SUBHKAM VENTURES (I) PRIVATE LIMITED

INFORMATION TECHNOLOGY POLICY

Version	Approval	Version Description	Regulatory Reference
1.0	Board Meeting dated 21st August, 2018	2018	Reserve Bank of India Master Direction
2.0	Board Meeting dated 21st April, 2025	2025	Reserve Bank of India Master Direction

SUBHKAM VENTURES (I) PRIVATE LIMITED

TABLE OF CONTENTS

SUBHKAM VENTURES (I) PRIVATE LIMITED

INFORMATION TECHNOLOGY POLICY

1. PREAMBLE

1.1 Objectives of IT Policy

The objective of the Policy is to set the guiding principles for establishing IT infrastructure and IT operations and governance, that would enable the users to identify opportunities, improve performance and understand business environment, and at the same time to achieve Confidentiality, Integrity and Availability of the information and information systems used by those IT Operations. This document provides the framework to manage IT infrastructure by means of structured service delivery, service management and IT governance processes. It states the responsibilities of management, executives, employees, and suppliers to ensure that the IT supports business objectives.

1.2 Document Confidentiality

This document is confidential – Internal use only.

1.3 Authority

The policy document is issued and approved under the authority of Board of Directors, based on the review and recommendation of Information Technology Strategy Committee (ITSC).

1.4 Review and Approval

This policy shall be updated once annually or in the case of change in IT environment or a regulatory requirement. This policy shall be updated by CTO and approved by the Board.

1.5 Procedures and Guidelines

Company has a separate document for "Procedures and Guidelines". It documents the detailed guidelines for implementation of the policies and standards.

The key objectives of Procedures and Guidelines are:

a) To ensure that IT Policy is interpreted correctly and uniformly across the group entities.
b) To provide guidelines for implementation of the policies
c) To create awareness about policies and assist in policy compliance.

1.6 Scope

These policies & standards are applicable to SVIPL and Group entities including all IT and IS assets, all IT and IS processes, all business processes supported by IS and all employees in India along with its third-party vendors.

1.7 Management of IT Policy

The ITSC shall have the overall responsibility of implementation & maintenance of this policy, and it shall review this Policy on yearly basis or if any significant changes occur. ITSC shall also review the compliance & implementation status, effectiveness of controls & their implementation, Incidents, suggestions & feedback from various stakeholders.

2. IT GOVERNANCE

2.1 IT Governance Framework

IT Governance is an integral part of corporate governance. It involves leadership support, organizational structure and processes to ensure that the organisation's IT sustains and extends business strategies and objectives.

2.2 IT Strategy Committee (ITSC)

IT Strategy committee shall periodically review organizational IT structure to check if it commensurate with the size, scale and nature of business activities carried out. The ITSC shall meet at least on quarterly basis. The Committee shall work in partnership with other Board committees and Senior Management provide input to them.

It will also carry out review and amend the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance. Its deliberations may be placed before the Board.

Composition of the Committee shall be approved by the Board of Directors in compliance with the regulatory guidelines on IT Governance.

Responsibilities:

1. Approving IT strategy and policy documents
2. Ensuring that the management has put an effective strategic planning process in place.
3. Ratifying that the business strategy is indeed aligned with IT strategy.
4. Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
5. Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable.
6. Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.
7. Ensuring proper balance of IT investments for sustaining growth and becoming aware about exposure towards IT risks and controls.

2.3 Chief Technology Officer (CTO)/ Head of IT Function

Roles and Responsibilities:

1. Ensuring that the execution of IT projects/ initiatives is aligned with the IT Policy and IT Strategy.
2. Ensuring that there is an effective organisational structure to support IT functions in the organisation.
3. Putting in place an effective disaster recovery setup and business continuity strategy/ plan.
4. Ensure effective assessment, evaluation and management of IT controls and IT risk, including the implementation of robust internal controls, to

    a. Secure the entities information assets.
    b. Comply with extant internal policies, regulatory and legal requirements on IT related aspects.

2.4 Chief Information Security Officer (CISO)

Roles and Responsibilities:

1. The CISO shall be responsible for driving cyber security strategy and ensuring compliance to the extant regulatory/ statutory instructions on information/ cyber security.
2. The CISO shall be responsible for enforcing the policies that a RE uses to protect its information assets apart from coordinating information/ cyber security related issues within the RE as well as

with relevant external agencies.

3. The CISO shall be a permanent invitee to the ITSC and IT Steering Committee.
4. The CISO's Office shall manage and monitor Security Operations Centre (SOC) and drive cyber security related projects.
5. The CISO's office shall ensure effective functioning of the security solutions deployed.
6. The CISO shall place a review of cyber security risks/ arrangements/ preparedness of the entity before the Board/ RMCB/ ITSC at least on a quarterly basis.

2.5 Governance through boards and committees

Risk Management Committee (RMC)

- RMC is constituted ad empowered by the Board, in accordance with the guidelines framed by regulator.

3. IT PLANNING

3.1 IT Strategy

1. The IT Strategy committee, based on key inputs from the business leadership and the board of directors of the organization design an IT strategy that is aligned with the enterprise/business strategy.
2. While defining the IT strategy, due consideration should be given to attributes such as cost-effective, appropriate, realistic, achievable, enterprise and technological obsolescence.
3. The strategy shall be designed and maintained in a manner that it will serve as a guidance for building an IT roadmap around IT-enabled investment commitments, IT programs/Projects to be undertaken, business IT services to be instituted and IT assets to be acquired.
4. The IT strategy shall be communicated and be accessible to all appropriate business and IT stakeholders and throughout the enterprise.

3.2 IT Budget & Cost Management

IT budget shall help IT achieve business goals in a cost-efficient manner.

1. The IT and finance function shall establish and maintain a method for accounting for all IT-related costs, investments and depreciation as an integral part of the organizations cost and financial management process.
2. The Board and senior management shall provide adequate support for financial allocations to the budgets to ensure that IT strategy objectives can be met effectively.
3. The IT function shall prepare a budget reflecting the investment priorities supporting the IT strategy and Operational requirements based on the portfolio of IT-enabled programs and IT services.

3.3 Access Management

1. User Access Management
   a) User Management is standardized, and governance controls are implemented over the Registration, Modification and De-registration of users.
   b) Access/authorization should be granted to the users as per business requirements and only against approval from the designated authority based on the principle of least privilege.
   c) Users are informed about their legitimate accesses and also educated about the consequences of access violations. Reviews are done of the user management process.

2. Third Party Applications / Software
   a) For usage of any application which is not in the list of approved applications, approval is required from COO /CTO/HOD and CISO along with SVIPL Entity Exception Request

Form.

b) Transactions by users need to have maker-checker controls at the application level. Each transaction needs to be made and checked by separate authorized users. Maker and checker functions can co-exist in a single user, but a single user cannot make and authorize a single transaction.

3. Termination / Resignation
   a) The HR Department shall inform the date of termination of services to the IT/Tech Team within 48 hours after the resignation of the employee is accepted or termination of services decision is taken. HR team shall also confirm if the deactivation/removal of access should be immediate, on last working day or any other day as management thinks fit.
   b) The IT Team will disable/deactivate the e-mail Id, domain id and all the application access are disabled. For SSO enabled applications, domain id disablement would discontinue the access.
   c) In case the emails of the employee need to be forwarded to another employee, the Head of the Department & CISO team shall authorize the request and the IRA will send it to the Tech Support Team. The request shall also contain the time period for which the forwarding is required (cannot be more than 30 days of Last working day).
   d) In case of other applications, the Application Administrators shall delete or deactivate the user ID from the system on the day of termination of service. (In case of generic user IDs used for applications, the user ID needs to be transferred to another owner).

4. Transfer of Employees
   a) The HR Department shall inform Tech Support about the transfer of the employee.
   b) The Tech Support shall check the access to the applications and other IT facilities available to the employee by referring to the Logical Access Register.
   c) The Tech Support shall revoke the access to the application based on approval from the new IRA and inform the HR Department.
   d) The user registration procedure shall be followed for granting access at the new location for the new job profile.

5. Change of Access Rights
   a) The users are responsible to notify if there have been any changes in their roles and the type of access required.
   b) The user shall fill the change in access rights form/emails/tickets.
   c) The HOD of the user shall verify the required access to be discussed.
   d) The user registration procedure shall be followed for granting access to change job profiles.
   e) Maker checker process has to be put in case of modification of the access rights.

6. Access to Third Party and Vendors
   a) Access to third parties shall be restricted based on the principle of "need to know" and as per the principle of least privileges required for operations.
   b) Third party or vendor requiring access to SVIPL Entities resources including network resources from their own systems shall connect through VPNs or VDI or SVIPL issued laptops.
   c) It shall be ensured that the third parties and vendors have signed non- disclosure agreement/ clause before granting access.
   d) On completion/ termination or extension of the contract, the Head of Department shall send a request for revocation of user access rights or extension of period of access respectively to the Head - IT Infra / CISO.

7. Sharing of User IDs
   a) User IDs shall not be shared by the users.

b) In situations where the login credentials need to be shared, suitable audit trails shall be maintained.

c) Critical user IDs which may be required for emergency procedures may be shared with limited number of system admins to support.

d) Exception to above shall have approval from CISO Team.

8. Privilege Management

a) Access to information and Information Systems including applications, operating systems, database, and networking / security devices should be provided to users only after proper authentication. The allocation and use of privileges should be restricted and controlled.

b) Every administrative / privileged account should have one-to-one relationship with an individual User. Access to any resource of Information System via shared administrative / special privileges user accounts should not have permitted.

c) The access privileges associated with each system product, e.g. operating system, network, database, application and system utilities, and the users to which these privileges need to be allocated should be clearly identified and documented.

d) Privileged user's access rights (administrative & special privilege) for all Information systems should be reviewed at least every 6 months.

e) For all privileged access, all the user activities should be logged and reviewed periodically.

3.4 Teleworking Controls

a) VPN access shall be given on the request of user with approval from Business Head and CISO Team.

b) VPN ID creation/deletion/extension shall be initiated through Change Management Process

c) Reconciliation / Re-certification of the VPN IDs shall be conducted on quarterly basis.

d) Ensure that data/ information shared/ presented in teleworking is secured appropriately.

3.5 Physical & environmental controls

1. Secure Area Objective:

a) To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.

2. Physical Security Perimeter:

a) Appropriate physical security controls shall be implemented to protect areas that contains sensitive and critical information and information processing facilities such as data centre, server rooms, office area where sensitive physical documents stored or processed to prevent unauthorized physical access, damage, and interference.

b) Physical access to the critical systems should be revoked immediately if the same is no longer required.

c) Periodic audits and mock drills shall be conducted for addressing the issue of physical threats.

3. Physical Entry Controls:

a) Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

4. Securing Offices, Rooms, and Facilities

a) Appropriate physical security controls shall be implemented to secure offices, rooms and facilities that contains sensitive information.

5. Working in Secure Areas

a) Physical protection and guidelines for working in secure areas should be designed and applied.

6. Protecting against External and Environmental Threats
   a) Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

7. Public Areas, Delivery, and Loading Areas
   a) Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

8. Equipment Security Objective:
   a) To protect equipment's from physical and environmental threats to prevent loss, damage, theft or compromise of assets and interruption to the Organizations' activities.

9. Equipment Siting and Protection
   a) Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

10. Supporting Utilities
    a) Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities such as electricity, water supply, sewage, heating/ventilation, and air conditioning.
    b) UPS, Back-up Generator, Air-conditioning supporting equipment shall be adequate and periodically tested/monitored.

11. Cabling Security
    a) Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

12. Equipment Maintenance
    a) Equipment should be correctly maintained to ensure its continued availability and integrity.

13. Security of Off-Premises/Off-Site Equipment
    a) Security should be applied to off-site assets taking into account the different risks (damage, theft or eavesdropping etc.) of working outside the organization's premises.
    b) Adequate insurance cover should be in place to protect off-site and in transit equipment, wherever appropriate.

14. Secure Disposal or Re-use of Equipment
    a) Any sensitive data and licensed software shall be removed or securely overwritten prior to disposal or re-use of equipment containing storage media.
    b) Physical Assets including storage media and systems shall be disposed of appropriately using suitable mechanisms such as cleaning, wiping, overwriting, degaussing etc.

15. Removal of Asset
    a) Critical equipment, sensitive information or software should not be taken off- site without prior authorization.

16. Unattended User Equipment
    a) Users should ensure that unattended equipment has appropriate protection.

4. IT & INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK

4.1 Risk Assessment and Management

SVIPL shall have a standard Risk Management policy. The risk management policy shall also include IT related risks, including the Cyber Security related risks, and the Risk Management Committee of the Board (RMC) in consultation with the ITSC shall periodically review and update the same at least on a yearly basis.

4.2 IT and Information Security Risk Management Framework

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment.

1. Risk Assessment Process

The risk assessment methodology encompasses nine primary steps,

i. System Characterization
ii. Threat Identification
iii. Vulnerability Identification
iv. Control Analysis
v. Likelihood Determination
vi. Impact Analysis
vii. Risk Determination
viii. Control Recommendations
ix. Results Documentation

2. Risk Mitigation Process

Risk Mitigation as below;

i. When vulnerability (or flaw, weakness) exists → implement assurance techniques. to reduce the likelihood of a vulnerability's being exercised.
ii. When a vulnerability can be exercised → apply layered protections, architectural. designs, and administrative controls to minimize the risk of or prevent this occurrence.
iii. When the attacker's cost is less than the potential gain →apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
iv. When loss is too great → apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss.

3. Evaluation and Assessment Process

i. Risk management should be conducted and integrated in the SDLC for IT systems as it is a good practice and supports the organization's business objectives or mission.
ii. The periodicity shall be yearly basis and as and when there are major changes to the IT system and processing environment.
iii. Security infrastructure configuration and security policies shall be reviewed yearly basis.

4. Key Roles

i. Senior Management- Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission.
ii. Chief Technology Officer (CTO)- The CTO is responsible for the IT planning, budgeting, and performance including its information security components. Decisions made in these areas should

be based on an effective risk management program.

iii. Chief Information Security Officer (CISO)- The CISO is responsible to risk related to information security, data security and cyber security related risk.

4.3 Risk Assessment

1. Risk assessment for each information asset within the scope shall be guided by appropriate security standards/ IT control frameworks.
2. Review of security infrastructure and security policies shall be performed at least annually, factoring in their own experiences and emerging threats and risks.
3. Adequate steps shall be taken to tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.

Refer Risk Assessment Template

4.4 Vulnerability Assessment (VA) / Penetration Testing (PT)

1. Critical information systems shall be identified and approved by Board.
2. For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. Also, VA/ PT shall be conducted of such information systems throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.).
3. For non-critical information systems, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA/ PT.
4. In the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/ PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, it shall be ensuring that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC.
5. Ensure that the vulnerabilities detected are promptly remediated so as to avoid exploitation.
6. Approach document shall be prepared to conduct of VA/ PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects.
7. Exception to closure of VA/PT observation shall be documented with necessary approvals.

4.5 Cyber Incident Response and Recovery Management

1. **Incident detection and Monitoring**

i. All the devices/appliances/applications of the organisation including servers, endpoints, network devices, applications and any other IT resources shall be integrated with the Security Operations Centre – Monitoring solution.

ii. Logs of all the above-mentioned devices shall be monitored for any anomalies and

iii. Incidents shall be raised, if any, post analysis of the logs and corresponding alerts shall be generated.

2. **Response and Recovery**

i. Alerts shall be raised post investigation including forensic and impact analysis to mitigate and prevent incidents.

ii. Response and recovery shall be aimed at timely restoration of the systems affected, if any, in line with the Business Continuity policy.

3. **Incident Types**

i. The incidents should be classified as non-IT incidents (e.g. unauthorized access to confidential information, loss of theft of Mobile, laptop or IT equipment etc.) and IT incidents (e.g. DDOS, Email spoofing etc.)

4. **Incident Reporting / Logging**

i. All IT incidents should be logged in Tool by tech Support.
ii. All Non- IT Incidents should be informed to Admin/HOD, Tech Support Team.
iii. IT Incidents should be classified as per Service Catalogue as discussed with Service provider and signed off by CISO/Head IT Infra.

5. **During Working Hours**

i. Reporting shall be done through appropriate management channels as quickly as possible.
ii. Tech Support shall decide the severity level of the IT incident and shall inform Head IT Infra and CISO Team.

6. **During Non-Working Hours/ Holidays**

For incidents that happen after normal working hours, following sequential actions shall be followed:

i. The concerned employee shall focus on containing the damage and dealing with the crisis using all available assistance.
ii. The concerned authority shall be reached to inform on the incidents within a reasonable time and as early as possible.
iii. The reporting procedure shall remain the same.

7. **Escalation Matrix**

i. All incidents shall be immediately reported to the CTO and CISO Team.

8. **Recovery and restoration**

i. The primary focus is to contain the incident once it's verified and to prevent the incident from horizontal or vertical movement.
ii. Logs shall be investigated and the concerned shall be notified of all the actions.
iii. Recovery from backup or shifting to secondary/DR site shall be carried out, if necessary to ensure Business Continuity.

9. **Analysis of the Incident**

i. The respective teams shall collect evidence and audit trails of all the incidents from the relevant personnel.
ii. If the incident cannot be resolved by known means, then root-cause analysis shall be carried out by the concerned departments.
iii. Based on the analysis appropriate workarounds, preventive or corrective controls shall be suggested.
iv. The root cause analysis and the action taken report shall be submitted to the CISO Team for approval.

10. **Management Reporting of the Incident**

i. The IRA shall compile a report of all IT and cyber incidents if any and forward it to CISO monthly basis.
ii. A copy of the report shall also be sent to the Head HR for taking disciplinary actions, if required.
iii. All incidents shall be reported to Board, senior management, and customer as and when required and to Reserve Bank of India as per regulatory requirement.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY MANAGEMENT

5.1 Business Continuity Management

1. The BCP and DR policy shall adopt best practices to guide its actions in reducing the likelihood or impact of the disruptive incidents and maintaining business continuity. The policy shall be updated based on major developments/ risk assessment.

2. BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents.

5.2 Disaster Recovery Management

1. BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents.
2. Any major issues observed during the DR drill shall be resolved and tested again to ensure successful conduct of drill before the next cycle.
3. The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.
4. DR readiness shall be tested under different scenarios for possible types of contingencies, to ensure that it is up-to-date and effective.
5. Backup data shall be taken and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorised access.
6. The DR architecture and procedures are robust, meeting the defined RTO and RPO for any recovery operations in case of contingency.
7. Minimal RTO (as approved by the ITSC) and a near zero RPO for critical information systems shall be achieved.
8. In a scenario of non-zero RPO, methodology for reconciliation of data while resuming operations from the alternate location shall be documented.
9. The configurations of information systems and deployed security patches at the DC and DR shall be identical.

6. INFORMATION SYSTEM (IS) AUDIT POLICY

The objective of this section defines the scope of audit along with the roles and responsibilities of the IS Audit function.

6.1 Purpose and Authority

The IS Audit function will have sufficient authority, stature, independence, and resources thereby enabling internal auditors to carry out their assignments properly.

6.2 Governance

The Audit Committee of the Board (ACB) of the Board shall be responsible for exercising oversight of IS audit of the SVIPL entity. The IS Audit policy shall be reviewed & approved by the ACB at least annually.

6.3 Competence

1. Requisite professional competence, knowledge and experience of each internal auditor is essential for the effectiveness of internal audit function to conduct the IS Audit.
2. The areas of knowledge and experience may include financial entity's operations, accounting, information technology, cyber security, data analytics, forensic investigation, among others. The collective skill levels should be adequate to audit all areas of the entity.
3. External resources may also be used for IS Audits based on the expertise but however, it will be within the overall ambit of the Internal Audit function housed with SVIPL Limited.

6.4 Objectives of the IS Audit

It is essential that the system assets/ resources and IT processes are dependable, always controlled and protected from misuse. It is necessary that all the IT systems are audited at periodic intervals and report on

their status are submitted to the Audit Committee of the Board to ensure the following:

1. **Safeguard Information System Assets/ Resources and IT processes.**

Monitoring effective usage of hardware, software, networking and communication facilities, people, system documentation, etc.

Evaluation of infrastructure (Power, Air conditioning, Humidity control, physical security, surveillance and monitoring, incident monitoring, etc.) in safeguarding of IS resources.

2. **Verification of Data Integrity and Security**

Validation of the data entered and captured in the system is duly authorized, verified and completed and that proper control is exercised at all stages viz. Data protection, input, verification, output, modification, deletion, electronic transmission, etc. to ensure the authenticity and correctness of the data.

3. **Evaluation of system effectiveness and efficiency**

Evaluate the extent to which organizational goals, business and user needs have been met and to determine whether the resource utilization is effective and efficient while achieving the desired objectives.

4. **Verification of compliance to internal guidelines and procedures in addition to legal, regulatory, and statutory requirements Evaluation of compliance on**

i. Adherence to maintenance of Integrity, Confidentiality, Reliability and Availability and Dependability of information resources
ii. Legal, regulatory, and statutory requirements
iii. Internal Policy and Procedures based on prescribed standards and guidelines.

6.5 Approach

The entity shall carry out the IS audit using a risk-based approach. A continuous auditing approach may be adopted for critical systems if required.

6.6 Scope of IS Audit

The scope of IS Audit includes the collection and evaluation of evidence/ information to determine whether the Information System in use safeguards the assets, maintain data security/ integrity/ availability, achieve the organizational goals effectively and utilize the resources efficiently.

Changes to the scope of IS Audit will be reviewed and recommended by the Audit Committee annually.

1. **IT Governance**

The IS Audit evaluates the effectiveness of the organizational IT Governance framework, which includes the policies and procedures, and processes that govern the use of IT in the organization. This includes assessment of organization's IT strategy, risk management practices including the independence of the IS function/ CISO from the Technology function, and compliance with relevant laws and regulations.

2. **Information Security**

It evaluates the effectiveness of the organization's information security controls, including access controls, encryption, firewalls, intrusion detection and prevention, and other security measures designed to protect the confidentiality, integrity, and the availability of the organization's data.

3. **IT Operations**

It evaluates the effectiveness of the organization's IT operations, including the management of organization's IT infrastructure, the effectiveness of the organization's IT service management practices, and the organization's ability to respond to and recover from IT incidents and disruptions.

4. **System Development**

It evaluates the effectiveness of the organization's System Development Life Cycle (SDLC) processes, including requirements gathering, design, testing, and deployment.

5. **Business Continuity Planning**
It evaluates the organization's ability to maintain business continuity in the event of disaster or other disruptive event. This includes an assessment of the BCP, including risk assessments, business impact analysis, and the development of disaster recovery plans.

6.7 Audit Universe

The Audit Universe will include the following:

1. **IT General Controls** – Physical and Logical access controls including logs, change management controls, data backup and recovery controls.
2. **IT Application controls** – Input controls, Data validation, processing controls, output controls, data file controls
3. **Network security controls** – network vulnerabilities, physical access controls, network security including wireless networks.
4. **Data migration controls** – data mapping strategy and plans review, operational changes, implementation readiness, pre -migration testing, data conversion verification, post implementation
5. **Business Continuity and Disaster management** – Policies and procedures review, Risk Assessment, Business Impact analysis, development, and implementation of BCP DR plans, training, and testing

6.8 Audit Frequency

The IS Audit will be done once a year along with the IT Internal Audit.

6.9 IS Audit Plan

1. A detailed IS audit plan will be prepared to ensure that all critical information assets are covered with the above described three stage approach.
2. The IS audit calendar should be planned and scheduled in such a way that the audits should not become hindrance to the day-to-day operations of the business.

6.10 Audit Reporting

The Audit findings will be rated High, Medium or Low based on the criticality and the severity of impact. Management response along with the due date for implementation of remediation action plan will be obtained for the audit findings.

7. IT SOLUTION DELIVERY

7.1 System Acquisition, Development & Maintenance Policy

A standard approach which ensures compliance with functional, security, performance and applicable regulatory requirements shall be followed for software development/procurement.

1. **Procurement Strategy**

i. Organization should treat all vendors with fairness and ensure that they are given the same level of information when preparing quotations or tenders as the case may be.

ii. Quotations and tenders should be evaluated not only on competitiveness in pricing but also factors such as the quality of the products/services and track records of the bidders.

2. **Procurement Proposal**

i. A proposal containing the details of the proposed procurement request should be defined and approved.

3. **Supplier Database**

i. A database should be maintained by procurement team in order to store performance records and results of the IT supplier evaluation. Database should be referred whenever a new IT procurement process is being initiated or considered.

ii. Centralized database for all existing Technology, IT Hardware & Software inventory should be maintained and reviewed annually.

4. **Technology Refresh**

i. The existing applications, IT systems and technology should be assessed at least yearly for a need of technology refresh. The assessment of new technology should follow the complete procurement process.

7.2 Contract Management

IT services shall have well defined contract agreements that specify scope of services and establish accountability of suppliers.

1. **Contract Requirements**

i. Supplier Contract Agreements together with other supporting service agreements and corresponding procedures should be defined with suppliers providing services related to management of SVIPL 's information assets.

ii. Supplier Management - SVIPL shall establish and manage the supplier relationships so as to ensure quality of service provided by suppliers.

2. **Maintenance of Supplier and Contact Database**

i. Supplier and contact database for all the IT supplier relationships should be maintained with IT- Partner Relationship Department.

3. **Supplier and Contract categorization and Risk Assessment**

i. Risk assessment of suppliers should be performed to ensure availability and continuity of services procured by the respective Verticals.

4. **Contract Review, Renewal and Termination**

i. The supplier contracts should be reviewed at least on annual basis by the respective department and status to be confirmed to IT- Partner Relationship Department.

ii. In case of termination of contract, supplier should be informed and exit transition plan should be defined. Transition plan should include Knowledge transfer and handholding activities for SVIPL or new supplier.

8. IT OUTSOURCING

The objective of this section is to identify risks associated with external parties and establish appropriate controls to ensure security in line with the SVIPL Outsourcing Policy.

8.1 Framework and Governance over decision to outsource.

1. The IT function and the senior management shall ensure that sound and responsive risk management practices for effective oversight, due diligence and management are in place for outsourcing of IT activities as per the policy framework.
2. The IT outsourcing propositions shall be put to the IT steering committee for approval (only if core IT activity is being outsourced).

3. Risk assessment and mitigating controls to be defined as per the Policy.
4. The current material/significant IT outsourcing arrangements shall be reviewed on an annual basis by the IT steering committee to assess and ensure that the risks posed by such a function are low and adequately mitigated. The board shall be informed of any material risk arising of an outsourcing arrangement in a timely manner.

8.2 Evaluating Vendors Outsourcing arrangements

1. All requirements for outsourcing of IT activities shall clearly be defined in the RFI/RFP's floated to vendors. Ensure the below clauses/conditions are contractually enforced by the outsource vendors on their sub-contractors.
2. Maintaining, confidentiality, integrity, availability of internal data, customer, and compliance data (to the extent relevant to the context of outsourcing).
3. Sign off NDA's by the vendors and their employees (where relevant to context).
4. Secure deletion of SVIPL data and its customer data at the time of contract termination
5. Right for SVIPL to audit the service provider or their sub-contractor to ensure compliance to contract and prevailing regulations/legislations.

8.3 Vendor Risk Assessment

Risk Assessment shall be conducted before engagement to assess the risk and materiality which will include.

1. Concentration of Risk
2. Conflict of Interest
3. Risk associated with Single point of failure.
4. Customer data security and privacy
5. Business Continuity
6. Supply Chain risk
7. Information and Cyber Security

9. TRANSITION

9.1 Change Management Policy

All changes to Information assets must be recorded, classified, assessed for risk, impact and business benefit, approved and implemented in a controlled manner.

1. Change Request & Approval

i. SVIPL to prioritize and responding to change proposals from business.
ii. Perform cost benefit analysis of the changes proposed.
iii. Assess the risks associated with the changes proposed.
iv. Change Approval Board (CAB) should be established for all application groups to take decisions on changes to be implemented. A committee shall be formed to review and approve the change request on basis of business requirement and risk assessment. The committee shall involve Head of application, Head of Infrastructure, Member from Business team, Member from Risk team and Member from CISO team.
v. For every change, a change request should be documented and shared with appropriate authorities for review. A Change Request Form (CRF) shall be documented with business justification, type of change, activity date, time required for change along with change performer details. The outcome of said change shall be documented along with issues raised during change management activity if any. The CRF shall be approved by Change Management Committee before and after change activity.
vi. All change requests should be approved before implementation.

vii. All changes should be compliant with statutory and legal/regulatory requirements as applicable to SVIPL.

viii. RACi Matrix

Activity	Change Manager	Change Owner	Change Coordinator	Change Approver	Business
Raising Change and Gathering Information	I	AR	R	I	R
Classification/Prioritization of Change	I	AR	R	R	CI
Impact Assessment	I	AR	R	AR	CI
Review of Change Request	AR	R	-	R	RCI
Approving of Change Request	AR	CI	-	R	R
Release and Test Acceptance	AC	R	R	CI	I
Change Implementation	AR	R	R	CI	I
Verify of Change Completion	AR	R	I	I	R
Post Implementation Review	R	AR	R	I	CI
Roll back	A	R	R	CI	I

2. Implementation of Change

i. Change should be implemented based on the implementation plan approved as part of change request.

ii. Post Implementation, business verification review should be performed to confirm if the change is working as desired.

iii. Mechanism shall be established to recover from failed changes/ patch deployment or unexpected results.

3. Documentation of Change

i. All Documents related to change request should be retained for audit purpose.

9.2 Data Migration

SVIPL shall ensure migration of data between systems or with any vendor in controlled manner to ensure data Confidentiality, integrity and authenticity.

1. Data migration requirement should be identified, analysed and impact of data migration should be communicated to respective stakeholders.
2. An identification and feasibility study should be conducted, reviewed and approved before initiating the data migration activity.
3. Procurement of migration software or outsourcing of migration activities shall be performed after thorough assessment of software and vendor resources.
4. Post migration audit/reconciliation should be performed to ensure integrity of data.
5. Two copies of back-up of the data, both pre-migration and post-migration along with reconciliation details should be maintained.

9.3 Project Management

SVIPL shall ensure that all IT projects are approved, managed and tracked in controlled environment to minimize errors and risks associated.

Steps/Activities to be followed in each project will be:

1. Project Initiation
2. Project Planning
3. Resource Planning
4. Project Monitoring
5. Project Closure

10. IT OPERATIONS

10.1 Service Request Management

SVIPL shall have a service request fulfilment process to provide quick and effective access to standard services which can be used to improve productivity and the quality of business services and products.

1. **Logging Service Request**

   Service request should be raised by user department either by writing an email/ or using a portal (service desk) for the same.

2. **Approval for Service Request**

   Cost of fulfilling the request should be established. Estimate of the cost should be produced And submitted to the user department/authorized dept for management/financial approval.

3. **Request Fulfilment**

i. Request fulfilment activity should depend upon the nature of the Service Request. Simple requests should be completed by service desk, while others should have to be forwarded to specialist group/ technical team for fulfilment.

ii. Service desk should monitor and track progress and keep users informed about the request fulfilment.

10.1 Asset Management

SVIPL's IT assets shall be controlled and managed throughout the asset lifecycle.

1. **Asset Lifecycle**

i. IT Asset acquisition request should be approved by respective department head and CTO.

ii. All assets should be identified, classified and protected during their whole lifecycle as per the Information and Cyber Security Policy.

iii. All SVIPL's Hardware IT Assets should be insured for damage, theft or loss.

iv. The IT Assets should have a unique identification code and it should be maintained in the centralized database.

v. In case the retired IT assets needs to be destroyed, the process for disposal of media should be followed.

vi. Asset Inventory should be updated upon retirement and disposal of assets.

2. **Asset Records**

i. An inventory of all assets shall be maintained and updated. The inventory should at least include the details of unique asset identification number, the asset owner, contact details, asset allocation period.

ii. An inventory of all software licenses shall be maintained and updated in the database.

3. **Asset Review**

i. The inventory of assets should be reviewed at least annually.
ii. The inventory of software licenses should be reviewed at least annually.

10.2 Application Management

SVIPL shall manage the entire life cycle of application including maintenance to provide resilience, availability of application in efficient and cost-effective manner.

1. Application Maintenance

i. Application Portfolio should be created with the record of the applications and content. Portfolio should be linked to supporting infrastructure and devices.
ii. All resources required for managing and supporting the applications should be trained at least annually.

2. Continuity of Operations

i. Applications should be monitored for capacity, performance and availability.
ii. Application should have a comprehensive EOD process plan to conduct activities in off business hours.

3. Application Assessment

i. Risk Matrix / Criticality Rating for the applications based on their risk criticality should be defined and reviewed at least annually.
ii. Risk Assessment should be conducted for all applications on periodic basis.
iii. Vulnerability Assessment and Penetration Testing should be conducted for all applications on periodic basis at a frequency and the test report with the action taken and mitigation plan to be submitted to CTO/COO.

4. Training

i. Applications should be managed by personnel with appropriate technical skill sets and training.

10.3 Infrastructure Management

SVIPL shall ensure efficient management of the IT infrastructure and build the technical capabilities to manage IT Infrastructure.

1. IT Infrastructure Management

i. Roles and responsibilities should be defined for managing and monitoring the IT infrastructure.
ii. All IT infrastructure related incidents/ problems should be logged in the service desk.
iii. Identified risks should be mitigated and communicated to stakeholders.
iv. Network architecture diagrams as applicable to be maintained for any
v. application's infrastructure.

2. Continuity of Operations

i. Continuity should be ensured by executing the daily and periodic processes.
ii. IT Infrastructure should be continuously monitored for threats and operational issues.

3. Training

i. Technical skills development activity should be conducted for the users/ teams, responsible for operating, maintaining and supporting the IT infrastructure at least half annually.

10.4 Access Management

i. Apply environment/ instance design principles/ environmental controls

ii. Separate instances shall be maintained for development, test and production environment.
iii. Access to any system shall be provided on least privilege basis.
iv. Access to production environment to be limited to a small set of privileged users only.

10.5 Back up Policy

SVIPL shall manage the entire life cycle of application including maintenance to provide resilience, availability of application in efficient and cost-effective manner.

1. Backup Strategy
   i. Information backup and recovery procedures should be established and implemented as per legal, regulatory and contractual requirements.
   ii. Information backup frequency and retention period of backup should be defined based on identified requirements of backup.
   iii. Business-critical data should be duplicated and stored at different site. In case of backup media, the same should be kept in fireproof safe
   iv. Backup logs should be stored with appropriate access rights assigned to them. The backup operator should carry out a log analysis for all failed backup and restorations and take necessary actions including raising an incident.
   v. Restoration testing should be conducted for the backed-up data on regular basis to check the integrity and adequacy of the backup.

10.6 Patch Management

1. The purpose of this policy is to define patch management of the organisation's information systems, networks, data, databases, and other information assets.
2. All information technology systems, software, databases, applications, network and other information resources that are being used by the organization to conduct its business.
3. All the IT systems including servers, network & security devices, operating systems, applications, any information processing devices and applications shall be properly configured to install the recommended software updates to maintain operational efficiency.
4. Patches shall be identified and categorized according to their priority.
5. Security patches shall be given priority and deployed as soon as the testing is complete.
6. Servers managed by the organization shall apply regular patches as per the schedule.
7. Patches for business-critical systems shall be carried out manually in a controlled manner.
8. All patches shall be tested prior to full implementation by deploying in a test environment that is similar to the production environment, wherever applicable.
9. A remediation plan that allows for return to the previous stable state prior to the patch deployment shall be devised in case a roll back is required.

11. IT SUPPORT FOR BUSINESS MIS

11.1 IT Support for Business MIS formulation and Compliance

The business user group shall be responsible for design of MIS requirements for monitoring business scenarios and requirements such as:

1. **Performance MIS** - A dashboard for the Top Management summarizing financial position vis-à-vis targets. It may include information on trend on returns on assets across categories, major growth business segments, movement of net-worth etc.

2. **Functional requirement for automation of Fraud alerting & design of Transaction Anomaly MIS System** - The business teams may evaluate conceptualizing from time to time the functional requirement for aspects like:

3. **Account Classification** - System enabled identification, alerting and classification of Special Mention Accounts and NPA as well as generation of MIS reports in this regard.

4. **Lending Transaction MIS** -The MIS should facilitate pricing of products, especially large ticket loans and any alerts on deviation on lending terms.

5. **Regulatory reporting & MIS** - The MIS should capture regulatory requirements and their compliance.

6. **Financial Reports** including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. (also regulatory compliance at transaction level)

7. **Treasury Transaction Reports**- MIS Reports relating to treasury operations (including anomaly alerts like trade limit breaches, high volume transactions).

8. **Fraud analytics and alerting** - Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. The regulatory requirement of reporting fraud to RBI should be system driven.

9. Integration of systems to regulatory reporting portals.

10. IT team along with the business teams shall provide an adequate infrastructure and support in updating business applications for generating MIS and automated control features wherever possible.

Place: Mumbai
Date: 21/04/2025