www.slicebank.com
help@slicebank.com
+91-9148595496

slice small finance bank ltd

Code of Conduct

Date of Review:
Policy Owner: HR Committee
Approver: Board of Directors
Approved On:04-12-2025
Review Frequency: At least Annual Basis

slice small finance bank limited
CIN : U65100AS2016PLC017505

Registered Office: Unit no 2D2, Second floor, Fortune Central, Dr B.N Saikia Road, Near Old Regional Passport Office, Guwahati, Beltola, Kamrup, Assam, India, 781028

1. Purpose

An organization can be successful in the long term only if the Organization's employees adhere to the highest standards of business conduct. The Organization's commitment and vision requires adherence to high ethical standards and compliance with the law.

This Code of Conduct Policy ("The Code") governs the environment of the Organization. Adherence to the Code will help to create and maintain an environment of trust and loyalty in the Organization. Non-adherence of any of the codes on the part of any of the employees will be treated as committing misconduct and employees with such misconduct will be subject to the imposition of penalty or any other disciplinary action that the Management of the Organization deems fit which may result in punishment including termination of their services.

The information it contains is to be treated as confidential and shall not be made available to unauthorized persons. This Code will be reviewed and updated on an as needed basis.

2. Scope

The content of this Code applies to all employees, officers, directors, and representatives of the Organization. Employee shall mean all individuals on full-time or part-time employment with the Organization, with permanent, probationary, trainee, intern, retainer, temporary or contractual appointment.

All employees should read this Code carefully so as to have a clear understanding of the Organization's policies and should follow them accordingly. Upon acceptance of any employment with the Organization, all employees shall be deemed to have agreed to the terms of this Code. In case of any conflict between this Code and the appointment letter issued to an employee, the terms of this Code shall prevail.

3. Responsibility of Management

Under the Code, all levels of management are subject to the Code and have a special responsibility for implementing the Code and will be measured in their performance for:

- Ensuring that all existing and new employees under their supervision receive a copy of the Code and are offered training in a timely fashion as the management considers necessary, in its meaning and application. Primary responsibility for ensuring distribution of the copies of the Code will be that of the CHRO. This document should be made a part of the welcome kit for the employees and be given against his/her acknowledgement.
- Reviewing the knowledge and understanding of this policy by employees under their supervision and ensuring that "refresher" programs are provided as necessary.
- Stressing in word and deed the need for a continuing commitment to the Code.
- Demonstrating their own commitment by conducting themselves and managing their functions and the activities of all employees under their supervision in accordance with the Code.
- Promoting a workplace environment that encourages frank and open communication, free of the fear of reprisal, concerning the upholding of the Code.

4. Responsibility of Employees and Board Members

Under the Code, all Employees, Consultants on contract or Off-roll employees working for the Organization and all the Board Members are responsible for:

- Having knowledge and understanding of the Code
- Upholding the Code and policies, procedures and practices that support it as demonstrated by their daily business conduct.
- Contributing to a workplace environment that is conducive to the maintenance of the Code in their daily business activities.
- Seeking help from HR when the proper course of action is unclear or unknown and disseminate such clarifications.
- Remaining alert and sensitive to situations that could result in actions that are illegal, unethical, or in violation of the Code or the policies and procedures that support the Code, or are otherwise improper.
- Reminding others of their responsibilities when it appears they may be in danger of violating the Code or Organization's policies and procedures.
- Conducting oneself in a professional manner as part of the Organization.
- Reporting immediately all violations or potential violations of the Code to those who have responsibility for implementation of the Code.

The Organization expects and encourages its employees to initially direct their inquiries and reports to the immediate supervisor or to the HR email id hr@sliceit.com

5. Personal and Professional Integrity

Each employee and board member is expected to adhere to the highest standards of personal and professional integrity, to observe and comply with all laws and government regulations, and to avoid any illegal, unethical, or other situation that might reflect unfavourably on the employee/board member or upon the Organization. Employees and board members must perform their duties with honesty, integrity, and fairness. They are expected to avoid situations that may result in conflicts of interest or the perception of such conflicts. Incidents of theft, corporate credit card misuse, forgery and other fraudulent and/or dishonest activity will not be tolerated. Any such incident will be treated as violation of the Code.

6. Our Practice

The organization does the utmost to create a supportive work environment, where everyone has the opportunity to reach their fullest potential, and be free from harassment, intimidation, bias, and unlawful discrimination.

7. Equal Employment Opportunity and Anti-Discrimination Guidelines

The Organization is an equal opportunity employer, and is committed to diversity, inclusion, and equity at the workplace and embraces these as fundamental. All employment decisions in the Organization are based on the job requirements, individual qualifications, and the business needs without regard to caste, religion, ancestry,

gender (including pregnancy), marital/domestic partnership status, gender identity or expression/gender affirmation surgery, sexual orientation, age, nationality, cultural origin, disability, or any other category protected by applicable laws.

The Organization stands up against any discrimination and harassment, and has zero tolerance and is committed to a zero-occurrence approach to these. The Organization requests employees to report any discriminatory action against oneself or their colleagues to HR. Retaliation against employees who report discrimination to the Human Resources function or any member of management is not tolerated by the Organization.

The Organization does not engage in or encourage unlawful labor practices and does not discriminate based on the protected characteristics in hiring, job assignments, remuneration, rewards, benefits, access to training, promotion, transfer, discipline, termination, retirement, and any employment terms and conditions.

The Organization does not support engagement of children (below 16 years) for any work, whether on a temporary or permanent basis. Further any person above 16 years but below 18 years shall be given all the benefits prescribed under law regarding working hours, working days, payments, etc.

8. Grievance Redressal and Disciplinary Action

The Organization has established a structured process for addressing and resolving grievances raised by employees in a timely and effective manner, ensuring fairness, transparency, and respect for all parties involved. Breach of the code of conduct, a formal or informal disciplinary action is to be taken against the employee. This policy enlists the types of misconduct and describes the disciplinary action that must be taken to ensure fair and just treatment of the accused employee.

General Provisions related to Grievance:

1. Grievance arises out of an order of Management; the order shall be complied with by the due date and the employee can invoke the grievance procedure simultaneously.
2. Grievance is on an issue concerning/against any officer nominated/authorized to hear or given a decision of grievance, the matter shall be referred to the next higher level.
3. Officers dealing with the grievance shall maintain a record of all discussions and shall ensure that the proceedings are maintained confidential.
4. Officers dealing with the grievance should demonstrate an empathetic approach to the issue and handle the issue in a dignified manner.

All records shall be transferred to the Personal Folder after the final decision is communicated to the employee.

Exclusions from Grievance Redressal Procedure:

- A decision given at the conclusion of the disciplinary procedure of the Organization or decisions regarding redundancy of an employee given on account of commercial /business reasons are excluded from the purview of the grievance procedure.
- A sexual harassment /other harassment that falls within the purview of the Prevention of Sexual Harassment against Women should be taken up through the Internal Complaints Committee constituted as per Law in the first instance itself.

If the grievances are of such nature which indicates misconduct by any employee, then, such incident/s shall be handled in accordance with the provisions of Sub-Section – Misconduct with regard to Grievance and Redressal and Disciplinary Action.

The Grievance Redressal Committee, after hearing all concerned parties, submit its recommendations to the CHRO within 30 working days of referring the grievance to it. If a decision cannot be made within the prescribed period, the reason for the delay shall be noted. In any case a decision shall be given within 45 days of the receipt of the grievance.

Disciplinary guidelines set out details of actions to be taken against individuals for violation(s) of policies of the firm.

Non- compliance with applicable laws, regulations or professional standards present a legal threat and reputational risk to the Organization. Appropriate disciplinary action will be determined by a Disciplinary Committee after providing the individuals facing disciplinary action with an opportunity to explain any mitigating circumstances which may be considered when such violations are evaluated. The Disciplinary Policy can be found in the Grievance Redressal and Disciplinary Action Policy.

The Organization is committed to look into all matters reported and take action as appropriate in a time bound manner and the decision of the Organization shall be final and binding.

9. Gifts and Entertainment

a) Unacceptable Gifts & Entertainment

As per the Code of Conduct, employees are strictly forbidden to accept any bribe, improper or inappropriate favour of any kind. Besides cash payment, such inappropriate payments would include: -

- Kickbacks or kickback schemes, especially in cash forms.
- Unexplained rebates
- Payment for advertising or disguised allowances or expenses.
- Personal favors such as club memberships, entertainment and preferential treatments.

b) Acceptable Gifts & Entertainment

Some gifts are acceptable provided they are infrequent, not excessive in value, part of normal business and are not embarrassing to discuss. These acceptable gifts shall be divided into two categories viz. sponsored trips, and Festival related gifts.

I. Sponsored Trips

a. From time to time third party (vendors, partners, and financial institutions) hold seminars and conferences and invite Organization employees to participate in those events. They may also sponsor visits of Organization employees to large international conferences being held by international associations. Such invitations may include tickets, hotel accommodation, meals and other such hospitality.

b. All such invitations, including those received personally by employees, must be sent to Pre-Approving Authority (Annexure A) of their respective Business unit, who will decide on the appropriateness of accepting the invitation and assign the invitation to the person considered most suitable to attend the said function. No such invitations can be accepted, or trips undertaken without the requisite pre-approval.

II. Festival Related Gifts

a. Building and maintaining business relationships is an important aspect of doing business and small gestures during the festival season to acknowledge these relationships are an accepted norm. Infrequent gifts (e.g., during the festive seasons), which are merely tokens of relationship as they are not excessive in value (e.g., less than Rs. 5000/-) can therefore be constructed as a normal part of business. The receiving or giving of such gifts should therefore be limited to this amount. Anything above this amount, especially from more than one person of the same organization, stands to infringe on the 'obligation aspects' and therefore is best avoided.

b. At times, it becomes difficult to refuse the gifts or to judge its value. In such situations, where you may choose to accept the gift to appease the business associate but should not keep the gifts yourself. The gifts should be handed over to the HR department to be dealt with in a transparent manner for appropriate distribution (e.g., for charitable purposes).

c. For giving of gifts, the same limit of Rs. 5,000 /- applies. However, Managing Directors/ CEO, COO, CHRO can make an exception of a limit of Rs. 5,000/- for giving gifts as demanded by the situation.

Reporting of Acceptable Gifts & Entertainment

All sponsored trips and gifts along with their estimated value must be reported on quarterly basis, in writing, to the respective Zonal Heads, Department Heads and Head HR at Zones and Head Office respectively.

Pre-Approving Authority for Vendor Sponsored Trips

Departments	**Approving Authority**
Head of Department	Head of Human Resources/CPO

10. Privacy of Employee Information

A large volume of employee information is solicited and maintained by the Organization. Therefore, safeguarding the privacy interests of employees is a fundamental concern of the Organization.

If, as a part of job responsibilities one is entrusted with personally identifiable information regarding employees of the Organization, disclosure of this information to any person or entity within or outside the Organization is prohibited without the express authorization of the employee, except as provided under the proper policy and

procedures for the distribution and/or use of employee information within the Organization and to approved third parties/ as may be required by regulatory authorities and law.
Personally identifiable information may include information that not only concerns employment matters, but details about an employee such as living arrangements, physical and mental health and/or other highly personal matters. Whether or not this information is marked as being confidential, every precaution should be taken to protect the information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
Whether or not this information is marked as being confidential, every precaution should be taken to protect the information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

11. Privacy of Customer Information

Protecting our customers' privacy is fundamental to the Organization's business and there are laws regulating disclosure of customer records or other communications.
Employees may not participate in or permit another person to have unauthorized access to customer records or communications.
A large volume of customer information is distributed via electronic transmissions. Accordingly, it is the Organization's responsibility to protect the privacy and content of information conveyed in this manner.
Any use of customer information for any reason other than Organization's business is strictly prohibited.
Any allegation of misuse of client information will be investigated and, if substantiated, may be grounds for termination.
Any subpoena, court order or other request for customer information from law enforcement or government agencies or other outside parties is to be immediately referred to the supervisor. Supervisors should contact the applicable subsidiary legal function for assistance in every instance. However, certain information may be shared with credit bureau with the permission of the customer, as permissible under relevant regulation.

12. Customer Wrong-Doing

The Organization's customers are the greatest assets. However, the Organization becomes aware of a customer using our services for an unlawful purpose, such as to defraud the government or others, we have an obligation to investigate and report any such acts to the appropriate authorities.
If any employee suspects a customer of using the Organization services for an unlawful purpose, the employee is required to refer the same to the supervisor immediately.

13. Reporting of Fraud/ Theft/ Unethical Practices

Employees are required to report any information that they may have of the following including possibilities thereof to the Chief Vigilance Officer of the Organization immediately in confidence.

- Violation of laws of regulations
- Fraud or theft
- Conflict of interest/unethical practices

The recipient of the information shall not disclose the name of the informant to anyone else, if specifically requested. They are required to maintain such information confidentially until the investigation is completed. All such dealings will be guided by the Whistle Blower Policy of the Organization.
Concealment of such information, whether with ulterior motives or not, will be construed as misconduct.

14. Outside Activities – Employment, Consulting, and Volunteering

Employees are not permitted to be involved in activities (including other employment, self-employment, consulting services, or service on a board of directors or committee outside of the Organization) that compete with the Organization unless it has been approved in advance by the Competent Authority.
An employee should not engage in such activities with any other entity/Organization that provides services to the Organization or its competitors — where such services constitute more than one percent of the annual revenues of such Organization.
The Organization encourages its employees to be involved in voluntary activities except political activity that better our communities provided that the employee has informed the same with the immediate supervisor in advance.
Employees are expected to ensure that any involvement in outside activities should not come in the way of the quality or timely performance of their duties to the Organization.

15. Political Contributions and Activities

The Organization encourages all employees to personally participate in the political process by exercising his or her right of franchise.
The Organization will never require or expect its employees to express a political view that is contrary to their personal views.
Employees must inform the Organization and take approval of appropriate authority when considering either running for public office or accepting a public position. The purpose is to prevent a conflict, or the appearance of one, between private employment or benefits and the officeholder's performance of their duties.
In addition, numerous laws, regulations, and court decisions regulate relationships between public officeholders and private enterprise.
The Organization does not seek to limit the activities in which employees may participate on their own time, or the gifts or contributions employees may make with their own funds, but no payment, gift or contribution shall be made or authorized to be made with Organization's funds to any candidate for public office, campaign fund, political party or organization, except as may be authorized by the MD & CEO or any other competent authority approved by the Board of Directors of the Organization in this behalf.
The Organization does not endorse or enable any employee to engage in offering, receiving, or participating in any actions that could be construed as bribery in any form. It is imperative that all employees are fully aware of this policy and refrain from engaging in such activities.

No payment, gift or contribution shall be made either with Organization's funds or an employee's personal funds, to any government official or employee for the purpose of influencing conduct, actions or decisions in any matter.

16. Confidentiality

No employee shall during the continuance of his/her employment except in furtherance of the Organization's interests or thereafter on cessation of employment, without the prior written consent of the Organization, divulge, disclose, disseminate, publish or use any business or other information which may come to his/her knowledge in the course of his/her employment with the Organization or its associates / sister companies, including (but not limited to) any product or service, process, technique, method, result of investigations/surveys, price and cost calculation, computer system / code/ program, particulars of suppliers, customers, information pertaining to materials procurement, sales, information relating to tenders or any other information or documents relating to any area of operations, which the employee may acquire during the course of, or incidental to, his/her employment, concerning the Organization, its associates, affiliate or subsidiary companies or companies of its customers, suppliers or business associates.

a) Employee responsibilities extend beyond not revealing Confidential Organization material – but must also:
    - Properly secure, label, and (when appropriate) dispose of Confidential material.
    - Safeguard confidential information that Organization receives from others under non-disclosure agreements.
    - Take steps to protect and keep trade secrets and other confidential intellectual property of the Organization.
b) At times, a particular project or negotiation may require employee to disclose "Need to Know" or Confidential information to an outside party: Disclosure of that information should be on an "only as needed" basis and only under a non-disclosure agreement.
c) There are, of course, "grey areas" in which employees will need to apply best judgment in making sure that he /she doesn't disclose any confidential information. To provide an example, "Giving your friend tips that are available on public articles and blogs isn't likely the problem, but giving tips from the credit policies that are not publicly available information would be". If an employee is in a grey area, be cautious about the information provided, better yet, ask for guidance from the HR.
d) Employees shall exercise all due care and diligence to prevent the Organization's confidential information from unauthorized access, use, process, publication, or disclosure. Employees shall not disclose any Organization's confidential information to any person except to other employees of the Organization who are authorized to have access to such information for the execution of their duties. All notes, memoranda, records, writings and designs obtained by an employee during employment with the Organization shall be and remain the property of the Organization and shall be handed over by such employee to Organization any time on demand and in any event, upon the termination of employment.
e) Vendors/ Consultants - While working with vendors or consultant's employee must assure to conduct the appropriate due diligence and have the appropriate agreement in place before he/she discloses the information.

f) Employee must take special care in handling the following types of data that employee may collect from our clients, customers, vendors, etc.:
   - "Personal data" is the data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.
   - "Sensitive personal data" is such personal data, which may reveal, be related to, or constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation (x) any other similar data.

g) Any processing of personal data or sensitive personal data shall be with the due consent of the natural persons about whom the data is collected and shall be duly protected as per applicable law. However, if such data has been anonymized it shall be treated as non-personal data and while the normal confidentiality obligations shall continue to apply, there shall be no need to treat the data as personal.

h) If employee have access to any personal data or sensitive personal data of any persons, including employees, service providers, clients, customers, vendors, etc., employee are hereby undertaken to comply with all applicable laws, and only access the data on a need-to-know basis.

i) Employee shall not utilize any personal data or sensitive personal data which he/she has access to for his own motives, gain, personal relationships, or otherwise. Employee shall utilize such access for the limited purpose of carrying out your duties to the Organization and maintain such data strictly in a fiduciary capacity.

17. Protection and Usage of Organization/Organization Property

All Employees of the Organization are responsible for protecting and taking reasonable steps to prevent the theft or misuse of, or damage to assets, including all kinds of physical assets, movable, immovable and tangible property, corporate information, and intellectual property such as inventions, copyrights, patents, trademarks and technology and intellectual property used in carrying out their responsibilities. Employees must use and maintain resources efficiently and with due care and diligence.

18. Intellectual property

I. Organization's intellectual property rights (our trademarks, logos, copyrights, trade secrets, "know-how", and patents) are among our most valuable assets. Unauthorized use can lead to their loss or serious loss of value. Employees must respect all copyright and other intellectual property laws, including laws governing the fair use of copyrights, trademarks, and brands. Employees must never use Organization's (or its affiliated entities') logos, marks, or other protected information or property for any business or commercial venture without pre-clearance from the Marketing Team. Organization strongly encourages employees to report any suspected misuse of trademarks, logos, or other intellectual property to Legal.

II. Likewise, respect the intellectual property rights of others. Inappropriate use of others' intellectual property may expose the Organization and its employees to criminal and civil fines and penalties. It is advised to seek advice from Legal before soliciting, accepting, or using proprietary information from individuals outside the Organization or let them use or have access to Organization's proprietary information. Employees should also check with Legal if developing a product that uses content not belonging to the Organization.

III. All resulting intellectual property rights in any form of the work done by the employees during their course of employment or using Organization's resources, fully belong to the Organization. The employees agree that all services provided by them shall constitute 'work for hire' and expressly disclaim any interest in all intellectual property rights and will not, during or at any time after the termination of their employment challenge such right of the Organization. Organization will have the unencumbered right to make alternations to any intellectual property and to transfer intellectual property rights to affiliate companies or third parties.

19. Organization's Equipment (Device & Network)

Organization gives its tools and equipment to its employees to do jobs effectively but counts on its employees to be responsible and not wasteful with the resources they are given. Communication facilities (which include both Organization's network and the hardware that uses it, like computers and mobile devices) are a critical aspect of Organization's property, both physical and intellectual. Be sure to follow all security policies. If employees have any reason to believe that the Organization's network security has been violated – for example, Employee loses his/her laptop or smartphone or thinks that the network password may have been compromised – please promptly report the incident to IT team.

Employees are prohibited from using personal laptops, mobile phones, tablets, or any other personal electronic devices for work-related activities unless explicitly authorized by management. All work-related tasks must be conducted using company-provided devices to ensure compliance with security protocols

Employee Data

I. Organization's HR collect and store personal information from employees. Organization may use your personal information:
   - for the purposes of record keeping
   - for any additional purposes that Organization advises you of and where employees consent is required by law that have obtained the consent in respect of the use or disclosure of personal information.

II. Organization may use your personal information without your knowledge or consent were permitted or required by applicable law or regulatory requirements to do so.

III. Organization may share your business contact information with its clients, vendors, consultants, other employees and such other persons as may be required in the day-to-day operations and in accordance with your role at the Organization. Employees hereby expressly consent to such sharing of information as required to discharge their duties to the Organization.

IV. Organization may share your personal information with its employees, contractors, consultants, service providers, clients and other parties (including other members of the organization) who require such information to assist with establishing, managing or terminating employment relationship with employees, including: parties that provide products or services to the Organization or on its behalf and parties that collaborate with the Organization in the provision of products or services to its employees. In some instances, such parties may also provide certain information technology and data processing services to the Organization so that Organization may operate its business.

V. Further, your personal information may be disclosed:

- as permitted or required by applicable law or regulatory requirements. In such a case, we will endeavor to not disclose more personal information than is required under the circumstances.
- to comply with valid legal processes such as search warrants, subpoenas or court orders.
- as part of Organization's regular reporting activities to other members of the Organization.
- to protect the rights and property of the organization.
- during emergency situations or where necessary to protect the safety of a person or group of persons.
- where the personal information is publicly available; or
- with your consent where such consent is required by law.

20. Smoking

The Organization and its premises are declared as "Non-Smoking Areas". Smoking in any part of the Organization is not permissible.

21. Intoxication

Employees are prohibited to come to work in a state of intoxication under the influence of alcohol or drugs or any other narcotic / prohibited substance or be in possession thereof at work. They are also prohibited to consume alcohol or drugs during the duty hours or during their presence in the Organization's premises.

22. Damage or attempt to cause damage to property

No employee shall deliberately or inadvertently cause any type of damage to a property belonging to a colleague, the Organisation, the customer, or vendor.

23. Personal Transactions in Securities

No employee shall deal in any securities (including shares of the Organization) except for his personal investment based on any information, which he/ she acquires in the course of his/her employment with the Organization nor shall he/ she counsel any other person if not warranted by the nature of his/ her duties assigned to him/her, to deal in securities of such a Organization on the basis of such unpublished price sensitive information.

"Dealing in Securities," means the act of buying, selling, or agreeing to buy, sell or deal in any securities either as principal or agent.
An employee with unpublished price-sensitive information about companies with whom the Organization has business dealings (e.g., MSME etc.) should exercise due diligence to maintain it in confidence and must not trade in the securities of the Organization before such information is announced to the public.
The Compliance Function will publish the name of insiders with sensitive information about the Organization who would need to obtain prior approval from Head - Compliance to deal with the shares of the Organization.
No employees should deal with the shares of the Organization during the published shut down period.

24. Negligence / Cash Shortage

Employees causing financial or other loss to the Organization on account of negligence will be required to reimburse/make up the loss as directed by the Management.
Cash shortages from employees will be recovered in full of the concerned employee and disciplinary action will be taken up.
Notwithstanding the above, the negligence / misappropriation / not following procedures will be examined and for each case appropriate action will be taken that may result even in dismissal of the employee concerned.

25. Harassment

The Organization is committed to provide a work environment that is free of discrimination and harassment.
Harassment of any nature is prohibited, and any employee proved to be harassing any other employee will be subject to serious disciplinary action including but not limited to termination. The Management may report the matter to the Police as per the relevant laws of the country.
If an employee believes he/ she has been a victim of harassment, or know of another employee who has been, he/ she shall report it immediately to the Head HR. Employees can raise concerns and make reports without fear of reprisal or victimization.
Any employee who becomes aware of harassment should promptly advise the Head HR and is required to handle the matter in a timely and confidential manner.
The employee being aware of the harassment, or the Head of Function / Manager and other officials involved in the investigation should handle the matter with great sensitivity without disclosing the identity of the victim.
Harassment in the workplace can take many forms. It can be obvious or subtle, direct or indirect (e.g., where a hostile feeling/environment is created without any direct attacks being made on a person).
Common forms of workplace harassment and discrimination include but are not limited to:

- Usage of abusive language
- Bullying
- Exclusion
- Incorrect dressing and deportment
- Shouting, talking loudly in an offensive manner
- Targeting

- Lack of courtesy
- Improper conduct with client
- Breach of professional code of conduct

Personal harassment means any objectionable or offensive behavior that is known or ought reasonably to be known to be unwelcome. It includes objectionable conduct, comment or display made on either a one-time or continuous basis that demeans, belittles, or causes personal humiliation or embarrassment. Without limiting, personal harassment includes harassment on the grounds of discrimination based on race, color, religion, ancestry, place of origin, age, physical disability, mental disability, marital status etc.

Misuse of Authority: Harassment also includes misuse of authority where an individual improperly uses the power and authority inherent in a position to endanger a person's job, undermine the performance of that job, threaten the person's economic livelihood, or in any way interfere with or influence a person's career. It is the exercise of authority in a manner which serves no legitimate work purpose and ought reasonably to be known to be power intimidation, threats, bullying, blackmail or coercion.

Sexual harassment, whether carried out by superiors, peers, subordinates, employees of contractors/ agencies, or individuals of the same gender, is unwelcome and unacceptable behavior that undermines the dignity of individuals at work. It can manifest as a single incident or a pattern of behavior that interferes with an individual's performance or creates a hostile, intimidating, or offensive work environment. All instances of sexual harassment will be taken seriously and addressed in accordance with the provisions of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

Guidelines on Prevention of Sexual Harassment:

The Organization and its management must ensure that the due process is followed to deal with the POSH cases as per the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

The following must be ensured by the Organization:

- **Internal Committee (IC):**
  - Establish an Internal Committee (IC) as mandated by the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013.
  - The IC should consist of at least one external member, preferably a legal expert, and representatives from various departments.
  - Ensure that IC members receive appropriate training on handling POSH cases.
- **Awareness and Training:**
  - Conduct regular awareness sessions for employees to educate them about POSH policies, their rights, and the complaint process.
  - Train managers and supervisors on recognizing and addressing harassment issues.
- **Complaint Mechanism:**
  - Establish a confidential and accessible complaint mechanism for reporting incidents of sexual harassment.
  - Provide multiple channels (email, phone, in-person) for reporting complaints.

- Ensure that complainants are not victimized or retaliated against for coming forward.

➢ **Investigation Process:**
- Investigate complaints promptly and impartially.
- Maintain confidentiality throughout the investigation.
- Interview the complainant, alleged harasser, and any relevant witnesses.
- Document findings and recommendations.

➢ **Disciplinary Action:**
- If the complaint is substantiated, take appropriate disciplinary action against the harasser.
- Disciplinary actions may include warnings, suspension, termination, or legal action.
- Ensure consistency in applying consequences.

➢ **Support for Complainants:**
- Provide emotional support to complainants during the process.
- Offer counselling services if needed.
- Keep complainants informed about the progress of the investigation.

➢ **Preventive Measures:**
- Conduct regular workshops and training sessions on respectful behavior, boundaries, and maintaining a safe workplace.
- Encourage a culture of respect and zero tolerance for harassment.
- Monitor and address any recurring issues.

The management will ensure that the changes in Internal Committee (IC) to be updated to all employees from time to time to ensure that all employees are aware of the Committee existence and the respective contact persons for any such incidents.

26. Computer / Email Usage

Official e-mail system is to be used solely for bona fide official purpose.
All information and messages that are created, sent, received, or stored on the Organization's e-mail system is the sole property of the Organization.
E-mail is subject to monitoring by the Organization without prior notice to the originators or recipients of such e-mail. E-mail may be monitored and read by authorized personnel of the Organization for any violations of law, breaches of Organization policies or for any other reason.
Employees should ensure that e-mails do not contain statements or content that are defamatory, offensive, illegal, derogatory, or discriminatory or that could be termed as harassment.
Inappropriate or offensive messages including but not limited to racial, sexual, or religious slurs or jokes are prohibited.
Sexually explicit/suggestive messages or images, cartoons or jokes are prohibited.

No software, executable files, databases or other "live" technology may be received through Email, downloaded from the Internet, installed from external discs, or otherwise placed on the Organization's computer system without the prior approval of the Chief Technology Officer or designated I.T. personnel.
The Organization shall have the right to monitor and inspect the computer systems (hard drives and external drives), history files, log files and all other aspects of the Organization computers and software for any reason at its discretion.

27. Telephone / Internet Usage

Employees are responsible for using their mobile phones and -Internet in a manner that is ethical and lawful during business hours. The Organization reserves the right to access and monitor all telephone calls and internet messages on its systems.
Employees are prohibited from using the internet for any of the following activities:

- Engaging in illegal, fraudulent, games or malicious conduct
- Working on behalf of organizations without any professional or business affiliation with the Organization
- Sending, receiving or downloading / storing offensive, obscene, or inflammatory materials
- Obtaining unauthorized access to any computer system
- Using another individual's account or identity without explicit written authorization
- Visiting sites, which are, inappropriate in a public or business environment.

28. Social Media Guidelines

Publication of articles in electronic Media

All communications and disclosures related to the Organization and its operations, intended for public audiences such as the media, the financial community, employees, shareholders, and agents, must be handled exclusively by specifically authorized employees. Before an employee publishes an article, opinion, or any content in newspapers, magazines, blogs, webinars, award nominations/applications, etc., that mentions the Organization, its customers, or any related matters, it must be reviewed by senior management representatives from the Corporate Communications, Audit, and Compliance teams, or other designated officials.

Social Media and Public Commentary

Employees are expected to exercise prudence when using social media platforms. They should avoid expressing opinions on sensitive societal or political issues that could harm the Organization's reputation or create conflicts. The policy explicitly state that any comments made by employees in their personal capacity do not represent the Organization's official stance.
It is also to advise that employees should direct grievances related to the Organization to the HR department or the relevant internal channels. Publicly airing grievances related to the Organization is discouraged.

29. Whistle Blower Policy

The bank encourages every employee to express concerns openly or to report on any suspected violations of this Code or any policies of the bank or any other activity that may be unethical or illegal to their department Manager and HR

30. Health, Safety, and Environment Responsibility

The organization is committed to conducting its operations in a manner that upholds the highest standards of health, safety, and environmental responsibility. We comply with all applicable laws and regulations, maintain safe and sustainable workplaces, and integrate HSE principles into our business practices. All employees are expected to follow safety protocols, maintain a clean and hazard-free work environment, participate in safety drills, and promptly report any unsafe or unlawful activity.

We encourage responsible environmental behavior by minimizing waste, conserving energy and natural resources, and supporting initiatives that reduce our carbon footprint. The organization also ensures appropriate fire and safety measures are in place across all premises and prohibits employment of individuals below 18 years of age. The organization recognizes the importance of mental health and wellbeing. Employees are encouraged to use available resources such as counselling services, sabbaticals or HR support when needed

31. Remote Work & Hybrid Work Guidelines

Employees working remotely or in hybrid models are expected to maintain the same standards of professionalism as when working on-site.

- Confidentiality & Security: Work must only be conducted using Organization-issued devices, secure networks, and approved applications.
- Workspace Conduct: Employees must ensure a distraction-free environment and comply with work hours and availability requirements.
- Virtual Meetings: Professional conduct, respectful participation, appropriate attire, and confidentiality must be maintained during online meetings.

32. Technology, Cybersecurity & Responsible use of AI

Employees must follow all cybersecurity protocols including strong passwords, multi-factor authentication, and vigilance against phishing attempts.

Use of AI or generative tools must be ethical, transparent, and must not compromise data confidentiality. Sensitive customer, employee, or organizational data must never be entered into public AI tools.

Any suspected cyber threats, data breaches, or loss of devices must be reported immediately to the IT Security team.

33. Financial Integrity, Anti-Bribery & Anti-Money Laundering

The Organization upholds strict compliance with all anti-money laundering (AML), anti-bribery, and corruption laws.

Employees must not engage in or facilitate money laundering, fraudulent transactions, or activities designed to disguise the origin of illicit funds.

Any suspicious transaction must be reported immediately to the Compliance and Vigilance teams.

34. Regulatory & Legal Compliances

The Organization upholds strict compliance with all anti-money laundering (AML), anti-bribery, and corruption laws.

Employees must not engage in or facilitate money laundering, fraudulent transactions, or activities designed to disguise the origin of illicit funds.

Any suspicious transaction must be reported immediately to the Compliance and Vigilance teams.

35. Indemnity

The employee shall, at their own expense, indemnify, defend, and hold harmless, its directors, management, and other associated parties from any and all losses, liabilities, obligations, damages, third-party claims, demands, causes of action, costs, and expenses of any kind, arising from or related to a breach of any representations, warranties, or covenants made by the employee as outlined in their appointment letter, this code of business conduct, or any other policies of the Organization.

36. Conclusion

It is not feasible to anticipate and outline every ethical situation that may arise. Therefore, we rely on the sound judgment of all employees to maintain a high standard of integrity for both ourselves and the organization. At times, determining the appropriate course of action may be challenging. If there is any uncertainty, employees are encouraged to seek guidance from their manager, the Human Resources department, or the Legal team