Code of Conduct Guidelines

Code of Conduct Guidelines

Applicable to all Employees and Suppliers

SBI Card and Payment Services Ltd. (hereinafter referred to as "SBICPSL" or the "Company"), is committed to eminent standards of ethical business conduct. In doing so, SBICPSL has created an invaluable asset – its reputation for high standards of ethical business conduct and integrity. We base all our business relationships and associations on honest, lawful, efficient and fair practices and expect our employees and suppliers to adhere to the same, thereby ensuring that we consistently meet our integrity commitments.

In this regard, SBICPSL has prepared this **Guide for Its Employees & Suppliers.**

Applicability:

Code of Conduct Policy applies to all SBI Card employees. It also applies to SBI Card suppliers, contractors, third parties representing SBI Card and consultants (collectively referred to as 'suppliers'). Suppliers and their employees, workers, sub – contractors and representatives must also comply with the policy.

Employees handling Suppliers are expected to share these guidelines with the suppliers and ensure that only those Suppliers are onboarded who are willing to abide with the Company policy.

Suppliers are expected to collaborate with Company's employees so that Company employees can continue to stay complaint and meet the integrity commitments.

The Guide is divided into four parts:

- Code of Conduct
- Compliance Obligations
- Responsibilities of Suppliers
- How to Raise a Concern

Employees & Suppliers should go through this Guide carefully. Suppliers are responsible for ensuring that they and their employees, workers, representatives and sub-contractors comply with these standards. Suppliers shall contact the relevant Company Manager or any Company Compliance Official if they have any questions about this Guide or the standards of business conduct.

Code of Conduct

SBICPSL has established a Code of Conduct that imbibes the Company's commitment to ethical business practices. All SBI Card employees are expected to understand, imbibe and display the Company's values at all times:

- **Act with integrity:** We do what is right, not what is easiest. We are honest and ethical in all that we do, at all times and in every situation.
- **Earn Trust:** We honour our commitments. To customers, to employees, to partners and to society. We say what we mean and we mean what we say.
- **Respect for All:** We treat others as we expect to be treated; with respect, dignity and honour. Especially when things go wrong.
- **Lead with Courage:** We challenge convention and pursue our convictions. Irrespective of the outcome, we always own our decisions and choices.
- **Customer First:** Customers are at the heart of all our choices. We understand that we exist because of our customers and the privilege to serve them has to be earned every day.

Each employee is personally accountable to ensure that they follow this Code of Conduct –

- Obey all applicable laws and regulations that govern our business.
- Be trustworthy, fair and honest in all our activities and relationships.
- Create and sustain a work environment in which diversity is respected and all employees are treated fairly.
- Avoid all conflicts of interest between work and personal affairs.
- Through leadership at all levels, create a culture where ethical conduct is recognized, valued and exemplified by all employees.
- Provide a safe workplace and protect the environment.

No matter how high the stakes, no matter how great the challenge, SBICPSL will do business only by lawful and ethical means. When working with customers and Suppliers in every aspect of our business, SBICPSL will not compromise its commitment to integrity.

Compliance Obligations

It's the responsibility of all employees to comply with the requirements of the Compliance guidelines set forth in this guide. The guidelines detailed in this document are in addition to business – specific Compliance procedures and guidelines.

A summary of some of the important compliance obligations and Code of Conduct Policy guidelines are as under -

Improper Payments

- Always adhere to the highest standards of honesty and integrity in all contacts on behalf of the Company. Never offer bribes, kickbacks, illegal political contributions or other improper payments to any customer, external party, or third parties.
- Follow Corporate and business guidelines regarding gifts and entertainment and other business courtesies and do not offer gifts or provide any entertainment to a customer or supplier without prior approval of the relevant approving authority. Make sure all business entertainment and gifts are lawful and disclosed to the other party's employer.
- Employ only reputable people and firms as Company representatives and understand and comply with requirements governing the use of third party representatives.
- Maintain accurate records, and accounts that correctly reflect the true nature of all transactions.

Money Laundering Prevention

- Follow all applicable laws, regulations, Company policy and Reserve Bank of India ('RBI') Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT) that prohibit money laundering and that require the reporting of cash or other suspicious transactions.
- Learn to identify warning signs that may indicate money laundering or other illegal activities or violations of Company policies. Raise any concerns to the Chief Compliance Officer and/or senior management.
- Adhere to risk-based "Know your Customer" due diligence processes on prospective customers.
- Conduct business only with customers involved in legitimate business activities, with funds derived from legitimate sources.
- Follow your business rules concerning acceptable forms of payment.
- Learn the types of payments that might be associated with money laundering (for example, payments on behalf of a customer from an unknown person).

Privacy and Data Security

- Never obtain, use or disclose individual information in ways that are inconsistent with privacy policies or with applicable privacy and data protection laws and regulations.
- Maintain secure business records of Company information, including computer-based information.

- Limit access to Company related information to authorized individuals who need it for legitimate business purposes.
- Prevent unauthorized access, accidental loss, disclosure or destruction of Company related information and assets:
    - Secure storage areas and physical copies of documents.
    - Use strong passwords; don't share your password with anyone.
    - Use only Company approved systems and tools for storage, transmission and backup of Company's information.
    - Do not use personal email, unapproved devices or software to conduct Company business.
    - When posting information online, do not disclose company/customer/employee non-public/personal information, proprietary or other commercially sensitive information. Know the signs of phishing and recognize efforts to improperly acquire Company's information.
    - Communicate as appropriate with customers about cyber security issues.

Working with Suppliers/Third parties

Conduct business with only those suppliers who comply with local and other applicable legal requirements and Company standards relating to labor, environment, health and safety, intellectual property rights and improper payments.

- Vendors and third parties shall also comply with these guidelines set forth by the Company for its dealings with any External Parties.
- Follow applicable laws and regulations covering contracts, transactions and vendor and third-party relationships.
- Ensure proper due diligence when dealing with External Party and agencies.
- Provide a fair, competitive & equal opportunity to vendors and third parties.
- Avoid potential conflicts of interest when selecting a supplier, and never accept improper payments, gifts or other items of value.
- Do not offer, promise, make or authorize the giving of anything of value to an external party and their employees that is inconsistent with Corporate and business guidelines.
- Do not do business with suppliers or subcontractors that are prohibited from doing business with the External party, basis publicly available data.
- Never engage in discussions with external party and their employees or people close to them about prospective employment of non-employees while they can influence decisions affecting the Company.
- Before submitting a proposal to an External Party, review the requirements with all applicable stakeholders and only accept those terms with which Company can comply.
- Report issues and concerns regarding suppliers, third parties and vendors through appropriate open reporting channels.

Regulatory Excellence

- Be aware of the specific regulatory requirements where work is performed and that affects the Company.
- Gain a basic understanding of the key regulators and the regulatory priorities that affect the Company.
- Promptly report any red flags or potential issues that may lead to a regulatory Compliance breach.
- Develop strong processes to anticipate risks**,** including new and changing regulations.
- Assure that coordination with business experts is sought when working with or responding to requests of regulators.
- Always treat regulators professionally, with courtesy and respect.
- Monitor regulatory compliance on an ongoing basis and ensure periodic audits of key processes are conducted.
- Incorporate regulatory requirements into business strategy and processes.

Competition Law

- Understand and follow your business's specific guidelines about contacts with competitors, obtaining and handling competitive information, and participating in trade and professional associations.
- Do not propose or enter into any agreements or understandings with customers restricting resale prices.
- Never propose or enter into any agreement or understanding with a competitor to fix prices, terms and conditions of sale, costs, profit margins, or other aspects of the competition for sales to third parties.
- Never propose or enter into any agreements or understandings with suppliers that restrict the price or other terms at which Company may resell or lease any product or service to a third party.
- Comply with all applicable competition laws and regulations.
- Avoid any contacts with competitors that could create the appearance of improper agreements or understandings, in person or in writing, by telephone, through e-mail or through other means of electronic communication.
- Competitor contacts/Third Party contacts rated 'High Risk' are prohibited;
- Competitor contacts/Third Party contacts rated 'Medium Risk' shall be reviewed and approved by the relevant Function Leader each time prior to such contact taking place;
- Competitor contacts/Third Party contacts rated 'Low Risk' shall be reviewed and approved by the relevant Function Heads prior to the first time such contact is taking place;

- "High Risk/Prohibited / 'Medium Risk' / 'Low Risk' Contacts on topics are as under:

High Risk	Medium Risk	Low Risk
Imposing conditions on sale, distribution or supply of products that may	Membership of and attendance at formal meetings of recognized	Interaction between function and market counterpart as part of business operations, where

impede fair competition in the market	Trade Association / Professional Body	the subject of the discussion is based on public information
Divulging in any form, confidential information about company's products features, pricing, marketing, distribution to a competitor.	Joint lobbying activity whether or not through Trade Associations	Attending conferences/ seminars/ events as participants, guest speakers or jury and not making any statements about the Company or its business, etc.
Any discussion with a competitor, (within or outside a TA), on matters pertaining to fixing prices, market allocation, collusive bidding	JV, Mergers with or acquisitions of a competitor or any of its business divisions	Discussion within a Trade Association (TA) or similar framework (including training events regarding specific ancillary topics in/out of TA ambit HR, AML, fraud, quality control, internal audit, public relations, communications, IT, tax, etc.)
Any discussion with a seller, distributor or customer supplier for exclusive purchase, distribution or supply of products or services for the purpose of restricting competition	Contact with former colleagues/ friends who now work with competitor	Discussion on general economy/market only
		Discussion relating to actual or potential transaction with the concerned party / entity only (including M&A, JV's, outsourcing (but not with competitors)).

Environment, Health and Safety

- Conduct activities in compliance with all relevant environmental and employee health and safety laws and regulations.
- Ensure that all new product designs or changes or service offerings are reviewed for Compliance as per Company guidelines.

- Take care in handling hazardous materials or operating processes.
- Report any potential violation of environmental, health or safety laws, regulations or company practices or requests which violate established EHS procedures.
- Develop and follow safe work procedures to ensure workplace safety and prevent injuries.
- Any conduct on Company premises, while conducting Company business or while otherwise representing the Company, that is intended to cause physical harm to a person or property or otherwise intended to have a negative impact on the safety and/or security interests of the Company is strictly prohibited. This also includes workplace harassment/ sexual harassment and threats (written or verbal).
- Drug abuse, alcohol consumption, being under the influence of or in possession of drugs/alcohol at workplace or within office premises is strictly prohibited.

Fair Employment Practices

- Extend equal opportunity, fair treatment and a harassment-free work environment to all employees, co-workers, consultants and other business associates without regard to their race, color, religion, national origin, sex (including pregnancy), sexual orientation, age, disability, or other characteristics protected by law. In addition ensuring compliances with the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 and rules made thereunder.
- Never disclose employment data to a person who does not have a business need, the authority, or, where required, the subject's consent.
- Comply with all laws pertaining to freedom of association, privacy, working time, wages and hours as well as laws prohibiting forced, compulsory and child labor or trafficking in persons.
- Employment decisions should be made without considering a person's race, color, religion, national or ethnic origin, sex (including pregnancy), sexual orientation, gender identity or expression, age, disability, or other characteristic protected by law.
- Respect human rights everywhere within the company and at places of work and business.

Security and Crisis Management

- Implement rigorous plans to address security of employees, facilities, information, IT assets and business continuity.
- Protect access to facilities from unauthorized personnel.
- Protect IT assets from theft or misappropriation.
- Create and maintain a safe working environment.
- Ensure proper business continuity plans are prepared for emergencies.
- Screen all customers, suppliers, agents and dealers against international economic sanctions/ terrorist watch lists (for this purpose, a watchlist screening may be done based on recommended watchlists by regulators.)
- Workplace violence is strictly prohibited. Identify and report indicators or incidents of workplace violence to the concerned manager, HR, Security Leader or Compliance.

- Implement rigorous Security and Crisis Management (SCM) plans designed to ensure the security of people and operations.
- Ensure to Include under Security and Crisis Management (SCM) plans, a process for identifyingand protecting against, the risks posed by man-made or natural incidents that affect our people, facilities, information technology assets and systems, or products and services.
- Communicate, as appropriate, about prevention, emergency response and business continuation with the Company, the media and the public.
- Conduct rigorous background checks on new hires and third parties as permitted by law.

Conflicts of Interest

- Financial, business or other non - work related activities must be lawful and free of conflicts with one's responsibilities to the Company.
- Report all personal or family relationships, including those of significant others that may appear to be in conflict with the job responsibility or employment at SBI Card.
- Do not use Company equipment, information or other property (including office equipment, e-mail and computer applications) to conduct personal or non-SBICPSL business without prior permission from the appropriate Manager.
- Misusing Company's resources, position, rights or influence is prohibited. Even when nothing wrong is intended, the perception of a conflict of interest may have negative effects.
- Do not accept gifts other than those of nominal value from suppliers, customers or competitors.
- Obtain prior approval before accepting officer or director positions with an outside business or not-for-profit organization.
- Obtain prior approval from concerned manager, HR and Compliance before hiring, promoting or directly supervising a family member or close friend.

Controllership and Fair Reporting

- Keep and report all Company records, in an accurate, timely, complete and confidential manner. Release records to third parties only when authorized by the Company.
- Follow Company's general accounting procedures as well as all standards, laws and regulations for accounting and financial reporting of transactions, estimates and forecasts.
- Financial statements and reports prepared for or on behalf of the Company (including any component or business) must fairly present the financial position, results of operations, and/or other financial data for the periods and/or the dates specified.
- Comply with all Company policies and applicable laws and regulations relating to the preservation of documents and records.
- Maintain effective processes and internal controls that fairly reflect transactions or events, as well as prevent or detect inappropriate transactions.
- Never engage in inappropriate transactions, including those that misrepresent the reporting of other parties such as customers or suppliers.

- Manipulation, falsification, omission or alteration of company, customer, employee or personal information is strictly prohibited.

Insider Trading or Dealing & Stock Tipping

- Never buy, sell or suggest to someone else that they should buy or sell stock or other securities of any company (including JV parent companies) while being aware of significant or material non-public information ("inside information") about that company, as and when applicable. Information is significant when it is likely that an ordinary investor would consider the information important in making an investment decision.
- Do not pass on or disclose inside information unless lawful and necessary for the conduct of business and never pass on or disclose such information if you suspect that the information will be used for an improper trading purpose.

Intellectual Property

- Identify and protect Company intellectual property.
- Consult with Company legal counsel before soliciting, accepting or using proprietary information of outsiders, disclosing Company proprietary information to outsiders or permitting third parties to use Company intellectual property.
- Do not provide Company's proprietary information to third party without proper internal approval(s) and the necessary confidentiality agreement with the third party.
- Do not bring, access, keep, share or use a third party's proprietary information (e.g. proprietary information from a previous employer) without first consulting with and receiving prior approval from concerned Manager, HR and Legal counsel.
- Respect valid patents, trademarks, copyright materials and other protected intellectual property of others; and consult with Company legal counsel for licenses or approvals to use such intellectual property.
- Do not use any source code or other software from a third party in any of Company's product or as a tool without obtaining prior approval.

Responsible behavior on Social Media

In addition to the above compliance obligations, the guidelines on usage of social media should be adhered to.

- Establishing/ promoting any group/community on any internet site which uses the name or logo of SBI Card or becoming member of any such group or community unless such group is expressly created or permitted by the SBI Card, is prohibited.
- Using any ID other than employee's real name and/or using business email address on personal blogs or public social networking sites is also prohibited.

- Employees must never post, forward, upload or express any remarks/ views on any internet site or social media or share a link of any content on social media which may be defamatory, indecent, abusive, discriminatory or derogatory to the Company or its officials/ employees in their official capacity and/or may damage the reputation of the Company or any of its employees.
- Employees are also prohibited to discuss, disclose, post, forward, upload or share any content that may breach intellectual property rights or is related to any colleagues, competitors, customers, suppliers or other third parties including their personal details on any internet site or social media without prior consent. Expressing/ forwarding any views or opinion on behalf of the Company, using the Company name while expressing any views and publishing/ forwarding any official/ internal Company information is not permitted.
- Employees must also refrain from writing about, commenting on, or answering questions regarding any legal matter, litigation, or party to a lawsuit involving SBI Card.
- Employees shall use the social media sites judiciously in personal capacity.
- All employees shall be personally responsible for the content they publish/forward in any form on social media.

Responsibilities of Suppliers

Overview

The Company has zero tolerance towards all forms of bribery and/or corruption/Improper Payments and it has resolved to initiate proactive measures to mitigate such risks by putting adequate controls, accordingly all Vendors/Suppliers at all times shall comply with all applicable laws including Prevention of Corruption Act,1988.

SBICPSL will only engage in business with vendors and third parties that comply with all applicable legal and regulatory requirements. Today's regulatory environment requires that the Company and its Suppliers continue to be knowledgeable and compliant with all applicable regulations.

A Supplier's commitment to compliance with their contractual obligations, and all applicable laws and regulations is the foundation of a mutually beneficial business relationship with the Company.

The Company expects its Suppliers, and any Supplier's subcontractors (if applicable), that support Company's work to be honest, truthful and accurate when dealing with any Third Party or any External Parties.

As stated above, Company requires and expects each Supplier to comply with all applicable laws and regulations. Unacceptable practices by a Supplier include:

- **Minimum Age:** Employing workers younger than eighteen (18) years of age or the applicable required minimum age, whichever is higher.

- **Forced Labour:** Using forced labour, or workers subject to any form of compulsion or coercion, or the

trafficking in persons in violation of applicable laws or regulations.

- **Environmental Compliance:** Lack of commitment to observing applicable environmental laws and regulations. Actions that the Company will consider as evidence of a lack of commitment to observing applicable environmental laws and regulations include:

- Failure to maintain and enforce comprehensive environmental management programs.
- Failure to maintain and comply with all required environmental permits.
- Permitting any discharge to the environment in violation of law, issued/required permits, or that would otherwise have an adverse impact on the environment.

- **Health & Safety:** Failure to provide employees a workplace that meets applicable health, safety and security standards.

- **Human Rights:**
  - Failure to respect human rights of the employees of the Supplier .
  - Failure to observe applicable laws and regulations governing wage and hours.
  - Failure to prohibit discrimination, harassment and retaliation.

- **Code of Conduct:** Failure to maintain and enforce Company policies requiring adherence to lawful business practices, including prohibition against bribery of any kind.

- **Business Practices and Dealings with the Company:** The Company also prohibits a company Supplier from offering or providing Company employees, representatives or customers or any External party with any gifts or entertainment, other than those of nominal value to commemorate or recognize a particular Company Supplier business transaction or activity. In particular, a Company Supplier shall not offer, invite or permit Company employees and representatives to participate in any Supplier or Supplier-sponsored contest, game or promotion except for justified business and/or training purposes and duly approved by Function Leader.

- **Unusual Business Entertainment of Company Employees and Representatives:** Unusual Business entertainment should not be offered to a Company employee or representative by a Supplier.

- **Collusive Conduct and Company Procurements:** Sharing or exchanging any price, cost or other competitive information or the undertaking of any other collusive conduct with any other third party to the Company with respect to any proposed, pending or current Company procurement.

- **Intellectual Property & other Data and Security Requirements:** Failure to respect the intellectual and other property rights of others, especially SBICPSL. In that regard, a Company supplier shall:
  - Use Company information and property only for the purpose for which they are provided to the Supplier and for no other purposes.
  - Take appropriate steps to safeguard and maintain the confidentiality of Company proprietary information, including maintaining it in confidence and in secure work areas and not disclosing it to third parties (including other customers, subcontractors, etc.) without the prior written permission of the Company.
  - If requested to send data over the Internet, encrypt all such data.
  - Observe and respect all Company patents, trademarks and copyrights and comply with such restrictions or prohibitions on their use as the Company may from time to time establish.

- Comply with all applicable rules concerning cross-border data transfers (where applicable).
- Maintain all personal and sensitive data, whether of Company employees or its customers in a secure and confidential manner, taking into account the applicable legal & regulatory requirements and the relevant Company policies provided to the Supplier.

- **Trade Controls & Customs Matters:** The transfer of any Company technical information to any third party without the express, written permission of the Company. Failure to comply with all applicable trade control laws and regulations in the import, export, re-export or transfer of goods, services, software, technology or technical data including any restrictions on access or use by unauthorized persons or entities, and failure to ensure that all invoices and any customs or similar documentation submitted to the Company or External party in connection with transactions involving Company accurately describe the goods and services provided or delivered and the price thereof.

- **Use Subcontractors or Third Parties to Evade Requirements:** The use of subcontractors or other third parties to evade legal requirements applicable to the Supplier and any of the standards set forth in this Guide is also prohibited.

The foregoing standards are subject to modification at the discretion of SBICPSL. Suppliers shall contact the concerned Company Manager or any Company Compliance Officer if they have any questions about these standards and/or their application to particular circumstances. Each Company Supplier is responsible for ensuring that its employees and representatives understand and comply with these standards. Company will do business only with those Suppliers that comply with applicable legal and regulatory requirements and reserves the right, based on its assessment of information available to the Company, to terminate, without liability to the Company, any pending purchase order or contract with any Supplier that does not comply with the standards set forth in this section of the Guide.

How to Raise a Concern

Each Employee and / or Supplier is expected to promptly inform the Company of any concern involving or affecting SBICPSL, as soon as the Employee/Supplier has knowledge of such concern. Employee/ Supplier shall also take such steps as the Company may reasonably request to assist the Company in the investigation of any concern involving SBICPSL:

I. Define your concern: What is the concern? When did it arise? What are the relevant facts?

II. ***Prompt reporting is crucial*** – A concern may be raised as follows:

- By discussing with a cognizant Manager; OR

- By contacting Company Compliance team, HR, Ombudsperson or senior management. The concerned SBICPSL resource will thereupon promptly have the concern addressed as per the process.

III. SBICPSL forbids retaliation against any person reporting a concern.

Anti-Corruption Guidelines

Overview

SBI Cards and Payment Services Limited (hereinafter referred to as "SBICPSL" or "the Company") has set out its commitment to ethical business practices. The Company will not give or promise any money or other thing of value, directly or indirectly to External Parties for the purpose of influencing/inducing any act or decision relating to any candidate, official, officer, employee or agent in his, her, or its official capacity in order to assist the Company in obtaining or retaining business for or with, or directing business to, any person, firm or corporation.

These guidelines (also referred to as Improper Payment Policy Guideline) are being put in place to strengthen Company's ethical practices & dealings and for prevention of corruption. The core aspects of the guidelines are as under:

1) Prohibition of bribery of any kind;
2) Maintenance of reasonable internal controls aimed at preventing and detecting bribery offences; and
3) Maintenance of accurate books and records that represent company's transactions fairly and in reasonable detail.

Compliance Program to strengthen the commitment

Bribery or corruption risk may occur because of internal or external parties. This Compliance Program shall provide specific instructions to facilitate consistency in identifying and managing bribery and corruption risk.

Employees – All employees must comply with the relevant requirements of law and regulation as well as the policies and procedures set out within SBICPSL. In addition, employees must receive regular training as appropriate to their role in order to familiarize themselves with the anti-corruption risks and be vigilant in recognizing risks and escalating red flags of potential corruption issues identified in the course of their business activity.

It is an employee's obligation to report any potential corruption or bribery risk to the reporting channels as defined above.

Employees are required to obtain pre-approval of High Risk Transactions from the following and/or their authorised representatives:

(i) Function Leader,
(ii) Financial Controller/Chief Financial Officer
(iii) Head -Legal
(iv) Chief Compliance Officer
(v) Managing Director & Chief Executive Officer

A. Training

- All SBICPSL employees shall receive training on SBICPSL Code of Conduct Guidelines, including guidelines on prevention of Improper Payments.
- Anti-corruption shall be a topic in the training plans to be delivered and shall be consistent with the compliance risk assessments.
- Personnel with responsibility for specific control functions designed to identify and assess exposure to anti-corruption risks and personnel in functions where exposure to such risks is identified through the compliance risk or Money Laundering risk assessments shall preferably be considered for Anti-Corruption training.
- The training plan shall consider local requirements and regulations as applicable to SBICPSL's business.

High Risk Transactions

i. Identification of High or Low Risk vendor based on certain predetermined questionnaire as defined in the Sourcing process
ii. For the purposes of Improper Payment Risk Management, an indicative list of High-Risk Transactions is annexed as Annexure A.
iii. High Risk Transactions as indicated in annexure A present a heightened risk of exposure to improper payments and therefore are subjected to enhanced Controllership oversight and monitoring.
iv. High Risk Transactions require a pre-approval from the (a) Functional Leader. (b) Finance Controller/ Chief Financial Officer (c) Legal Counsel (d) Chief Compliance Officer (e) Managing Director & Chief Executive Officer (MD & CEO)
v. Employees are required to obtain pre-approval of High Risk Transactions as in point (iii) and provide such approvals to the Finance Controller for appropriate booking in the chart of accounts.
vi. In exceptional circumstances the Managing Director & CEO may pre-approve a High Risk Transaction without following the approver hierarchy and such transactions shall not require additional approvals and will be booked by the Finance Controller in appropriate chart of accounts.
vii. The Finance Controller shall implement an auditable process for booking the transactions into appropriate chart of accounts.
viii. Copy of all High Risk Transactions shall be maintained in accordance to the Document Retention Policy of SBICPSL.
ix. Quarterly monitoring of High Risk Transactions may be conducted by the Controllership team to ensure all High Risk Transactions were pre-approved and booked to the appropriate chart of accounts.
x. Financial Controller will ensure that the details of transactions are sent outside SBICPSL only after the approval of the Managing Director & CEO.

Third Party Risks

A. Vendor Risk Management Program

- The Vendor Risk Management team shall be responsible for running a vendor risk management program which will clearly spell out the key risks in onboarding any third parties.
- Whenever an improper payment risk/High Risk payment is highlighted by any function to VRM team, the requesting function must provide information describing the proposed engagement and any information collected about the supplier's controls related to anti-corruption / improper payment prevention. VRM team will request for a Compliance assessment of the improper payment / corruption risk relative to the engagement.
- Appropriate confirmations/declarations will be taken from suppliers to perform verification/ due diligence for anti-corruption / Improper Payment prevention (as applicable and as required, to the proposed specific engagement).

- For suppliers that are not rated as satisfactory, the requesting function seeking the engagement with the supplier will be required to develop remedial action plan. In the event the remedial action plan cannot be implemented and/or formulated then in case of a new arrangement such engagement should not be carried on and in case of existing arrangement the engagement shall be terminated.

B. Continuing Obligations: Due Diligence and Red Flags

High Risk transactions/red flags must be closely monitored throughout the term of the relationship. If, at any time, any employee recognizes a red flag, the issue must be examined and resolved in consultation with Head-Legal.

Red flags such as the ones listed below are caution signals that should trigger further review. If there is a legitimate explanation for the circumstance, that finding should be documented. If, on the other hand, the investigation suggests the probability of a policy violation, appropriate steps (up to and including the immediate termination of the Agreement) should be swiftly taken, with the advice of Legal Counsel.

C. Indicative lists of Red Flags

- Unusual payment requests, such as up-front payments, abnormal commissions or price discounts, political or charitable contributions (excluding Corporate Social Responsibility contributions), payments to individuals, or midstream requests for additional compensation.
- Possible unethical practices, such as preparing false documents, press reports of improprieties, false answers to questions.
- Relations to External Parties, such as principals who are related to persons working in an agency or ministry of relevance, or employees who concurrently hold public office positions.
- Comments that infer Improper Payment will or has taken place.
- Apparent lack of commitment to Company policies.
- Termination of relationship by other clients.
- Unfavorable reference checks.
- Requests to keep the relationship secret.
- Payment terms unusually favorable or generous to the vendor
- Lack of concern about product quality, training or warranty.
- Lack of core competency.
- Request to split payments into small amounts.
- Request for additional compensation for a sales project
- Request to make payments in a different currency than that appropriate for the agreed address for such payments.
- Adverse information in public domain research.

Examples of red flag expenses

Expense Type	Explanation
Monetary Donation	Contribution checks, purchase table at a fundraiser, slots at charity golf event
In-Kind Contribution	Use of SBICPSL facilities or personnel at no charge. Gift of SBICPSL products to charity
Sponsored Event	Events organized by SBICPSL to which key strategic customers are invited.
Political Contribution	Account used for monetary and in-kind political contributions
Educational Grant	SBICPSL contributes to educational institution, does not include SBICPSL employee training
Travel Expense	Funding to or involving External Party for reasonable travel and travel related expenses (excluding meals) for a bona fide professional reason. Lodging / Transportation (airfare, taxi, train, car rental)
	Funding to or on behalf of a Customer for reasonable travel and travel related expenses (excluding meals) for a bona fide professional reason. Lodging / Transportation (airfare, taxi, train, car rental)
Meals/Events	Events - Organized event associated with a bona fide business purpose (SBICPSL presentation, training, customer meeting
	1. Gifts 2. Tickets to events not attended by SBICPSL representative, 3. Charitable contribution in the name of an External Party. 4. Does not include small value marketing promotional items with SBICPSL logo (costing upto Rs. 1,000 per item)
	5. Tickets to events not attended by SBICPSL representative, Charitable contribution in the name of External Party. 6. Does not include small value marketing promotional items with SBICPSL logo (costing upto Rs. 1,000 per item)
	7. Entertainment 8. Theatre tickets, sporting event tickets (with SBICPSL representative in attendance)

Note: Corporate Social Responsibility initiatives undertaken by the Company as per the prescribed guidelines under the Companies Act, 2013 will be excluded from the above indicative list.