

**POLICY ON CORPORATE CODE OF CONDUCT**

---

**I. POLICY**

It is the policy of Amalgamated Bank of Chicago (the “Bank”) to require compliance by all directors, officers, employees, agents and attorneys with the Bank’s corporate code of conduct and ethics. This measure is taken to protect the Bank, its management, employees, customers, suppliers and others from unethical behavior and practices; to maintain appropriate workplace protocol and conditions; to promote honest and ethical conduct, compliance with applicable rules and regulations, and accountability in adhering to a corporate code of conduct or ethics policy; and to provide an appropriate environment for the transaction of all Bank business matters.

**II. GUIDELINES**

This code includes guidelines and procedures on acceptable and unacceptable business practices as outlined in statements of policy. Please review the following policies:

- 2-1: Corrupt Practices and Conflicts of Interest Under Federal Bank Bribery Law
- 2-2: Confidential Nature of Bank Affairs
- 2-16: Elder Abuse Policy
- 5-9: Information Technology Systems Security Policy
- 6-1: Professional Work Environment
- 6-2: Policy on Alcohol and Drugs
- 6-3: Sexual Harassment
- 6-4: Policy on Equal Employment Opportunity
- 6-5: Travel Expense Policy
- 6-9: Cellular Phone Business Expense Policy
- 6-10-: Corporate Credit Card Policy
- 7-2: Data Backup and Recovery Policy
- 7-3: Electronic Mail Policy
- 7-7: Incident Response Policy
- 7-8: Malware Protection Policy
- 7-10: Workstation Policy
- 7-12: IT Acceptable Use Policy
- 7-14: Media Tracking Policy
- 7-20: IT Acceptable Use Policy for Employee-Owned Mobile Devices
- 7-21: IT Acceptable Use Policy for Bank-Owned Mobile Devices
- 7-22: Social Media Employee Policy and Guidelines

Please note that other policies as found in the Bank Policy and Procedure book serve as a comprehensive primary reference for appropriate interaction, conduct, ethical behavior and internally and externally established rules and regulations.

Compliance with the code of conduct will be monitored by managers and supervisors along with the Legal, Information Services and Human Resources departments. Violators will be subject to specific and appropriate actions to deter wrongdoing, compel accountability and promote adherence to all policies and codes and may evoke the disciplinary process (up to and including termination).

Bank directors, officers, and employees shall sign a written acknowledgement of the corporate code of conduct or ethics policy, including written acknowledgement of any subsequent material changes to the code or policy on a regular basis. Additionally, periodic training on ethics and conduct is provided. New employees to the Bank receive initial information from the employee handbook as well as during new employee orientation.

### **III. GENERAL PROVISIONS**

Integrity and ethical values of the highest standard are to be maintained by Bank personnel (directors, officers, employees, agents and attorneys) at all times. Such personnel are prohibited from:

1. soliciting for themselves or for a third party (other than the Bank itself) anything of value from anyone in return for any business, service or confidential information of the Bank, and
2. accepting anything of value (other than bona fide salary, wages and fees referred to in 18 U.S.C. 215(C) from anyone in connection with the business of the Bank, either before or after a transaction is discussed or consummated.

#### **A. Observing Applicable Laws**

The Board of Directors is to ensure that Bank management is cognizant of all applicable laws and regulations and that compliance with all laws and regulations is a high priority. Bank management consideration includes the following regulations in policies, when applicable:

- **Section 18(k) of the Federal Deposit Insurance Act (FDI Act)**– "Authority to Regulate or Prohibit Certain Forms of Benefits to Institution-Affiliated Parties"
- **Part 359 of the FDIC Rules and Regulations** – "Golden Parachutes and Indemnification Payments"

- **Section 39(c) of the FDI Act** – "Compensation Standards"
- **Section 32 of the FDI Act** – "Agency Disapproval of Directors and Senior Executive Officers of Insured Depository Institutions or Depository Institution Holding Companies"
- **Section 19 of the FDI Act** – "Penalty for Unauthorized Participation by Convicted Individual"
- **Part 349 of the FDIC Rules and Regulations** – "Reports and Public Disclosure of Indebtedness of Executive Officers and Principal Shareholders to a State Nonmember Bank and its Correspondent Banks"
- **Sections 22(g) and 22(h) of the Federal Reserve Act** – "Loans to Executive Officers of Banks and Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Member Banks"
- **The Federal Reserve Board's Regulation O** – "Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks"
- **Section 337.3 of the FDIC Rules and Regulations** – "Limits on Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Insured Nonmember Banks"
- **Part 348 of the FDIC Rules and Regulations** – "Management Official Interlocks"
- **Section 7(j) of the FDI Act and the Change in Bank Control Act of 1978**
- **Section 737 of the Gramm-Leach-Bliley Act** – "Bank Officers and Directors as Officers and Directors of Public Utilities"
- **Section 8(e) of the FDI Act** – "Removal and Prohibition Authority"
- **Section 8(g) of the FDI Act** – "Felony Charge Involving Dishonesty or Breach of Trust as Cause for Suspension, Removal, or Prohibition"

## **B. Background Checks**

Human Resources has developed a risk-focused approach in the implementation of pre-employment background screening. It is appropriate to increase the level of screening based upon the position and responsibilities.

**C. Audit Responsibility in Monitoring Corporate Code of Conduct**

Internal controls against self-serving practices and conflicts of interest are monitored primarily by the Audit Department to identify operational weaknesses and to ensure corrective action and compliance with laws, regulations and internal policies.

**D. Management Responsibility in Monitoring Five-Day Vacation Absence Requirement**

All employees who are eligible for five (5) days or more of vacation during any calendar year are required to take 5 vacation days consecutively at least once during that year. Neither holidays nor non-business days can be counted as part of the 5-day absence period.

Furthermore, employees who have VPN capabilities must notify Information Services at least 5 days in advance of the scheduled 5-day vacation period in order to suspend VPN capabilities for those dates. This will ensure that online transactional capability is unavailable to the vacationing employee.

Managers are responsible for ensuring compliance with these guidelines for employees who report to them.

**E. Periodic Policy Updates to Reflect New Business Activities**

Institutions should update policies frequently to encompass new business activities.

**F. Confidentiality**

It is the policy of the Bank as well as a requirement of federal and state law that employees shall keep in strict confidence all information received by them regarding the affairs of customers and general Bank business (i.e., business and financial conditions, credit status, management planning, etc.). Safeguarding confidential information shall be in accordance with the Gramm-Leach-Bliley Act (GLBA) of 1999 which outlines that financial institutions are required to have administrative, technical and physical safeguards for sensitive customer information. Sensitive information collected by the institution must not be used or disclosed for any reason other than the intended purpose and must be protected from misuse that could result in identity theft.

The improper release of such information is grounds for disciplinary action up to and including termination. If you should disclose such information after leaving the Bank's employ, the Bank reserves the right to take legal action against you.

#### **G. Conflicts of Interest**

The Bank has a policy regarding the receipt and reporting of offers under the Federal Bank Bribery Act. This policy is intended to outline compliance procedures to all Bank directors, officers, employees, agents and attorneys concerning the receipt of gifts and reporting offers of gifts from customers and prospective customers.

Requests for or acceptance of gifts, fees or other rewards from customers or prospective customers of the Bank is prohibited unless (a) the situation is covered by one of several stated exceptions, or (b) advance approval is received from the Bank's General Counsel.

An offer of a gift, fee or other reward must be reported even if not accepted if (a) it cannot be accepted because of the policy, or (b) if advance approval is required in order to accept it.

Human Resources supply each new employee with information regarding this Act on the first day of employment. At that time, employees are required to sign a statement acknowledging receipt of this information. Additionally, the Legal Department obtains Conflict of Interest statements from all Bank officers on an annual basis.

#### **H. Outside Employment**

To avoid potential conflicts of interest while employed by the Bank, employees are prohibited from accepting additional employment with other non-affiliated financial institutions, current Bank customers or companies that do business with the Bank. Outside employment is additionally subject to federal regulations dealing with conflict of interest and to other applicable principles of law. Additionally prohibited are second jobs that interfere with an employee's ability to perform his/her regular Bank responsibilities. Consequently, the Bank reserves the right to approve all outside jobs (includes jobs with affiliated companies) prior to accepting the position. You must immediately notify the Human Resources Department in writing, if you are considering a second job, for a more detailed explanation of this policy. Failure to do so is grounds for disciplinary actions up to and including termination.

**I. Privacy**

Every effort must be made to respect and protect the privacy of all employees. For audit and security purposes, the Bank reserves the right to unlock, open or inspect any desk, locker, cabinet or other containers on Bank premises. In addition, checking accounts are periodically reviewed by our Audit Department.

**J. Internal Asset Controls**

Employees, officers and directors must comply with all internal control procedures established by the institution for the safeguarding of assets and proper reporting and disclosure of financial information.

**K. Dealing with Auditors, Examiners and Legal Counsel**

All directors, officers, employees, agents and attorneys should be required to respond honestly and candidly when dealing with the Bank's independent and internal auditors, regulators and attorneys.

**L. Record Integrity**

Records and accounting information must be accurate and maintained with reliability and integrity and transactions must be reflected in an accurate and timely manner. Bank policy prohibits false entries and activities that result in false entries.

**M. Media Contact**

Any communication with or disclosures of information to the media must be in accordance with the policies and procedures established by the Bank's Legal Department. This includes responding to calls from the media, taking a public stand on political matters in the name of the Bank, making a financial commitment with Bank funds, taking a leadership position in a political or public organization, or taking a position on behalf of the Bank before any regulatory or political agency. Employees may not endorse or publicly advocate the support of a candidate or political party in the name of or on behalf of the Bank.

**N. Solicitation**

Solicitation for products, services or charities during business hours or on Bank property can have a negative impact on our ability to serve customers. For this reason, no soliciting is allowed during working hours unless all parties involved are on a lunch or break in the Bank lunchroom.

**O. Misuse of Bank Accounts**

Employees are prohibited from performing transactions/maintenance on their own accounts at the Bank. This includes, but is not limited to: increasing credit card limits, waiving fees, changing maturity dates, changing float dates, tellers cashing their own checks, etc. Failure to adhere to this policy will be grounds for disciplinary action up to and including termination.

**P. Reporting Questionable Activity**

Any employee who has observed any questionable activity as outlined in this policy should immediately bring the matter to the attention of the Legal Department. Retaliation against any employee for filing a complaint or participating in an investigation is strictly prohibited.

All complaints will be investigated and information will be treated as confidentially as is necessary for the investigation. If an investigation confirms that an employee has violated this policy, prompt corrective action, up to and including discharge, will be taken.

**IV. SUMMARY**

Compliance with the code of conduct is required for all directors, officers, employees, agents and attorneys of the Bank. Violations are subject to specific and appropriate actions to deter wrongdoing, compel accountability and promote adherence to all policies and codes and may evoke the disciplinary process (up to and including termination).