for protecting SG MART's information and information systems against theft, abuse and other forms of harm and loss;
ii. Educate and enhance awareness of administrators and employees to maintain the responsibility for ownership and knowledge about information security, to minimize the risk of security incidents;
iii. Ensure that SG MART can continue its functions even if a major security incident occurs;
iv. Ensure financial data is available in case of any incident;
v. Ensure the availability and reliability of the network infrastructure operated by SG MART.

1.2 Scope

This policy applies to all SG MART employees, contractors, consultants and to any guests who have been temporarily granted access to use SG MART's network and IT infrastructure. Any computer, laptop, printer or other device that is capable of being connected to or transmitting data on the SG MART network is subject to this policy document.

2. Roles and Responsibilities

2.1 Senior Management

Information security and management requires strategic direction and motivation. Effective information security and management can be accomplished only by senior management involvement in approving and timely updating policies and procedures, appropriate monitoring of controls as per the organization's policy.

2.2 IT Head/ Chief Information Officer

Develop the IT security strategy; oversee the security programs and initiatives. Liaise with business owners for ongoing alignment of security initiatives with the business objectives. Ensure smooth functioning of IT operations to meet the business need/ objectives and evolve the IT security policy and program as per changes in IT environment. Develop risk mitigation plan and enforce policies and regulatory compliance. Promoting employee education and awareness programs for usage and understanding of IT applications and infrastructure in coordination with HR department.

2.3 Business Owners

Business owners are responsible for the creation of information in the IT applications and infrastructure. Their responsibilities include knowing the information for which they are responsible, classifying the information as per data classification criteria and ensuring appropriate controls and procedures are in place to protect security, confidentiality, integrity and availability of the information used or created within the unit. Authorizing access to the information and changes in the IT environment.

2.4 IT team

The IT team responsible for processing and storage of information. The responsibilities of IT team are as follows:

i. Administer access to application as per the organization's approved policy and procedures.
ii. Changes and enhancements to the IT applications and infrastructure is administered as per the organization's approved policy and procedures.
iii. To enable employees to make the most effective use of IT resources,
iv. Provide support to business users in case of any incident.
v. Help with new technology acquisition and development
vi. Support employees with hardware, software or any IT infrastructure related issues.

3. User Awareness and Training

IT security and management policy sets the standard for the way in which critical business information and systems will be protected from both internal and external threats. Personnel responsible for creating and maintaining the security policy must learn to recognize changes in technology that impact security and how those changes impact the organization and the people who work for the organization. It is important to cover following points as part of user awareness and training program:

i. Educate employees about importance of IT security
ii. Educate employees about importance of IT Policies and discuss the IT policies
iii. Communicate changes in IT policy to employees

4. Asset Management Policy

The asset management policy establishes the framework governing use of the IT Assets and set standards and practices to identify the rules of acceptable use and the rule of protection.

This policy specifies the requirements to designate who owns the assets. Designated owner is responsible for protecting information and technology assets, and to maintain the way assets are protected.

i. An inventory of all assets associated with information systems must be documented and maintained.
ii. Asset tagging is done to allows the tracking of the movement of fixed assets from location to location. Asset tagging is the process of numbering fixed assets
iii. End of Life cycle assets shall be decommissioned/migrated using a detailed project plan which shall include clear timelines for removal/replacement of effected assets.
iv. Information owners and information custodians must be designated for all assets associated with information systems.

4.1 Asset procurement

All the IT assets shall be procured from approved vendors and after obtaining all the necessary approvals from the authorized personnel. All IT assets are procured as per the SG MART's procurement policy and technical assessment is performed to evaluate that the asset will meet the organization's objectives and support for a reasonable

time period. Asset criticality is done to prioritize maintenance procurement and to identify the most critical assets

4.2 Asset usage

The use of the IT assets and resources in connection with business use is a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the IT assets and resources efficiently and responsibly.
Any action that may expose to risk of unauthorized access to data, disclosure of information, legal liability of other potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/ or criminal prosecution.

4.3 Asset life cycle

The life of an asset is considered till it can effectively serve business needs. Asset will be retired once their cost advantage to the company ceases. This can be because the equipment is aged, broken beyond repair or the repair is more expensive than cost of expected life, the lease/rental has expired or there is a newer technology that is required.

Asset life guidelines:
Servers and server peripherals - 5 years
Laptops - 4 years
Desktops - 4 years
Telecom hardware - 5 years
Cabling - 10 years
All IT hardware not covered above - 3 years

Exception: In case there is a need for replacement/ upgrade of hardware before expected age then the request should come from HOD with a valid business reason and approved by IT HEAD.

4.4 Asset Disposal

After the productive life of an asset, it has to be disposed. Disposal shall be recommended by the IT HEAD to the finance department. The finance department will then arrange for Disposal of the asset.

5. Email Usage Policy

Company has provided electronic messaging system to facilitate written communication required for business and official activities. The users are required to use email in a responsible manner for official purposes "ONLY" and any other personal communication (e.g. spam mails) shall be avoided.

5.1 Email activation/ termination

i. All employees, consultants and staff of the Company provided with an email account is controlled by a password. All email accounts should be named accounts and group/ common IDs are to be provided only on need basis after obtaining appropriate approvals.
ii. All email users shall be accountable for any communication made through their email accounts.
iii. Email access shall be terminated within 2 working days when the user terminates his association with Company, unless required to be kept active for business purpose. Email account shall be deleted within 30 days of disablement of account of the employee/ consultant.
iv. Company preserves the right of storing or forwarding the contents of an individual's email box, after the term of employment has ceased. This shall be

on the request from respective Department Head and approval by Head of HR function.

5.2 Appropriate Use

All the communication done using the IT medium should be in-line with Information Security Policy and Code of Business Ethics of the Company. The type of activities that shall be encouraged includes the following but not limited to:

i. Communicating with fellow employees, business partners of Company, and clients within the context of an individual's assigned responsibilities.
ii. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
iii. Participating in educational or professional development activities.

5.3 Inappropriate Use

Company's e-mail systems and services shall not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on Documented/ room). Individual e-mail should not interfere with others' use of email system and services. Email use at company must comply with all applicable laws, company policies, and company contracts.

The following activities are deemed inappropriate use of Company systems and services and are prohibited:

i. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
ii. Use of email in any way that violates Company's policies, rules, or administrative orders, including, but not limited to, Information Security Policy and Code of Business Ethics of the Company or violates applicable state, country or global laws and regulations.
iii. Viewing, copying, altering, or deletion of email accounts or files belonging to Company or another individual without authorized permission.
iv. Sending of unreasonably large email attachments. The total size of an individual email message sent (including attachment) should be as per the limit prescribed from time to time.
v. Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
vi. Sharing email account passwords with another person, or attempting to obtain another person's email account password. Email accounts are only to be used by the registered user.
vii. Forwarding of Company email to personal email accounts on Gmail, Yahoo etc.
viii. Sending official emails to official contacts on their personal accounts on Gmail, Yahoo etc., unless there is no alternate available and the necessary approval for sending to such account has been obtained in writing from the concerned Head of department.
ix. Use of personal email account to transact/ disseminate Company information.
x. Users shall limit the use of personal emails from Company IT network. The Company discourages the use of personal email on Company provided Information Systems.

5.4 Monitoring and Confidentiality

The email systems and services used at the Company belong to the Company and therefore shall always be considered as Company's property. The organisation reserves the right to monitor, inspect, copy, review, and store any and all employee email use at any time and without prior notice. In addition, Company may monitor, inspect, copy, review, and store any files, information, software, and other content

created, sent, received, downloaded, uploaded, accessed, or stored through the Company's email system. The Company reserves the right to disclose email information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.
If the Company discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, email records may be retrieved and used to document the activity in accordance with due process. The Company can't be held liable to communicate the same to the individual user of the account. The Company might seek requisite permission and exercise its discretion to access user's non-official email accounts if it suspects that any Company information is compromised through these accounts. All users shall take extreme caution when communicating confidential or sensitive business information via email. Users should understand that all email messages sent outside of the Company are be the property of the receiver and could be considered as acceptable evidence in court of law. Therefore, users shall not share information with external parties that may harm the Company in any way. Also, all users shall demonstrate due care while using the "Reply All" command during email correspondence to ensure the resulting message is not delivered to unintended recipients.

6. Bring Your Own Device (BYOD)

All employees should use SG MART provided IT assets for the official purpose. However, employees can get official emails configured over their mobile devices after obtaining approvals from respective HoDs and IT HEAD. Users are not allowed to access emails and any other applications over their personal laptop/ computers.

6.1 Mobile Device Management

Employees are allowed to use personal mobile phones to access official emails. After obtaining approvals from respective department heads and IT HEAD, employees can get emails configured on their personal mobile phones. Also refer to Email usage policy.

7. Network Operations Policy

7.1 Firewall

A firewall is combination of hardware and software designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset.

i. Firewall should be configured to restrict all inbound traffic outside SG MART network or VPN from accessing SAP application or any IT infrastructure.
ii. Firewall Rulesets and Configurations require periodic review to ensure they have the required levels of protection.
iii. Firewall Rulesets and Configurations should be backed-up frequently to alternate storage. Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.
iv. Firewall Administrators will perform changes to Firewall Configurations according to approved production maintenance schedule or after obtaining approval form IT HEAD and business departments.
v. Two user groups have to be created i.e. a) Admin Users b) Executive Users.
a) Admin Group users would have complete access to the firewall configuration and are responsible for maintenance/ configuration/ changes on the firewall.
b) Executive Group users will have access to monitor the firewall only and are assigned users who are responsible for monitoring of firewall.

7.2 Vulnerability Assessment/ Penetration Testing (VA/PT)

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, especially in software and hardware. Vulnerability management is integral to SG MART's network operation policy.

This policy lays following guidelines in context of VA/PT assessment:

i. The use of any network based vulnerability scan and penetration test tools to scan or verify vulnerabilities will be managed and approved by IT HEAD. Any use outside of this channel is strictly prohibited.
ii. VA/PT testing shall be conducted on atleast bi-annually basis. The results of these tests will be documented and remediated in a timely manner. Subsequent tests will confirm that remediation was successful.
iii. SG MART personnel are expected to cooperate fully with any vulnerability assessment being conducted on systems for which they are held accountable.
iv. Scans shall be performed during hours appropriate to the business needs and to minimize disruption to normal business functions. If a business disruption is suspected to be caused by the vulnerability scanning, such scan should be stopped immediately and further investigation shall be conducted.
v. Data obtained as a result of the scans are to be treated as Confidential.
vi. The vulnerability scanning tool should have the ability to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability.
vii. IT Staff shall not make any temporary changes to network infrastructure's systems, for the sole purpose of being approved by an assessment. Vulnerabilities on information systems shall be mitigated using proper analysis and methodologies
viii. No devices connected to SG MART's network shall be specifically configured to block vulnerability scans from authorized scanning engine.
ix. At the conclusion of each vulnerability assessment a mitigation and compliance report shall be produced, this report will summarize the following:
    - List of Vulnerabilities. All discovered vulnerabilities, the severity, and the affected information systems.
    - Remediation Steps. Each vulnerability listed will have information on potential remediation actions.
    - The report shall be submitted to the IT HEAD with a timeline for completion of remediation steps.

7.3 Virtual Private Network

This policy provides following guidelines for remote access using Virtual Private Network (VPN) connections to SG MART's network and applications:

i. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to SG MART's internal networks.
ii. VPN use is to be controlled using two factor authentication which includes certificate verification and login credentials authentication.
iii. At no time should any SG MART employee provide their login or email password to anyone.
iv. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
v. Dual (split) tunneling is not permitted; only one network connection is allowed.

8. Cyber Security Policy

The cyber security policy establishes the framework for protecting the SG MART's IT environment from all types of cyber attack.

i. All systems will be protected against maliIT Headus code that can steal, damage, or destroy information
ii. Antivirus software will be installed on all systems. Antivirus software will be set to update automatically. Employees are not permitted to turn off antivirus.
iii. All USB drives must be scanned for viruses.

All the above steps along with the other policies mentioned in this document should be adhered to in order to protect the organization of cyber-attacks.
Further, IT HEAD in collaboration with senior management should develop a program to perform the tabletop drills to check the organization's preparedness against the cyber-attacks and employees' reaction and reporting of the incident in such a scenario. It will help management to identify the strengths and areas of improvement.

9. Internet Usage Policy

Users shall be allowed access to the internet only when it has been established that it is required for business purposes. Use of email and access to the Internet, must be guided by good judgment and the company's policies. Any unauthorized access shall be recorded and be dealt with.
The personal use of social media and networking sites is allowed and at all times the company has the right, but not the obligation, to access, monitor, record, and audit internet usage. Although limited personal use is allowed as long as it does not violate any company policy or otherwise interfere with job duties, users should not expect that such use entitles them to any expectation of privacy in anything that they create, store, send or receive on or through the system, including any personal messages.

The company assumes no liability for loss, damage, destruction, alteration, disclosure or misuse of any personal data or communications transmitted over or stored on the system. The company accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on the system. The company strongly discourages employees from storing any personal data on the system. Use of the system is a privilege that may be revoked by the company at any time.

10. Cryptography

All encryption mechanisms implemented within SG MART shall be based on the guidance provided within this policy. The use of proprietary encryption algorithms are not allowed for any purpose, unless reviewed and approved by IT HEAD.

i. Company confidential information shall be encrypted both at rest and in transit.
ii. Company confidential information on servers and databases shall be encrypted at rest where appropriate.
iii. SG MART laptops shall be employed with full disk encryption and information stored within removable devices for authorized purposes shall be encrypted.
iv. Company confidential and customer confidential information transmitted through email (message or attachment) shall be encrypted using TLS encrypted emails or password protected attachments.
v. Secure encryption key management procedures shall be used to prevent unauthorized access of encryption keys.

11. Data Leakage Prevention Policy

The Company shall deploy appropriate tools to prevent accidental or deliberate leakage of information from Company owned network and/ or systems. The Company shall be authorized to monitor communication over network to scan for business sensitive information going to unauthorized sources within or outside the organization. Appropriate system shall be put in place to notify leakage of information and guidelines for handling such incidents shall be specified. The system shall be effectively configured as per business need to track or block leakage of business sensitive information. All efforts shall be made to ensure that personal information of users are not tracked as Company intends to prevent leakage of sensitive business information.

It should be understood that tools are as effective as their configuration and there is a possibility that some incidents reported by the tool are justified by appropriate authority as false positives/ required for business reasons. Such incidents shall be taken into account for creating exceptions to the rules.

At all times the company has the right, but not the obligation, to access, monitor, record, and audit internet and email usage and data stored and transferred using USB or any media. Company has right to block the USB ports of the company provided laptops and computers, for enabling the same approval from HoDs and IT HEAD is required.

Below is an indicative list of controls that users shall be expected to follow to prevent leakage of Company data

i. Users shall exercise caution while sending company information/ data outside organization through emails or web to ensure the information does not go to unauthorized or unintended recipients.
ii. Users shall not print business sensitive information unless it is required and justified for business purpose.
iii. Users shall not copy business sensitive information on external storage media like USB, CD/DVD, media card etc. without required business justification.
iv. Users shall not attempt to circumvent security systems deployed to prevent leakage of company data.
v. Users shall not use personal emails to disseminate company information/data.
vi. Users shall not publish or disclose any Company information/ data publicly unless the information is permitted for public disclosure.
vii. All the users shall be responsible to use the Company's information in a secured manner and ensure that confidentiality of the information is maintained at all times.

12. Information System Acquisition and Development

This policy requires security of IT infrastructure should be considered at every stage of an information system's (includes applications, software, tools, servers, firewall and any other component of IT infrastructure) life cycle (e.g., feasibility, planning, development, implementation, maintenance, retirement, and disposal) and specifies following points to be considered during Information System Acquisition and Development:

i. Ensure conformance with all appropriate security requirements
ii. Protect enterprise data throughout its life cycle
iii. Facilitate efficient implementation of security controls
iv. Prevent or minimize the introduction of new risks when the system is modified
v. Formal review and approval of all IT infrastructure and asset procurements
vi. Ensure proper removal of data when the system is retired
vii. Vendor assessment for solutions hosted outside of SG MART network
viii. Third-party penetration testing (as appropriate)
ix. Vulnerability analysis and remediation
x. Vendor should provide SOC1 or SOC2 report
xi. User acceptance testing is performed before systems go-live

xii. Securely designing the architecture of an application is critical to protecting the data and assets it contains.

13. Change Management Policy

The objective of the change management process is to ensure that changes to IT applications and their associated components are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. Changes to production systems (e.g. application and/or infrastructure) must be managed to ensure there is minimal or no impact to the business as a result of implementing those changes.

It also ensures that all changes should always move from Development client to Quality client and then finally to production client with prior testing and approval, except for Direct changes.

There can be following types of changes, which follow different approval process:

A. **Normal Changes:** Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed. These changes are most often scheduled outside of defined change blackout windows or during defined maintenance windows. The normal type is used to implement beneficial change for any change to a service that is not pertaining to a time critical business requirement.

B. **Emergency Changes:** A change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch. It is of such a high priority that it bypasses group and peer review and approval and goes straight to the Authorization state for approval by the IT HEAD and all other approvals are obtained post facto. IT team must maintain the record of all emergency changes for review by the management.

Emergency changes cover the following types of emergencies:

i. Fix on fail or retroactive situations where the impact to business has already been experienced.
ii. Fail or fail situations where the impact to business is imminent if action is not taken.

These changes do not follow the complete life cycle of a normal change due to the speed with which they must be authorized. However, post facto approvals are documented, which include business justification that qualifies for an emergency change and UAT. Emergency change must be moved to Production after obtaining approval from IT HEAD.

C. **Direct Changes:** Ideally there should be no direct changes made to tables, programs and configurations in a production system. Due to business and technical requirement when changes are to be made directly in SAP, such changes required approval from IT HEAD and justification is to be documented. IT team must maintain the record of all direct changes done for review by the management.

Standard rules laid down as part of the change management policy are:

i. All changes to Production environments must be via the approved change management process and procedures;
ii. A unique identification number *must* be associated to each Change;
iii. Each Change *must* identify who requested the change; this is also the Change Owner;
iv. Each Change *must* identify the reason for the change;
v. Each change must be approved by the appropriate business and or IT approvers;
vi. Any modifications to the Change process *must* be approved, documented, and communicated to all impacted stakeholders;
vii. All Changes *must* be tested and results signed off in quality environments prior to production; where testing is not performed, justification must be documented and approved by IT HEAD over email or workflow configured system.

viii. An Emergency Change must be completed with all documentation and approvals within 5 business days post change;
ix. Roll back plans for all Changes *must* exist
x. Business impact and risk *should* be attributed to all Changes;
xi. Change Advisory Board meetings *should* be held monthly, or as required and minutes of these meetings should be documented and shared with all participants.

14. Configuration Management Policy

This document provides requirements for the configuration management process which is required to assure that information systems are designed and configured using controls sufficient to safeguard the information systems.

i. A current baseline configuration must be developed, reviewed, approved, documented, and maintained under configuration control for each information system.
ii. A baseline configuration must document and provide information about the components of an information system including the following:
    - Standard operating system/ installed applications with current version numbers
    - Standard software load for workstations, servers, network components and laptops
    - Up-to-date patch level information
    - Network topology
    - Logical placement of the component within the system and enterprise architecture
    - Technology platform
iii. Proper authorization and approvals at all levels
iv. Successful testing of updates and new programs prior to their being moved into a production environment
v. Document configuration change decisions associated with the information system over emails
vi. Retain records of configuration-controlled changes to the information system for the life of the system

15. Patch Management Policy (As Per SAP HANA Cloud RISE contract)

Production servers must be regularly updated with necessary patches. A patch management process must be in place to ensure timely patch updates to SG MART's production systems. This includes:

i. Vendor Security updates
ii. Application & operating system updates
iii. Firmware updates & upgrades

All relevant security patches/ updates/ hot fixes are reviewed and approved after initial testing of patches on non-production machines.

System administrator reviews the Linux patches for their relevance in SG MART environment. In case of any relevant updates, system administrators review the requirement and apply the patches on Test Servers following the change request process. On successful deployment of patches in test environment, approval is obtained from IT HEAD for updating the patches on the production servers.

16. Incident Management Policy

An Information Security Incident is defined as any adverse event that harms or represents a serious threat to SG MART's IT resources such that there is actual or potential for loss of confidentiality, integrity, availability, non-repudiation and auditability of information.

A security incident should not just be viewed as an event that has occurred (i.e. an event in the past). It also extends to include security threats of which SG MART is aware of or suspects. Such threats represent future events which have not yet come to pass, which with the appropriate management can be mitigated and avoided by SG MART.
During the review and assessment of a security incident induces a change to be done in production environment, such a change should follow change management policy and procedures.

SG MART has defined three severity classifications for information security incidents:

i. Level 3 – Severe
ii. Level 2 – Major
iii. Level 1 – Minor

In accordance with this policy, all employee must be aware of following responsibilities as part of their daily role:

i. Be aware of what constitutes an information security event
ii. Be familiar with the process of reporting information security incidents and threats to SG MART's IT team
iii. Identify and report potential information security incidents and threats to SG MART's IT team
iv. Act immediately upon having any evidence of an information security incident or threat
v. Not contribute to, or willingly take part in any activities that may subject SG MART to an information security incident or threat.

17. Logical Access Policy

This policy specifies the mechanism that restricts access to SG MART's applications and infrastructure. Access restrictions protect organization from security threats such as internal and external intrusions.

Access control policy provides framework for management of user access, authorization and control mechanisms for database, operating system and applications.

i. Access to information systems and services must be consistent with business needs and based on security requirements.
ii. All users must be issued a unique identifier for their use only, and an approved authentication technique must be used to substantiate the identity of the user.
iii. Generic Accounts should be documented as to the purpose, what they have access to, and who has access to them. Requests to set up and access Generic accounts should be documented and approved by IT HEAD and Business owner over emails.
iv. There must be a formal user registration and de-registration process for granting access to all information systems. Approval from HOD and IT HEAD are needed before access to any user is granted to any system/ application.
v. The allocation and use of privilege logins must be restricted and controlled.
vi. If an individual no longer requires access to systems due to termination, resignation, or other reasons, access from the IT application and infrastructure should be revoked within 2 days.

vii. Interactive logon for service accounts must be disabled, unless it is necessary for the system, application, or process to function.
viii. Access to information system functions and information through applications must be restricted in accordance to the role of the user. In case of user access modification, approvals from HODs and IT HEAD should be obtained.
ix. Firefighter IDs shall be kept locked by the system administrator and assigned to users who need to perform tasks in emergency or extraordinary situations only after obtaining appropriate approvals. A firefighter ID is a temporary user ID that grants the user exception-based, yet regulated, access. The activity log of such user IDs are reviewed by IT HEAD and appropriate documentation is done the review activity.
x. The infrastructure IDs in the system be controlled and maintained by the basis team and interactive logon for service accounts must be disabled such IDs.

18. Password Policy

Passwords are an important aspect of information security. A poorly chosen password imposed risks that may result in unauthorized access and/ or exploitation of SG MART's resources. All users, including contractors and vendors with access to SG MART's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

i. Passwords must consist of a minimum of 15 characters.
ii. Passwords must contain characters from three out of four categories below:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base-10 digits (0 through 9)
    - Non-alphanumeric (for example, !, $,#, %),
iii. User passwords must be changed at least every 60 days
iv. Passwords must be kept private and never shared amongst users, even when requested by someone from IT.
v. Users must change temporary passwords at the first logon of the system.
vi. Temporary passwords must be unique.
vii. Vendor default passwords must be changed before installing any system on the network.
viii. End user computing devices must be configured to require a password for access at initial power on.
ix. Privileged passwords (e.g. for super user or administrator utilities or accounts) must be changed when there is any indication that they have been disclosed to people who do not need them for their work, or when someone knowing the password leaves the company.
x. Passwords must be changed as soon as it is discovered that a password has been compromised, or is believed to have been compromised.
xi. Passwords must never be stored in clear text in any computer systems; examples of these locations include text files and Excel spreadsheet.
xii. User accounts will be locked out after six failed logon attempts, at which time the user has to contact the SG MART IT team for assistance.

19. Data Center Security Policy (As Per SAP HANA Cloud RISE contract)

This policy specifies requirements for protection from environment and man-made threats to personnel and property in data centers. All data centers or server rooms shall implement and maintain their services via the standards outlined in this policy.

i. Data centers must be physically secured to restrict access to the data center. The access should be controlled by Electronic Access Control System (EACS) or Biometrics Access System.

ii. Environmental controls will exist in all data center or server rooms. This will include temperature monitoring and fire controls.
iii. All the entry and exit gates of the data centers and server rooms should be monitored by CCTV cameras.
iv. Access to Data Center facilities will be managed by pre-defined approved lists, maintained by the IT team member. Access by all other staff will require pre-approval by the IT HEAD.
v. Access to the data center must be restricted to only individuals that have a business need to access the data center.
vi. Access to the data center must be logged and monitored on a regular basis by the IT HEAD. Improper access to the data center must be investigated, actioned and documented where necessary.
vii. Access to the data center must be revoked immediately if the access is no longer required.
viii. Details of the Service Level Agreements for each outsourced data center will be maintained by IT HEAD.

20. Backup & Restoration Policy

Management will protect data in the organization by performing backups to be sure that data is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.
The guidelines laid down by this policy for backup and restoration are:

i. A defined backup schedule must be in place for production servers. The backup schedule must allow for daily incremental backups and complete weekly & monthly backups of production servers.
ii. Access to manage backups must be restricted to authorized IT resources. Schedule changes must be documented and approved by the appropriate personnel.
iii. Backup media must be stored in a physically secure protected location until rotated offsite. Backup media must be physically / logically transferred to an offsite location for storage on a regular basis.
iv. The status of all backup jobs should be logged and retained, and reviewed to identify failures. Any failures requiring intervention for resolution must be assigned to an appropriate IT resource for resolution. The designated IT resource should investigate the issue and take the necessary corrective action (if any) to ensure the next backup job runs successfully.
v. A data restoration test from the backup media must be completed at least once a year for core systems to validate that the data can be restored in the event of a disruption.

21. Business Continuity Policy

This policy specifies direction on planning the resumption of business or services in the event of a man-made or natural disaster. SG MART is required to be prepared and re-establish business or services as smoothly and quickly as possible.

i. There must be a process to ensure that business continuity programs address information security requirements.
ii. A risk assessment must be conducted to identify information security events that may interrupt business processes and recovery time for critical functions.
iii. A business continuity plan must be developed to resume and maintain business operations to the required level following interruption to or failure of essential service.
iv. Business continuity plan must be regularly exercised and updated.

Disaster Recovery remove (As Per SAP HANA Cloud RISE contract)

Disasters are inevitable but mostly unpredictable, and they vary in type and magnitude. The best strategy is to have some kind of disaster recovery plan in place, to return to normal after the disaster has struck. The disaster recovery plan begins by identifying these causes and effects, analyzing their likelihood and severity, and ranking them in terms of their business priority. Management should clearly define Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

22. IT Vendor Management Policy

The purpose of the IT Vendor Management Policy is to provide guidance relative to the management of IT vendor and partner relationships.
The due diligence process provides SG MART with the information needed to evaluate the potential IT vendor to determine if a relationship would help the company achieve its established goals and evaluate the technical competency of the vendors. The IT vendor due diligence process should be performed prior to the selection of any third party vendor and when renewing a contract.
When entering into a contract with a new IT vendor, the following areas should be included as applicable. These contracts should be appropriately documented and approved in Legal document repository:

i. Master Services Agreement (MSA)
ii. Statement of Work (SOW)

22.1 Master Services Agreement (MSA)

This is a standalone master agreement with vendors which we have a high probability of doing repeat business. With a MSA, subsequent SOWs will refer to the MSA for basic Terms and Conditions and the SOW will supersede the MSA in the event of any conflict in T&C's.

22.2 Statement of Work (SOW)

i. Scope of work/ services – the contract should clearly state:
    - Services being provided
    - Timeframe for delivery
    - Roles and responsibilities
    - Guidelines for any change orders due to scope changes
ii. Service Level Agreements – Service levels should be agreed to for the services provided.
iii. SLAs should be reported to SG MART on a regular basis in a formal report and reviewed by IT Management.
iv. SLA Penalties – Financial penalties should be included in the agreement for SLAs that are not met.
v. Security and Confidentiality – for IT vendor relationships that include hosting SG MART data, the contract should include verbiage that the data will be kept confidential and not used for any purpose other than the agreed upon services.
vi. Internal Controls – SOC Reports are required from the vendor when SG MART assets or data is being maintained by the vendor. These reports should be conducted in accordance with SSAE 18 guidelines or for international locations ISAE 3402. In the event that a SOC Report or its equivalent is not available, a "right to audit" clause at the expense of the vendor should be included in the agreement.
vii. Business Continuity and Disaster Recovery – The vendor should have a plan in place to ensure services are not interrupted in the event of a disaster, hardware failure, etc.
viii. Duration – the length of the agreement needs to be included in the contract with stipulations for renewal
ix. Termination Clause – with the assistance of SG MART Legal team, termination clauses should be included in the contract. This should include termination for

persistent failure of SLAs. For example, a failure of an SLA three consecutive months or 6 times in a rolling 12 month period calls for termination of the agreement.

23. Policy Compliance

All the employees within SG MART, third parties who have access to SG MART information or information systems shall follow this policy. Violation of this policy could lead to disciplinary actions for employees and contract termination for third parties.

24. Exception

Any exceptions to this policy shall be submitted to the IT team. The exception request shall be reviewed by the IT HEAD. The security exception shall be considered approved only when the exception is approved by asset/ information Owner/ HoD, IT HEAD and CFO.

Annexure