Code of Conduct

2025

Ethics .. Integrity .. Commitent

Our Principles at Work

بنك مصر

BANQUE MISR

Table of Contents

Our Values

AGILITY Delivering work with speed and simplicity, ensuring quick responses to changes and challenges. It enables the organization to become more dynamic through adopting opportunities and change direction swiftly towards its goals.

STEWARDSHIP Committing to adding sustainable value to the work place in everything we do. Providing directions and business insights, utilizing and managing resources effectively, while ensuring clients satisfaction at all levels.

CUSTOMER CENTRICITY Everything we do, revolves around bringing customers to the front. We focus our business services to provide adequate quality and enhance the customer experience. We respond effectively to customers needs and build mutual profitable relations.

INNOVATION Having the ability to think differently, develop impactful solutions and continuously adopt creative thinking. Seeking continuous improvement at all fronts, upgrading business outcome across all functions of the organization.

PRIDE Building on our great legacy with an utmost sense of belonging and loyalty to create a constructive work environment that enables us to sustainably perform our job with integrity, dedication and excellence.

Work Behaviors

We Commit to Our Code

We are committed to the highest standards of ethics and professional conduct in all our dealings within Banque Misr, including local and international branches and affiliated entities. As bank employees, we adopt these standards to foster a culture of excellence among staff, ensuring that we live our values both individually and collectively as one team.

The Banking Code of Conduct defines the ethical and behavioral principles that all employees and key officials must follow. This code is prepared in accordance with applicable laws and policies and is formally approved by the bank's Board of Directors.

Employees and key officials are provided with copies of the code through approved channels, whether electronic or printed, and are required to familiarize themselves with its contents and compliance requirements. Introductory sessions are organized to ensure understanding of the charter's key points, and employees and key officials sign a document pledging full adherence to its rules. The bank maintains signed records confirming that employees have read, understood, and committed to the charter.

The bank offers training programs designed to ensure proper understanding and application of the charter's principles across all departments and activities. These include mandatory periodic sessions that promote a culture of compliance and practical scenarios illustrating how to address ethical and compliance challenges. Regular follow-ups are conducted to verify adherence to the charter, identify any deviations, and review policies and procedures for alignment. Mechanisms for reporting violations are established, ensuring whistleblower protection.

Making Sound Decisions

We strive to make sound, well-informed decisions and to do the right thing. However, decision-making is not always straightforward. While some decisions are clear and easy to make, others may be more complex. Regardless of the situation, consider the following guidelines to help you make well-informed decisions:

- Gather all relevant facts and review applicable laws and policies across Banque Misr Group.
- Consider relevant laws, regulations, and internal policies.
- Identify potential alternatives and assess their consequences.
- Ensure your choice aligns with the bank's values.

We Act with Integrity

At Banque Misr, integrity is a core value guiding all our actions. Integrity without knowledge is weak and worthless, while knowledge without integrity is dangerous and harmful.

Our shared responsibility to protect the bank's reputation, built on integrity, is reflected in the following commitments:

1. **Upholding Professional and Ethical Conduct**
    - Avoid engaging in fraudulent, unethical, or unlawful practices. All related data and information must be documented and handled with strict confidentiality to ensure the highest levels of integrity and transparency.
    - Comply with all laws, regulatory requirements, policies, and internal procedures.
    - Maintain confidentiality of accounts and data; do not disclose any confidential or insider information that is not publicly available.
    - Always provide accurate and truthful information to customers, the bank, and the Central Bank.
2. **Promoting Transparency and Addressing Conflicts of Interest**
    - Immediately disclose any suspected conflict of interest, such as shareholdings in related-party companies.
    - Refrain from manipulating or falsifying documents in any form.
    - Use the bank's assets responsibly and professionally to safeguard institutional resources.
    - Report any suspicions of fraudulent practices or violations that conflict with the bank's values and policies, in accordance with approved procedures.

Reporting Concerns: If you suspect that your behavior or that of another employee conflicts with these values and principles, you must immediately report your concerns to the Banking Compliance Officer.

Commitment to Accountability: We must all act responsibly to ensure compliance with these rules and avoid any actions that could harm the bank's reputation.

Combating Fraud

As part of our commitment to fostering a culture of integrity and transparency, Banque Misr's Board of Directors, senior executive management, key officials, and all employees place the highest importance on combating all forms of fraud. Fraud is fundamentally incompatible with the core values that underpin responsible banking operations at Banque Misr. We affirm our absolute commitment to all applicable laws, rules, and regulations, including those related to fraud.

Fraud is defined as any act involving deception, misrepresentation, or abuse of trust or authority for personal gain at the expense of professional integrity or the interests of the bank or its stakeholders. Examples include:

- Manipulating information or documents
- Exploiting authority to achieve unlawful gains
- Concealing facts with the intent to mislead or cause harm
- Misappropriating funds or assets through unlawful means

The impact of fraud extends beyond financial harm; it undermines trust among employees, damages customer relationships, and harms the bank's reputation in society.

The Code of Conduct promotes individual responsibility in rejecting fraud in all its forms and urges employees to serve as role models of integrity and transparency. Employees must refrain from any behavior that violates professional honor, including participating in, overlooking, or facilitating fraudulent acts—whether directly or indirectly. The Code strictly prohibits any act intended to manipulate, mislead, or fraudulently influence others through concealment, misuse of information, misrepresentation of facts, or unfair practices.

Collusion, negligence, or failure to report suspected fraud constitutes a serious violation that may result in disciplinary or legal action. All employees are required to report any suspected fraud immediately through designated official channels.

Investigations into suspected or actual fraud are conducted by specialized departments with appropriate authority and expertise, ensuring avoidance of conflicts of interest.

Responsibilities of Managers

Managers serve as role models for ethical behavior. They must set positive examples that inspire and motivate others to conduct business according to the highest standards of ethics and professionalism. Managers are responsible for promoting a culture of compliance and integrity, fostering a positive work environment, and ensuring treatment with dignity and respect.

Managers must report all discovered fraud cases promptly, document them accurately and in detail, and handle such cases with complete confidentiality in coordination with the Compliance Department to ensure full adherence to policies.

As a Manager, How Can I Promote Ethical Behavior?

Include discussions about workplace ethics in team meetings.

Create an environment where team members feel comfortable asking questions and raising concerns.

Ethical Issues

Responsibility to Report Ethical Issues

What should you do if you suspect—without certainty—that someone has violated our Code of Conduct? Although remaining silent may seem easier when you witness potential misconduct or unethical behavior, the right and proper action is to report any concerns or doubts about your own behavior or that of others. Failure to report a violation in good faith and in a timely manner can damage our reputation and expose colleagues, customers, and Banque Misr to significant risk.

Reporting Ethical Issues

Our employees are the first line of defense in safeguarding the integrity and honesty of operations at all times. They bear full responsibility for maintaining our reputation.
Banque Misr operates a comprehensive compliance disclosure channel—via email or personal interviews—that enables employees to report concerns when normal reporting channels are unavailable or inappropriate. This disclosure channel serves as an outlet for employees to raise concerns regarding:

- Violations of laws and regulations
- Allegations of bribery or corruption
- Non-compliance with policies
- Suspicions of money laundering
- Internal control violations
- Fraud or deliberate errors in financial records

Work Environment

A Workplace Characterized by Respect

The bank provides a work environment free from pressure, violence, or discrimination based on gender, age, religion, or any other factor. We strive to ensure satisfaction and respect for the dignity of every employee, fostering mutual trust among colleagues and between employees and their managers.

Appreciating Colleagues

At Banque Misr Group, we value every colleague and take pride in our intellectual and cultural diversity, which enriches our work environment. We respect differences and promote an inclusive atmosphere across all local and international branches and affiliated entities.
A "colleague" is defined as any employee who is part of the workforce and is expected to demonstrate team spirit and mutual respect in all interactions inside and outside the workplace.
Everyone must recognize and uphold the values and principles that govern professional behavior, committing to transparency and integrity while refraining from unethical practices.

Professional Dealings with Managers

Employees must respect their managers and perform assigned tasks in a manner that serves the public interest. A "manager" is defined as an individual responsible for directing and developing their team. Employees are required to follow instructions and guidelines outlined in employment contracts and development plans efficiently and promptly, provided these tasks do not violate laws, internal regulations, or public morals.

Managers, in turn, must treat subordinates impartially, avoiding discrimination except on the basis of competence, and refrain from assigning personal or unlawful tasks. They must follow systematic procedures for submitting complaints and report any conflicts of interest that may affect the work environment. This includes adhering to approved methods for handling complaints transparently, protecting Banque Misr's reputation, and promoting a culture of trust and mutual respect.

Diversity

Banque Misr is committed to respecting the diverse values and opinions of its employees as part of its dedication to serving an inclusive community. All employees are encouraged to express their views freely, and no bias or discrimination based on gender, age, race, religion, or disability is tolerated.
Banque Misr has always embraced the principle of equal opportunity, recognizing diversity as a core value, strategic advantage, and driving force behind its culture. Employees must uphold principles that promote respect for the dignity of colleagues and customers, refraining from any practices that conflict with the bank's values, including equality and non-discrimination.

Dress Code and General Appearance

In line with the bank's commitment to providing a respectful and equitable work environment, employees are expected to comply with professional standards regarding appearance, reflecting the distinguished image of Banque Misr Group across all local and international branches and affiliated entities.

- **Commitment to Appropriate Dress:** All employees must adhere to the bank's Dress Code, which promotes professionalism and appropriate appearance.
- **Displaying Identification:** Employees are required to wear their personal identification badge during working hours to facilitate communication and identification.
- **Face Covering and Visual Communication:** Covering the face during work is prohibited to ensure effective visual communication with customers, thereby enhancing trust and professionalism.

Recommendations Regarding the Use of Masks or Face Coverings:

Masks are permitted, when necessary (e.g., health conditions or precautionary measures), provided they do not impede effective visual communication with customers. Wearing a niqab or any face covering that obstructs service delivery is prohibited, in accordance with the bank's authorized dress and appearance guidelines.

Abuse, Harassment, and Racial Discrimination

Banque Misr is committed to maintaining a work environment characterized by equality and non-discrimination. All forms of abuse—including verbal, psychological, physical behavior, threats, and unethical or illegal practices—are strictly prohibited.

Personal Data of Employees and Privacy Protection

To manage salaries, healthcare, and other routine benefits, Banque Misr uses employees' private and sensitive personal data strictly for work-related purposes. Employees must respect data privacy by accessing and using such information only for legitimate work purposes, with proper authorization and on a need-to-know basis.

Employees must not disclose or discuss this information with anyone lacking authorization. Recording or photographing employees' conversations without consent, or photographing workplaces, is prohibited. Circulation of such materials is also forbidden to maintain a safe and respectful work environment for all.

Employee Complaints

Banque Misr provides a secure and confidential mechanism for submitting work-related complaints and suggestions through the bank's internal network, particularly when issues cannot be resolved through direct managers or relevant departments.

Maintaining Professional Skills and Working Efficiently and Accurately

To foster innovation and professional excellence, every employee must maintain and develop their professional skills, including updating technical and administrative knowledge and understanding applicable policies. Employees should strive to reach their full potential and perform tasks efficiently, accurately, and diligently, adhering to work schedules to serve customers' interests and strengthen trust in Banque Misr.

Employees must also comply fully with mandatory training requirements set by regulatory bodies. Attendance at required training sessions is obligatory, and employees must not delegate their training to others. Failure to comply constitutes a violation subject to disciplinary action under applicable policies, ensuring fairness, transparency, and high standards of performance.

Workplace Safety

Banque Misr prioritizes a healthy and safe work environment in compliance with approved standards and laws by:

- Implementing and regularly inspecting industrial security systems, surveillance equipment, fire safety systems, and first aid facilities.
- Providing fire safety, evacuation, and first aid training to ensure employees understand safety requirements.
- Enforcing a complete ban on smoking in all workplaces and common areas.
- Prohibiting the consumption, possession, or influence of alcohol or narcotics, as such acts are crimes under law and internal regulations.

Employees must report unsafe working conditions to their manager or the designated officer responsible for reporting unlawful practices.

Protecting the Bank's Assets

Employees are responsible for safeguarding the bank's tangible and intangible assets, as well as customer data and assets under their control. This includes full compliance with information security controls and preventing any unauthorized disclosure, access, or misuse of data. Any negligence or failure to protect information constitutes a breach of duty.

Any falsification, forgery, preparation of misleading financial reports, or unlawful use of the bank's assets is considered fraud—even in the absence of personal gain—and represents a direct violation of your obligations to the bank.

Maintaining Confidentiality of Data and Information

Employees must not discuss work-related matters—especially confidential ones—in public places such as elevators, corridors, restaurants, public transportation, or on the Internet, including blogs and social media platforms.

All customer accounts, deposits, trusts, safes, and related transactions are strictly confidential. Access or disclosure of such information is prohibited except with written authorization from the customer, their heirs or beneficiaries, or pursuant to a judicial or arbitration ruling. This obligation remains in effect even after the customer's relationship with the bank ends.

Maintaining Financial Integrity

Creating and Managing Records:

- Employees must ensure that all data, information, accounts, and financial records are accurate and maintain the highest level of integrity. This responsibility applies to all employees, not just financial management personnel.
- Senior management must be notified if any employee is pressured to prepare or destroy documents in violation of bank policy, or if

incomplete, misleading, or incorrect documents are submitted to external parties.

- Employees responsible for providing supporting documents or approving banking transactions must verify the accuracy of all related data. All documents must be properly recorded and retained.
- Financial statements and reports must comply with generally accepted accounting standards and applicable regulations, providing a fair and complete representation of the bank's operations and financial position.
- Documents must be retained for legally specified periods and in accordance with the bank's policies.
- Destroying any records related to legal violations, litigation, or ongoing investigations is strictly prohibited.
- Before altering or destroying any document, employees must consult their direct supervisor to avoid accusations of concealing information or obstructing audits and justice.

Expense Management

Employees at all levels are responsible for managing and reviewing expenses to ensure compliance with bank policies and that they accurately reflect legitimate business costs. Expenses must be approved by the appropriate authority. Any false or fraudulent expense claims will result in disciplinary action under applicable regulations.

Communications, Equipment, Systems, and Services

The bank provides equipment and services—including computers, telephones, laptops, fax machines, intranet, internet access, email, and other electronic communication tools—for work purposes only, whether on-site or remotely.

Speaking on Behalf of the Bank

Dealing with Media and Public Appearances

The Corporate Communications Department is the sole entity authorized to make press or public statements on behalf of the bank. If contacted by a media representative, employees must refer them to the Corporate Communications Department.

Only individuals designated by the Corporate Communications Department may respond to media inquiries or provide official publications, regardless of the topic.

Using the Bank's Name, Facilities, and Logo

Employees must not use the bank's name, logo, trademark, or facilities for commercial purposes unrelated to their job or outside the scope of work, including on websites.

Using Social Media

The bank acknowledges that employees use social media platforms such as blogs, Twitter, Facebook, and LinkedIn for personal purposes. Employees must exercise caution and accuracy when referencing their job title or grade, if required.

Employees must not:

- Create or participate in groups that share information, data, or documents related to the bank, other banks, or customers on any social media platform—whether public, private, or personal.
- Post personal comments, inquiries, complaints, opinions, or responses related to the bank or its operations.
- Create accounts using the name or trademark of Banque Misr or other banks, or publish any content that could harm the reputation of the bank, its employees, or the banking sector.
- Engage in discussions on controversial topics—political, religious, sports-related, or otherwise—in a manner that is fanatical or abusive.
- Publish or circulate internal documents or sensitive information, such as internal circulars, decisions, policies, or confidential data, through external channels.

Personal use of social media must occur outside working hours. Using the bank's communication systems or services for personal social media activity is prohibited.

If You See Negative Content About the Bank Online, Do not respond directly. Instead, report the content to your manager or the bank's compliance officer so that the authorized spokesperson can address it.

Conflict of Interest

Many conflicts of interest can be resolved if disclosed promptly. If you believe that you or the bank may face an actual or potential conflict of interest, you must immediately inform your manager or the bank's Compliance Officer.

Always disclose potential conflicts before taking any action to avoid worsening the situation. Review the Conflict of Interest Policy approved by the Board of Directors and comply fully with its provisions.

What is a Conflict of Interest?

A personal conflict of interest occurs when an employee's private interests—such as external professional relationships or personal financial holdings—interfere with the bank's interests or the performance of official duties.

All employees must prioritize the public interest and the interests of customers over personal interests. Any type of conflict between personal and bank interests must be avoided.

The following sections describe common areas that may lead to actual or perceived conflicts of interest. Since it is impossible to list every potential scenario, Banque Misr relies on employees to exercise sound judgment, seek advice when necessary, and disclose activities appropriately.

Accepting Gifts

Employees must exercise caution when exchanging business courtesies with current or potential customers or suppliers to avoid conflicts of interest. Gifts and entertainment must never be perceived as bribes intended to influence business decisions. Any belief that a decision was made because of a gift or courtesy can damage the bank's reputation. Employees and their immediate family members must not accept gifts, services, loans, or preferential treatment from any person—whether customers or suppliers—in exchange for any past, current, or future business relationship with Banque Misr.

Permissible Exceptions:

- Invitations to events or business meals may be accepted with prior coordination and approval from the relevant manager.
- Symbolic, non-cash gifts of modest value may be accepted when refusal would cause embarrassment, provided there is no negative impact.

Gift Value Limits:

- For employees in Egypt: The maximum limit for symbolic gifts is EGP 2,500.
- For employees in international branches: The maximum limit is USD 50 (or equivalent in local currency).
  All gifts must be disclosed to the direct manager, who maintains a record of such disclosures.

If gifts exceed these limits or are received under special circumstances (e.g., cultural protocol or public events), a detailed report must be submitted to the direct manager and the Institutional Governance Department in the Compliance Sector for approval and further action.

Courtesy gifts exchanged between banking institutions or offered to senior officials in their official capacity may exceed these limits but must be disclosed and recorded in the designated register.

Prohibited Gifts:

Accepting cash, cash equivalents, gold, or valuable items from external parties—including customers, suppliers, or government entities—is strictly prohibited.

Procurement, Inspection Employees, or Members of Decision Committees:

Employees involved in procurement or decision-making committees must exercise special care to avoid allegations of unfair practices. Employees engaged in purchasing goods, assets, or services must not accept gifts or hospitality under any circumstances from current or potential suppliers.

Incidental Benefits from Purchases

Commercial organizations may offer free gifts for using their services or purchasing their products. These benefits belong to the bank, not the individual employee. Employees must notify the bank in writing about such benefits and must not personally benefit from them.

Free Offers for Official Travel

If airlines, shipping companies, or travel agencies offer free benefits due to frequent official travel, these offers must be directed to the relevant department at the bank. Employees must not accept such offers personally.

Discounts Offered to Bank Employees:

Discounts offered by clients must be arranged directly between the client and the bank, with the knowledge of the relevant department. This prevents any perception that discounts influence decisions regarding settlements, credit approvals, or preferential treatment. No discount programs should be accepted during negotiations with clients.

Paid Invitations to Seminars, Conferences, and Promotional Meetings:

Invitations to attend conferences or seminars must be directed to Banque Misr's management, which will nominate the appropriate employee. Employees—especially those evaluating suppliers—must not accept personal invitations from suppliers without disclosure and prior approval.

Tips for Handling Invitations:

- Request details from the inviter about the event, objectives, costs, and obligations.
- Discuss the invitation with your manager for guidance.
- Consider the potential impact on transparency and conflicts of interest.
- Suggest redirecting the invitation to bank management directly.

What Should You Do If You Are Offered a Gift You Know Is Inappropriate?

Politely refuse and explain that bank policy prohibits acceptance. Giving or accepting gifts or entertainment may represent a conflict of interest and, in some cases, violate anti-bribery laws.
If you receive a gift without the opportunity to refuse, consult your manager or the Compliance Officer for guidance.

Giving Gifts

If giving a gift or entertainment could appear as compensation for a government or business interest or favoritism, you must not offer the gift or entertainment.
Gifts may be given to customers or business partners as a gesture of courtesy and appreciation to promote goodwill, provided they are approved by the bank and bear its logo. Unjustified gifts intended to secure personal gains or influence decisions are strictly prohibited.

External Relations and Conducting Business and Activities

Conflict of Interest in Contracts or Business

- Employees must ensure there is no direct or indirect relationship between individuals responsible for supply, maintenance, or sales contracts and other parties.
- If a bank employee involved in a transaction has any relationship with a company, supplier, or customer, this must be fully disclosed to the direct supervisor and the Compliance Officer.
- The supervisor must take necessary measures to eliminate any conflict of interest, protecting the bank's interests and ensuring transparency.

Conducting External Business

- Employees must not enter into partnerships or business relationships with customers or suppliers.
- Engaging in private business activities or providing services (such as consulting, training, or serving on boards of directors) in addition to the primary role at the bank is prohibited unless prior approval is obtained from the competent authority. This excludes official representation in companies where the bank holds shares.
- Approval will only be granted if such activities do not conflict with assigned duties and comply with relevant laws and regulations.

Exploiting Official Position

- Employees are prohibited from exploiting their official position for personal gain.
- Any attempt to unlawfully use job authority will result in strict disciplinary action in accordance with bank policies.

Political, Social, and Sports Activities

- Employees may join political parties and legitimate organizations (such as charitable, civil, social, or sports clubs) provided these activities do not conflict with the bank's interests and involve no financial compensation.

- Participation must comply with applicable laws and regulations, and employees must not exploit the bank's name, capacity, assets, or properties. Disclosure is required if these entities have dealings with the bank. Executive roles in managing such institutions require prior approval from the bank.

Using Political and Religious Symbols

- Employees are prohibited from engaging in political or religious discussions or debates in the workplace, as these may cause disagreements and hostility.
- Employees must not affiliate with any political or religious entity in an official capacity or as a representative of the bank.
- The use of political or religious symbols or logos within the workplace is prohibited to maintain a neutral and balanced environment.

Employee Accounts

Commercial and Banking Use of Personal Accounts

- Employees are prohibited from using their bank accounts, whether with the bank or any other banks, for any commercial purposes.
- Employees are prohibited from conducting banking or financial transactions related to their personal accounts or any other related accounts (by proxy or otherwise) using their user ID.
- Using employees' personal accounts or electronic payment methods in transactions related to gaming sites, betting, speculation, or in trading and cryptocurrency mining operations is prohibited.
- Care must be taken not to misuse the bank's products and services by the employee for purposes other than those designated. For example, using credit cards to execute fictitious purchases from merchants for the purpose of converting the credit limit to cash proceeds.
- Using employees' personal accounts for fundraising operations (such as donations or activities related to associations among employees) is prohibited
- All financial transfers between employee accounts must be based on legitimate necessity and clear justification. Using employee accounts as a means to pass illicit funds or to conceal the nature of transactions is completely prohibited
- Lending or borrowing between colleagues or with any external parties related to the bank is prohibited (this means personal advances between employees or with current customers, suppliers, or any external parties related to the bank)

Banking Transactions on Behalf of Customers

- Employees are prohibited from using their personal accounts to execute banking transactions belonging to a third party or on behalf of customers, except in the case of strong justifications requiring this, and after obtaining prior approval from the Compliance Department
- Support service employees are prohibited from executing any transactions for the benefit of bank customers
- Transactions such as cash deposits by hand or signing documents on behalf of customers may not be executed except in case of fulfilling official procedures and obtaining necessary approvals from competent authorities

Managing Powers of Attorney and Updating Data of Employees' Relatives

- Any employee is prohibited from accepting powers of attorney from customers to deal with their accounts and must cancel all issued powers of attorney, except those for direct kinship relations (such as parents, spouse, children, siblings)
- Employees must immediately update their relatives' data when they obtain additional benefits (such as preferential returns) in case the reason for their entitlement to this benefit ceases, such as:
    - Marriage for females
    - End of marital relationship
    - Reaching the specified age
- Using the agency relationship granted to the employee to execute transactions that do not belong to the agent is prohibited, especially for the purpose of concealment or hiding of those transactions

Compliance with Responding to Regulatory Inquiries

- Employees must provide a comprehensive response to inquiries from the Compliance and Institutional Governance Sector regarding bank accounts, with supporting documents provided within two business days.

Information Security

1. General Principles – New Employee

1.1 Onboarding and Orientation

Upon completion of the Bank's onboarding process and formal acknowledgment of the Code of Conduct, the employee commences their employment by participating in the induction training program. This program includes a dedicated Information Security awareness session designed to ensure that the employee fully understands their responsibilities in safeguarding the Bank's information assets and complying with applicable Information Security policies, procedures, standards, and guidelines.

Accordingly, the employee is granted access privileges strictly commensurate with their assigned role and job level, in accordance with the principle of least privilege and based on approved access authorization procedures.

2. Personal Obligations

2.1 Protection of Access and Login Credentials

Once issued and received, the employee's access card represents the employee's official identification within the Bank. Accordingly, the employee is expected to exercise due care in protecting the access card and to ensure that it is used exclusively by its authorized holder at all times.

Likewise, information technology systems access credentials, including user identification (IDs), passwords, and authentication codes are the employee's digital identity within the Bank and must be treated with strict confidentiality. Such credentials are personal and must never be disclosed, shared, or used by any other party.

Any misuse, disclosure, or sharing of access credentials constitutes a violation of the Bank's Information Security and regulatory framework and may result in disciplinary action.

3. Operational Obligations – Data Protection

3.1 Data Handling

Throughout their employment with the Bank, employees are entrusted with access to information that must be treated as confidential at all times. This obligation continues beyond the termination of the employment relationship, regardless of the reason for separation.

Employees are required to handle, process, and use information strictly in accordance with its assigned classification and to communicate or share such information only through officially approved channels. This ensures appropriate protection of information and helps prevent unauthorized disclosure.

Compliance with the handling requirements and safeguards defined for each classification level is mandatory to ensure the ongoing protection of the Bank's information assets. Information is classified under the following categories:

- **Public Data (Public):**
  Information intended for public disclosure and permitted for unrestricted internal and external sharing. This includes content officially published by the Bank, such as public announcements and information made available through the Bank's official website or other authorized public channels.

- **Internal Use Data (Internal):**
  Information designated for internal circulation within the Bank and not intended for external distribution. This category includes internal communications, staff circulars, human resources notices, and internal policies or procedures.

- **Confidential Data (Confidential):**
  Sensitive information that requires an elevated level of protection and may only be accessed, processed, or disclosed by authorized employees in accordance with their assigned roles and responsibilities. Examples include customer-related information and future business strategies.

- **Highly Confidential Data (Restricted):**
  Critical information that requires the highest level of protection and strict access controls. Access to this data is limited to explicitly authorized individuals only. This category includes, but is not limited to, employee compensation details.

4. Technological Obligations – Protection of Information Assets

4.1 Use of Bank Devices

All devices issued by the Bank, including (desktops, laptops, tablets, and smartphones), are considered official Bank assets. Employees are required to use these devices in a responsible and secure manner that supports the protection of the Bank's information, systems, and operational integrity.

4.2 Use of Email, Internet, and Bank Systems

The Bank's email, internet access, and information technology systems are provided exclusively for business-related purposes. Employees must not use Bank email accounts for personal activities, including registering on external websites or online services unrelated to work.

The Bank reserves the right to monitor and oversee the use of its email, internet, and information technology

systems to ensure compliance with Information Security policies. Any such monitoring shall be conducted in accordance with applicable laws and regulatory requirements.

4.3 Use of Personal Devices

The Bank allows, under defined controls and after obtaining the necessary approvals, the use of certain personal devices for business purposes, provided that connectivity to Bank services (e.g., email) is performed via Bank authorized applications. Employees using such devices are required to comply with the Bank's Information Security policies, standards, procedures, and guidelines to safeguard data, and must immediately report any loss, theft, or suspected security incident involving the device.

The Bank confirms that it does not monitor employees' personal data or private activities on personal devices. Any monitoring is strictly limited to Bank-related applications and data, solely for the purpose of protecting the Bank's information assets and without infringing on employee privacy.

4.4 Use of Artificial Intelligence Tools

The use of generative Artificial Intelligence (AI) tools is restricted to general, non-sensitive purposes only. Employees must not input any internal, confidential, operational, or Bank-related data, instructions, or information into such tools.

Employees remain fully accountable for any misuse of AI tools that results in unauthorized disclosure of information or creates reputational, legal, or operational risks to the Bank.

4.5 Clean Desk Policy

Employees are required to adhere to the clean desk principle as part of professional conduct and personal accountability. Device screens must be locked when unattended, and documents or files must be secured in locked drawers or cabinets when leaving the workspace or at the end of the workday.

Documents or media containing Bank or customer information must not be left unattended in shared areas or on printers. Any unnecessary documents must be securely disposed of using approved shredding facilities to maintain information confidentiality and protection.

5. Reporting and Escalation – Incident Response

5.1 Incident Reporting

Employees must promptly notify the Security Operations Center (SOC) of any event that may pose a risk to the Bank's information or information technology systems. This includes, but is not limited to, suspected cyber intrusion attempts, loss or theft of devices, unauthorized access to information technology systems, potential data leakage, interaction with suspicious links or attachments, compromised passwords or access credentials, or the presence of access privileges exceeding job-related requirements.

Timely reporting of such events is a fundamental responsibility of every employee and a critical component of the Bank's Information Security framework. Employees are required to fully cooperate with the Information Security team throughout incident investigations and remediation activities to ensure effective and timely incident response.

All Information Security incidents must be reported through the officially designated reporting channel: socteam@banquemisr.com

6. Sustainability and Development

6.1 Continuous Awareness

The Bank recognizes that continuous awareness and professional development are essential to establishing and maintaining a resilient Information Security culture. Accordingly, employees are required to periodically review Information Security Policy and attend all Information Security training sessions within the designated timeframes and to actively participate in awareness activities organized by the Bank to enhance their knowledge and capabilities in protecting information assets.

In addition, the Bank encourages employees to support and engage in Information Security awareness initiatives throughout the year, with particular emphasis on October, which is internationally recognized as Cybersecurity Awareness Month. These initiatives aim to reinforce shared responsibility and promote a security-conscious mindset across the workplace.

Compliance

Combating Money Laundering and Terrorism Financing

Money laundering is a crime aimed at conferring legitimacy on commercial operations and funds resulting from criminal and illicit practices. Terrorism financing is the deliberate act, by any means, of providing, collecting, or arranging funds or property, even if lawfully obtained, with the intention of using them to commit a terrorist act by a person or group, or providing assistance or advice for this purpose.

Banque Misr cooperates with governments, international organizations, and financial institutions in establishing and developing programs and policies that provide strong support for international efforts to combat money laundering, terrorism financing, and other criminal activities. We screen and conduct investigations regarding clients and ongoing transactions using rigorous procedures and an automated monitoring system.

Banque Misr's anti-money laundering procedures are implemented across all our business units worldwide regardless of their location, and all employees and senior managers must comply with them to avoid misuse of our name or our products and/or services for money laundering purposes. To ensure we apply best compliance practices, Banque Misr periodically reviews its anti-money laundering strategies and policies.

Compliance with money laundering and terrorism financing laws is the Bank's responsibility in general; therefore, all employees must exercise due diligence in properly implementing the Know Your Customer principle, ensuring customers' transactions are consistent with the nature of their activities and income, and promptly and accurately reporting any suspicious or inappropriate activity during transaction processing or customer dealings.

Employees are strictly prohibited from disclosing to any customer or beneficiary any data or information related to the investigation, examination, or reporting of any suspected cases involving money laundering.

All Banque Misr employees are committed to the principles of disclosure, transparency, and credibility when providing any information or data to the Central Bank of Egypt or any other regulatory bodies. Providing inaccurate or misleading information, or concealing any significant data, is strictly prohibited. All disclosure processes must be conducted in accordance with the Bank's approved internal procedures, ensuring full compliance with relevant laws and regulations.

When government authorities make direct contact to obtain data and information about customers, the relevant employee must immediately contact the "Compliance Officer" to ensure that such information will not conflict with banking secrecy laws.

Economic Sanctions and Embargo Programs

Financial and trade sanctions are part of a set of measures implemented by national governments, international organizations, or regional bodies to prohibit dealings or regulate trade with certain countries, entities, and individuals. Some of these measures are designed to punish countries for human rights violations or weapons proliferation, while others aim to limit trade with entities and persons associated with terrorism or drug trafficking. These sanctions aim to stimulate change in the behavior of an individual or state, or to deprive terrorists and criminals of access to funds.

Banque Misr has established internal policies and operational procedures to fully comply with embargo laws and economic sanctions imposed by national governments, international organizations, or regional bodies to restrict individuals and companies from dealing with certain countries, groups, entities, and individuals falling under these sanctions, and all employees must follow them precisely.

Banque Misr and its employees cannot provide advice to customers on how transactions should be structured or provide advice to evade applicable sanctions. This includes, but is not limited to, advising customers and counterparties to modify certain instructions to include details that may be false or misleading, or to change, remove, or delete information from transactions that would reveal threats.

Dealing with Related Parties

Dealing with Stakeholders

All employees must fully commit to transparency and credibility when dealing with stakeholders, including auditors, suppliers, relevant external parties, and governmental and banking institutions. Employees are required to disclose any conflict of interest immediately to ensure transparency and compliance with Banque Misr Group's directives, and to manage the conflict in accordance with international best practices and ethical standards. Required advice and information shall be provided accurately and clearly, with documentation of these dealings to ensure accountability and credibility.

The public dealing with the Bank expects all their transactions to be conducted fairly, professionally, and with complete confidentiality. To ensure banking services are delivered to high service standards and to improve the quality of services provided, it is necessary to adopt an approach aimed at earning customer satisfaction and providing public service at a professional level, in a manner that conveys a willingness to help, and in a style characterized by courtesy and respect.

Fair Dealing with Customers

All employees are committed to using appropriate means to assist customers in completing their banking transactions efficiently and in a manner that safeguards their rights in accordance with the Bank's instructions. They must also adhere to the following principles:

- Providing accurate and transparent information about banking products and services, including fees and associated risks, and ensuring the customer's complete understanding before making any decisions.

- Maintaining integrity, transparency, and impartiality in dealing with customers, and avoiding discrimination based on religion, gender, or nationality.

- Providing advice to customers in their banking dealings with the Bank.

- Not concealing information, misleading customers, rushing them into making decisions, or using unethical sales and promotion methods.

- Handling customer complaints quickly and effectively in accordance with documented internal procedures.

- Respecting the confidentiality of customer information and not disclosing it to any party except based on legal or written authorization.

- Avoiding promotion or advertising of customers' commercial activities, and not conducting any banking transactions on their behalf or for their benefit without prior authorization from Compliance Management.

- Respecting meeting schedules and dealing with credibility and professionalism in responding to customer inquiries and providing services.

Employees are prohibited from unnecessary access to customer accounts or providing recommendations without comprehensive risk assessment that aligns with the customer's financial objectives.

The Bank must maintain customers' master data in terms of adequacy and quality, and work to continuously update it, which increases our ability to design products suitable for each age and cultural segment. We, as Banque Misr employees, are committed to maintaining the confidentiality of this data and not disclosing or misusing it.

Dealing with the Central Bank of Egypt

Banque Misr employees are committed to the instructions issued by the Central Bank of Egypt, taking into account the principles of disclosure, transparency, and credibility when providing data and information to the Central Bank of Egypt and other regulatory authorities. Disclosure processes are conducted in accordance with approved internal procedures to ensure full compliance with relevant laws and regulations, with careful verification before sharing any information or data of significance within the scope of work of any employee. This may include:

- Immediate reporting of detected fraud cases to the Central Department for Combating Fraud Crimes at the Central Bank.

- Notifying the Anti-Money Laundering and Terrorism Financing Unit when unusual transactions carrying illegal suspicion are detected.

- Informing the Central Bank of any violations by key officials to assess the extent to which they meet the standards of merit and technical competence, with documentation of the decision taken by the Bank.

Disclosure shall be made only by the Bank's competent departments.

Responsibilities of Key Officials and Promoting Ethical Conduct

Managers at Banque Misr, as role models in promoting a culture of integrity and adherence to the highest standards of ethics and professional conduct, must represent a positive image that inspires and motivates their colleagues to excel in a work environment characterized by dignity and respect. Similarly, the scope of application of this Code includes all key officials – individuals who hold leadership positions that directly affect the Bank's reputation and strategic decisions – namely the Chairman and members of the Board of Directors, and executive managers responsible for key and supervisory activities, whose designation and terms of reference are determined by a resolution of the Bank's Board of Directors. The Bank must immediately notify the Central Bank if any key official commits any violation of instructions.

"Merit standards" here refers to those standards that ensure a person's competence and ability to continue performing their duties with high technical proficiency and professionalism, while "technical competence" refers to the technical and managerial qualifications necessary for them to continue efficiently fulfilling the tasks assigned to them.

The decision taken regarding the status of key officials when a violation occurs must be documented in accordance with applicable disciplinary procedures, to ensure transparency, enhance institutional governance, and comply with banking work standards and regulatory systems. In this regard, key officials must adhere to the following:

Performance Assessment and Oversight

Ensuring an impartial performance evaluation process is conducted for their subordinate employees, monitoring their performance evaluation and developing their skills and capabilities to ensure they continue to perform their job duties in the best manner, and promoting a culture of professional development within the team.

Handling Violations

If key officials become aware or receive information about an employee's violation of banking conduct rules, they must not cover up the violation, conduct a comprehensive investigation with the employee or relevant work group, and take appropriate disciplinary action. They should encourage a culture of reporting violations in a manner that reinforces the principle of transparency without compromising the rights of whistleblowers, while ensuring no negative action is taken against the reporting employee.

Managing Conflicts of Interest and Compliance with Bank Policies

Encouraging employees to adhere to the principles of conflict-of-interest management and policies for reporting violations and unlawful practices, and ensuring disclosure of any relationship that may constitute a conflict of interest.

Commitment to not entering into partnership or business relationships with the Bank's clients, not engaging in commercial activities, providing consulting services, or holding additional positions without obtaining prior approval from the competent authority, and preventing exploitation of job position for personal gain.

Awareness and Training

Raising employee awareness of the gift acceptance policy and ensuring compliance with it, and ensuring that gifts exceeding the specified limits that may negatively affect the Bank's reputation are not accepted.

Guidance and awareness on how to deal with media and social media, in addition to implementing the information security policy. Requiring employees not to discuss religious or political matters during working hours, within the workplace, or when representing the Bank externally.

Preserving the Bank's Property and Assets

Emphasizing the necessity of preserving the Bank's assets and property, which include fixed and current assets, documents, intellectual property, and customer assets under the Bank's control. Any unlawful use or exploitation of the Bank's assets or deriving personal benefit from them is prohibited.

Accuracy in Disclosure

Before disclosing to the Central Bank any important information or data falling within the scope of the Bank's work, key officials must verify the accuracy and correctness of the information and disclose it fully and in a timely manner, in accordance with current instructions.

Monitoring Contracts and Tasks Assigned to External Parties

When contracting with an external party to assign certain specific tasks, the competence of those executing those tasks must be verified, and their completion must be monitored according to the required timeline and specifications, with necessary actions taken in case of failure to meet requirements.

Our community

Sustainability

The policies adopted by Banque Misr reflect a strong commitment toward achieving its objectives and ensuring compliance with sustainability principles. At Banque Misr, we strive to maintain high service standards by seeking new opportunities to develop our work and social environment, which will have a positive impact on the economy and society.

Our vision for sustainability includes three main dimensions:

Economic Dimension

Strongly emphasizes the ethical conduct of our employees within the Bank and includes: governance, combating corruption, protecting consumer rights, and respecting stakeholder interests, in addition to commitment to the rule of law in any decision-making process and developing a robust operational governance model.

Environmental Dimension

The Bank closely monitors any potential harmful effects on the environment that occur as a direct or indirect result of any of the Bank's operations, products, services, or resources.

Social Dimension

Requires the Bank's full respect for cultural standards, social values, and differences among employees, in addition to participation in projects with significant social and/or developmental impact.

Social Responsibility

Social responsibility lies at the core of Banque Misr's strategy and in the hearts of its employees. It is an integral part of the way we work and how we measure our success in maintaining sustainability.

Banque Misr's policy on social responsibility reflects the Bank's approach to achieving its objectives while ensuring commitment to good social responsibility conduct and practices. The Bank is always seeking appropriate opportunities to contribute to the well-being of the community in which we operate, as well as providing a good work environment for its employees.

For more information, please refer to: Banque Misr's Social Responsibility Policies

Scope of Application and Consequences of Non-Compliance

These instructions apply to all Bank employees in the Arab Republic of Egypt and abroad, as well as key officials and members of the Board of Directors. They represent the minimum ethical and professional standards that everyone must adhere to in their dealings inside and outside the Bank to protect the Bank's reputation and enhance its credibility. In this context, "employees" are defined as all individuals working for the Bank, and "key officials" are those who hold leadership positions whose decisions bear an impact on the Bank's overall performance.

In case of violation of these instructions, which constitute a binding framework based on the directives of the Central Bank of Egypt, appropriate disciplinary actions are taken in accordance with applicable procedures, and may include verbal or written warnings, deduction from incentives, or even dismissal from work, in order to preserve work integrity and maintain the Bank's reputation.

Everyone is required to fully comply with behaviors that ensure honesty and integrity and not engage in any fraudulent, unethical, or unlawful practices, as well as not violate laws, regulatory controls, internal policies and procedures, with the necessity of immediately reporting any situation that may put the Bank's reputation at risk.

The Bank provides a reporting mechanism in accordance with the Whistleblowing Policy, which enjoys complete confidentiality. The Bank provides full protection to the whistleblower, does not disclose their identity, and does not take any retaliatory actions against them as long as good faith is present. This is done by contacting (the Whistleblowing Manager and/or the Head of Compliance and Institutional Governance Sector) by phone, in writing, via email, or through a platform for receiving reports related to cases that employees wish to report with complete confidentiality, through the following channels:

Hotline: 2222

Email: ***Whistleblowing@banquemisr.com***

I Voice Up Platform

(For more details, please refer to the Whistleblowing Policy on the Bank's internal network)

Breach of compliance with the rules and regulations of professional conduct is subject to the penalty regulations regardless of job position, in accordance with the investigation system and procedures and the penalty regulations for Bank employees, taking into account whether the violation was committed intentionally or not, the extent of the violator's good faith when committing the violation, and whether they reported it or not.

Disciplinary action may be taken against:

- Any employee who allows, directs, approves, or participates in violating behavioral principles and controls.
- Any employee who did not report, concealed, or covered up the existence of a violation, or deliberately withheld information related to a violation of work principles and professional conduct controls.
- Any official who did not report the violation despite knowing of its occurrence through being informed of it by their subordinates. The employee's initiative to report any violation they committed is taken into account.
- Any report based on false or misleading information.
- Bad faith and malicious reports, or the whistleblower deliberately implicating an employee's name in the report without verifying accuracy, speculating without evidence, or fabricating evidence.

Acknowledgement

Acknowledgement of Commitment to the Code of Conduct

I, the undersigned, hereby acknowledge that I have reviewed the Code of Banking Conduct and fully understand all the provisions contained therein. I agree to abide by them, in letter and spirit, in the performance of my duties within the Bank.

I also pledge to perform my work with honesty, sincerity, and integrity, and to uphold the honor of the profession and comply with the provisions of laws and resolutions regulating banking operations, thereby ensuring the promotion of the principles of transparency and professional discipline.

I affirm my full commitment to protecting the secrets and confidentiality of the Bank and its customers, and to respecting all ethical rules and work conduct, which reinforces the spirit of belonging and loyalty to Bank Misr throughout my tenure.

I further acknowledge that the Code of Banking Conduct constitutes an integral part of the Bank's policies, and compliance therewith is an essential condition for continued employment for all employees.

Accordingly, I sign this Acknowledgement in confirmation of my commitment to everything stated herein.

This is my acknowledgement thereof.

Name **:** ……

Signature : ……

Oracle ID : …… Dated in: ……