CODE OF ETHICS AND BUSINESS CONDUCT
First Capital, Inc.

This Code of Ethics and Business Conduct ('Code') represents an overview of the corporate policies that should govern the actions of all employees, officers and directors of First Capital, Inc. and its subsidiaries (collectively, the 'Bank'). This Code is not a replacement for policies and procedures that address the specifics of our business or which may impose stricter or more detailed requirements.

No code of conduct can cover every potential situation. This Code is designed to provide written standards to promote honest and ethical conduct, compliance with the law, and a vehicle for prompt internal reporting and accountability to assure adherence to this Code. It is the responsibility of each individual to apply the principles set forth in this Code in a serious and respectful fashion and with the exercise of good business judgment. Failure to adhere to the requirements of this Code and the policies and procedures set forth in it may result in disciplinary action up to and including dismissal.

Certain parts of this Code may apply to specific 'executive officers.' Executive officer means a member of the management of the Bank or a subsidiary of the Bank so designated by resolution of the Board of Directors.

The policies and procedures contained in this Code do not constitute a legal contract and may be changed, modified or discontinued from time to time without notice (except as required by law) and in the sole discretion of the Bank. Except as otherwise provided by written agreement or applicable law, persons employed by the Bank or its subsidiaries are employed at will, and the Bank reserves the right to take employment action, including termination, at any time, for any reason, without notice.

FINANCIAL POLICIES

Use of Bank Assets
The Bank's assets are to be used exclusively in the pursuit of the Bank's business except for minimal personal use authorized by your supervisor in accordance with other Bank policies. The Bank's assets include equipment, facilities, supplies, services such as telephones and computer networks, and the time and efforts of its employees. Employees should not use Bank assets for personal gain or convenience, or make Bank assets available for the gain or convenience of anyone else, or for any purpose other than conducting the Bank's business unless they have management authorization to do so.

Authority to Make Commitments
Only specific employees are authorized to make financial or other commitments on behalf of the Bank. Commitments might be such things as approving a loan or other extension of credit, ordering equipment or materials, authorizing business travel, approving payment of an invoice or expense report, authorizing budgets or budget overruns, signing leases or other contracts, selling Bank assets, settling litigation or other claims, borrowing money, setting compensation or employee benefits, making charitable contributions and other transactions. Employees should not commit the Bank to any obligation unless they have the authority to do so. These authorizations are in writing and are governed by corporate policies.

Bribes and Other Illegal Corporate Payments
The use of Bank funds for payments to any individual, company or organization for the purpose of obtaining favorable treatment in securing business or other special considerations is prohibited by law. This policy does not prohibit normal and customary business expenses such as reasonable entertainment, trade organization dues or similar expenses that are allowed by applicable Bank policies, which must be properly reported on an expense report form.

Relations with Government Employees
The U.S. Government has various regulations prohibiting government personnel from accepting entertainment, gifts, gratuities or other business courtesies that may be acceptable in the private commercial sector. All Bank employees who may have to make these sorts of judgments must understand and comply with the letter and intent of such regulations.

Integrity of Records and Reports
The Bank's accounting records are relied upon to produce reports to the Bank's management, shareholders, government agencies and other entities. All Bank accounting records, and the reports produced from those records, shall be kept and presented in a timely fashion and in accordance with the applicable laws, rules and regulations of each jurisdiction. Such records and reports must constitute understandable disclosure and fully, accurately, and fairly reflect in reasonable detail the Bank's assets, liabilities, revenues and expenses.

Responsibility for accurate and complete financial records does not rest solely with the Bank's accounting employees. All employees involved in approving transactions, supplying supporting information for transactions and determining account classifications have responsibility for complying with our policies.

Reports to Management
The same high standards required in the Bank's external reporting apply to financial reports to management. Accruals and estimates included in internal reports (such as business plans, budgets and forecasts) shall be supported by appropriate documentation and based on good-faith judgment.

Payments and Disbursements
All payments made by or on behalf of the Bank must be documented in the accounting records with the appropriate approval(s) and an adequate description of the business purpose of the disbursement.

Cash Deposits and Bank Accounts
All cash that the Bank receives shall be promptly recorded in the accounting records and deposited in a bank account properly authorized by the Bank. All bank accounts and other cash accounts shall be clearly and accurately recorded in the accounting records. No unrecorded accounts, funds, or assets shall be established for any purpose.

Cooperation with Inquiries
Employees shall provide complete and accurate information in response to inquiries from the Bank's internal and outside independent auditors as well as the Bank's legal counsel.

POLITICAL CONTRIBUTIONS AND ACTIVITIES

No Bank funds or assets, including the work time of any employee, may be contributed, loaned or made available, directly or indirectly, to any political party or to the campaign of any candidate for a local, state or federal office.

CONFLICTS OF INTEREST

Employees must carry out their professional responsibilities with integrity and with a sense of loyalty to the Bank. They must avoid any situation that involves a possible conflict or an appearance of a conflict of interest between their personal interests and the interests of the Bank. Knowingly acting in a manner that presents a conflict between their personal interests and the best interests of the Bank is a violation of this Code.

A conflict of interest cannot be defined precisely, only illustrated. The basic factor that exists in all conflict situations is a division of loyalty between the Bank's best interests and the personal interest of the individual. Many, but not all, conflict situations arise from personal loyalties or personal financial dealings. It is impossible to list every circumstance giving rise to a possible conflict of interest, but the following illustrates the types of situations that may cause conflicts.

Family Members
A conflict of interest may exist when the Bank does business with or competes with an organization in which a family member has an ownership or employment interest. Family members include a spouse, parents, children, siblings and in-laws. Employees may not conduct business on behalf of the Bank with family members or an organization with which they or a family member is associated unless they receive prior written approval under this Code.

Ownership in Other Businesses
Employee cannot own, directly or indirectly, a significant financial interest in any business entity that does business with or is in competition with the Bank unless they receive prior written approval under this Code. As a guide, "a significant financial interest" is defined as ownership by an employee and/or family members of more than 5% of the outstanding securities/capital value of a corporation or ownership that represents more than 5% of the total assets by the employee and/or family members. This is <u>not</u> a "bright line" rule. Ownership interests less than this percentage may be deemed "significant" depending on the specific facts and circumstances.

Outside Employment
Employees must keep outside business activities, such as a second job or self-employment, completely separate from the employee's activities with the Bank. Employees may not use Bank assets, facilities, materials, or the services of other employees for outside activities unless specifically authorized by the Bank, such as for certain volunteer work.

Disclosure Required – *When in Doubt, Ask!*
Employees should avoid any actual or apparent conflict of interest. Conflicts can arise unexpectedly and prompt disclosure is critically important. Employees must disclose existing or emerging conflicts of interest (including personal relationships that could reasonably be considered to create conflicts) to their supervisor and follow the guidance provided. Executive officers and directors must disclose existing or emerging conflicts of interest to the President and Chief Executive Officer of the Bank.

ACCEPTING GIFTS AND GRATUITIES

Accepting Things of Value
Except as provided below, employees may not solicit or accept for themselves or for a third party anything of value from anyone in return for any business, service or confidential information with respect to the Bank. Things of value include gifts, meals, favors, services and entertainment. The purpose of this policy is to ensure that the Bank's business is safeguarded from undue influence of bribery and personal favors.

The solicitation and acceptance of things of value is generally prohibited by the Bank Bribery Act. Violations may be punished by fines and imprisonment.

Permitted Transactions
The following transactions are permitted and will be considered as exceptions to the general prohibition against accepting things of value:

- Acceptance of gifts, gratuities, amenities or favors based on family or personal relationships when the circumstances make clear that it is those relationships, rather than the business of the Bank, that are the motivating factors;

- Acceptance of meals, refreshments, travel arrangements, accommodations or entertainment, all of a reasonable value, in the course of a meeting or other occasion, the purpose of which is to hold bona fide business discussions or to foster better business relations, provided that the expense would be paid for by the Bank as a reasonable business expense if not paid for by another party;

- Acceptance of advertising or promotional material of reasonable value, such as pens, pencils, note pads, key chains, calendars and similar items;

- Acceptance of discounts or rebates on merchandise or services that do not exceed those available to other customers;

- Acceptance of gifts of reasonable value related to commonly recognized events or occasions, such as a promotion, new job, wedding, retirement, birthday or holiday; or

- Acceptance of civic, charitable, education or religious organizational awards for recognition of service and accomplishment.

The Bank maintains detailed written policies and procedures that govern the acceptance of permitted gifts and gratuities. You should refer to such policies and procedures for more specific guidance.

Other Transactions
If an employee is offered or receives something of value beyond what is permitted by this Code and related policies and procedures, they must obtain prior approval before they may accept or keep it. Transactions other than those described above may be approved so long as approval is consistent with the Bank Bribery Act. If an employee is at all uncertain as to whether they may accept something of value, they should not hesitate to ask.

CORPORATE OPPORTUNITIES

Directors and officers of the Bank stand in a fiduciary relationship to the Bank. It is a breach of this duty for any such person to take advantage of a business opportunity for his or her own personal profit or benefit when the opportunity is within the corporate powers of the Bank and when the opportunity is of present or potential practical advantage to the Bank, unless the Board of Directors knowingly elects not to avail itself of such opportunity and the director's or officer's participation is approved in advance by the Board. It is the policy of the Bank that no director or executive officer appropriates a corporate opportunity without the prior consent of the Board of Directors.

EQUAL EMPLOYMENT OPPORTUNITY, HARASSMENT, AND SEXUAL HARASSMENT

Equal Employment Opportunity
It is the policy of the Bank to provide equal employment opportunity in full compliance with all federal state and local equal employment laws and regulations.

Harassment Prohibited
The Bank is committed to providing a work environment where all employees work free from harassment because of race, color, religion, age, gender, sexual orientation, national origin, disability or any characteristic protected by applicable law. The Bank will not tolerate harassment by employees, supervisors, customers or others.

The Bank's policy is essentially based on common sense: all employees should treat each other with respect and courtesy. Harassment in any form – including verbal and physical conduct, visual displays, threats, demands and retaliation – is prohibited.

What Constitutes Sexual Harassment
The Equal Employment Opportunity Commission has guidelines that define sexual harassment as unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature when:

- Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment, or used as the basis for employment decisions affecting such individual; or

- Such conduct creates an intimidating, hostile or offensive working environment.

Sexual harassment can involve either a tangible employment action or a hostile work environment. Sexual harassment includes more than overt physical or verbal intimidation. Lewd or vulgar remarks, suggestive comments, posters, pictures and calendars, pressure for dates and sexual favors, and unacceptable physical contact are some examples of what can constitute harassment.

It is important to realize that what may not be offensive to one person *may* be offensive to someone else. Employees should consider carefully the effect of their words and actions on others, and should not assume that another employee's failure to object means that the employee welcomes the behavior at issue.

The Bank, as a general matter, does not seek to regulate the private social behavior of employees. However, intimate relationships between supervisors and employees whom they directly supervise are discouraged. Because of the undesirable workplace repercussions that they may have, any such ongoing relationship should be disclosed to the supervisor's department head. All employees should understand that no one at the Bank has the authority to offer job benefits or threaten job disadvantages based on the provision of sexual favors.

Sexual harassment also can occur among co-workers or result form behavior by contractors or other non-employees who have reason to interact with Bank employees. Our policy extends to those circumstances as well.

Obligation to Report
Any employee who has reason to believe that he or she is being harassed must promptly report the harassment. The official procedure for reporting violations or suspected violations of this policy is located later in this Code under the heading "How to Report a Violation." Employees should not allow an inappropriate situation to continue by not reporting it, regardless of who is creating the situation.

Investigations
As set forth later in this Code under the heading "Administration of the Code of Business Conduct," the Bank will promptly investigate allegations of harassment and, to the extent possible, conduct such investigations confidentially. Any employee who is found to have violated this policy is subject to discipline or discharge.

No Retaliation
The Bank will not tolerate retaliation in any form against an employee who has, in good faith, reported an incident of harassment, and employees should not fear that such a report will endanger his or her job.

ILLEGAL AND IMPAIRING SUBSTANCES

Employees may not possess, use, sell, distribute or be under the influence of illegal drugs while on Bank property or while conducting Bank business anywhere. Such behavior is a violation of Bank policy in addition to a violation of the law.

When reporting for work and throughout the work day, employees must be fit for duty at all times and, in particular, not pose a safety hazard to themselves or others through the use of alcohol or other legal, but impairing, substances.

WORKPLACE VIOLENCE

The Bank expressly prohibits any acts of violence or threats of violence by any Bank employee against any other person in or about Bank facilities or in connection with the conduct of Bank business elsewhere at any time.

Employees are prohibited from possessing firearms while on Bank property or while conducting Bank business anywhere at any time except as provided by law.

MARKETING PRACTICES AND ANTITRUST

Marketing Practices
The Bank's products and services must be sold fairly and honestly. Employees should not attempt to take advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair practice. Many of the products and services provided by the Bank are subject to laws and regulations that specify the information that must be provided to the Bank's customers. It is the policy of the Bank to comply fully with these disclosure requirements.

Antitrust
The antitrust laws are intended to foster free and open competition and it is important that the Bank comply with the letter and spirit of such laws. Agreements that reduce business competition are a core concern of the antitrust laws and violations may result in severe civil and criminal penalties to the Bank and to individuals. Antitrust laws pertain to dealings with customers and suppliers as well as competitors.

In some cases, depending on the circumstances, the antitrust laws prohibit discussions among competitors about competitively sensitive subjects. The most serious antitrust violations are agreements among competitors that directly restrict competition among them.

These include agreements:

- To raise, lower or stabilize prices;
- To divide the areas in which they will do business or the customers they will serve; or
- To refuse to deal with certain customers or suppliers.

Conduct intended to drive a competitor out of business may also violate antitrust laws. It is the policy of the Bank to comply fully with all applicable antitrust laws.

Antitrust is a complex area of the law and violations have serious consequences for the Bank and for individuals personally. The Bank's legal counsel should be consulted with any questions.

COMPUTER NETWORKS, VOICE MAIL, E-MAIL AND THE INTERNET

Many Bank employees depend on access to computer networks, voice mail, e-mail, and/or the Internet to perform their jobs. These tools come with risks and responsibilities that all employees must understand and accept.

Employees must use these resources only for the business activities of the Bank (except as described below under the heading “Authorized Uses”) and:

- Properly identify yourself in electronic communication;
- Use only your own password and user ID to gain access to systems or data;
- Accept full personal responsibility for the activities undertaken with your password and user ID;
- Delete e-mail, voice mail and other electronic files in accordance with applicable record retention policies; and
- Comply with the computer security policies of the Bank and conduct themselves in a manner that protects the Bank from damage, theft, waste and violations of the law, including:

  (a) Protecting against exposure to potentially destructive elements, intentional (viruses, sabotage, etc.) or unintentional (bugs); and

  (b) Protecting against unauthorized access to Bank information or resources (hacking).

Company Property and Privacy
Computer networks and electronic communications systems, and all messages and log files generated on or handled by them (including back-up copies), are considered to be the property of the Bank.

There should be no expectation of privacy in these electronic interactions. The Bank may monitor the content of employees’ electronic communications or monitor the content of server log files to review what websites or other Internet locations employees have visited and what files they may have sent or received. Computer networks, e-mail systems, voice mail systems and server logs are monitored regularly to support routine and non-routine activities such as operations, maintenance, auditing, security and investigations. Employees should also keep in mind that, as a matter of law, the Bank may be called upon to turn over this information to law enforcement and private litigants.

Employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications or Internet activity except as specifically provided above and only then with appropriate authorization.

Authorized Uses
Bank computer networks, e-mail and voice mail systems and Internet access generally must be used only for Bank business activities. Incidental personal use is permitted if it:

- Does not preempt or interfere with any Bank business activity or with employee productivity and consumes only a trivial amount of Bank resources.

Incidental personal use is subject to the same policies as business use.

Prohibited Uses
Under no circumstance should Bank computer networks, e-mail and voice mail systems or Internet access be used:

- For any illegal activity;
- To communicate offensive sexual, racial or other remarks, jokes, slurs and obscenities;
- For private business, commercial or solicitation activities;
- For chain-letter communications of any kind;
- For charitable endeavors that are not Company-sponsored or authorized, including any fundraising;
- For gambling;
- For pornography; or
- For social media
    - Employees may not post non-public information to any social media site via text or picture. This includes pictures taken in the branch that may contain computer screens, paperwork, or customers.
    - Employees may not post information about products or services offered by the Bank. This includes special promotions or new services. This type of information will be posted by the Marketing Department with approval from Compliance.
    - Employees may not post advice to potential or current stakeholders.

Additional uses may be prohibited or limited by other provisions of this Code or by other Bank policies.

CONFIDENTIAL INFORMATION

Many employees learn confidential Bank information in the course of their jobs and use it to perform important functions. It is vitally important that all employees handle confidential information properly.

There are two major concerns:

- Preventing the release of unauthorized or inappropriate information that might adversely affect the Bank's business; and
- Avoiding violations of the law, particularly the securities laws relating to disclosure of material financial information before the information is made public.

What is Confidential Information?

What follows is not a complete list of what is considered to be confidential information, but it illustrates what is typically confidential unless it has been disclosed by the Bank in a securities filing, press release, or other authorized formal or official public communication:

- Financial results, budgets or forecasts;
- Business plans, operating plans, strategy statements, memos, operating manuals, organization charts and other internal communications;
- Bank investments, acquisitions or divestitures;
- New products, processes or designs;
- Whether a product or business is meeting financial or other expectations;
- Business relationships or the terms of any business arrangement, including prices paid or received by the Bank;
- Customer data such as customer names and addresses or any confidential personal or business information of the customer;
- Advertising and marketing plans and campaigns;
- Wages and salaries, bonus or compensation plans, notices to employees or unannounced personnel changes; and
- Personal information about any employee.

In general, if the Bank has not made public information about itself, it should be treated as confidential.

Non-Disclosure and Non-Use
Employees may not disclose to unauthorized persons or use for their own personal advantage or profit, or the advantage or profit of another, any confidential information that they obtain as a result of their position with the Bank. That includes not only financial analysts and the press, but also business associates, family members and personal friends. It is a serious mistake to disclose such information to anyone simply because you are confident that the person will neither try to benefit from it nor disclose it to others.

An employee's obligation not to disclose the Bank's confidential information and not to use it for unauthorized purposes continue after their affiliation with the Bank ends.

Privacy of Customer Information
The Bank is entrusted with important information about individuals and businesses. It is essential that employees respect the confidential nature of that information. The Bank is legally obliged to protect the privacy of a consumer's personal financial information. The Bank's privacy practices are set out in a privacy policy that is circulated to its customers and made available to the public. All employees are expected to adhere to the Bank's privacy policy.

Public Disclosures
Employees may be asked for information about the Bank by the media, trade groups, consultants and others collecting information for various purposes. Employees should not make public statements on behalf of the Bank or provide confidential information in response to external inquiries unless they have been specifically authorized to do so.

Proper Disclosures
Some employees must disclose confidential Bank information as a part of their job responsibilities. This policy on confidential information is not intended to prohibit such authorized disclosures.

A few examples of situations in which confidential information might properly be disclosed are:

- Disclosure of operational data to vendors or consultants in connection with providing services to the Bank;
- Participation in legitimate and authorized industry surveys;
- Providing data to governmental agencies as part of required filings; or
- An authorized employee responding to media or financial analyst inquiries.

Employees should be certain that they understand what they have been authorized to disclose, and to whom, prior to disclosing any confidential information.

“Inside” Information and Insider Trading
Employees must not trade in the Bank’s stock when they have material information about the Bank that is not yet public. Material information is information that would reasonably be expected to either: (1) affect the price of securities issued by the Bank; or (2) be important to an investor in deciding whether to buy, sell or hold securities issued by the Bank. Furthermore, employees must not communicate material non-public information to persons outside the Bank so that they may profit from transactions in the Bank’s securities.

Engaging in insider trading, or providing confidential information that is used in insider trading, is illegal and can result in substantial fines and criminal penalties to an employee.

The Bank maintains a policy on insider trading that provides more complete guidance on this subject, including rules on trading in Bank securities by executive officers, directors and employees who have access to certain financial information. Employees should contact the President and Chief Executive Officer with any questions about buying or selling Bank stock.

EXAMINATIONS, GOVERNMENT INVESTIGATIONS AND LITIGATION

Regulatory Examinations
The Bank and its subsidiaries are subject to examination by federal banking regulators. It is Bank policy to cooperate fully with the Bank's regulators.

Government Investigations
It is Bank policy to cooperate with reasonable and valid requests by federal, state or local government investigators. At the same time, the Bank is entitled to all the safeguards provided in the law for persons under investigation, including representation by counsel. Accordingly, if a government investigator requests an interview with you, seeks information or access to files, or poses written questions, he or she should be told that you must first consult with the Bank's legal counsel. You should immediately contact the President and Chief Executive Officer of the Bank who will then provide advice as to further action.

Penalties
Employees should be aware that criminal sanctions could be imposed upon any person who submits false or misleading information to the government in connection with any regulatory examination or government investigation. Full cooperation and proper legal supervision of any response in connection with a regulatory examination or government investigation is essential from both corporate and individual viewpoints.

Litigation
In the event any litigation is begun or threatened against the Bank, notify the President and Chief Executive Officer of the Bank immediately even if the action or threat appears to be without merit or insignificant.

Preservation of Records
All records relating to the business of the Bank shall be retained as required by the Bank's record retention guidelines. Notwithstanding such guidelines, under no circumstances shall any records known to be the subject of or germane to any anticipated, threatened or pending lawsuit, governmental or regulatory investigation, or bankruptcy proceeding be removed, concealed or destroyed.

DETAILED POLICIES AND PROCEDURES

This Code does not contain all of the policies of the Bank or all of the details of the policies that are described in this Code. The Bank has written policies and procedures that provide more detailed information on many of the topics addressed in this Code.

Employees should talk to their supervisor about the Bank's policies and procedures that they are responsible for following in their job and make sure that they have reviewed and understand them.

ADMINISTRATION OF THE CODE OF ETHICS AND BUSINESS CONDUCT

Every Employee Has an Obligation to:

- ***Comply*** with this Code of Ethics and Business Conduct, which prohibits violation of local, state, federal or foreign laws and regulations applicable to our businesses, and requires compliance with all Bank policies;

- ***Be familiar*** with laws and Bank policies applicable to his or her job and communicate them effectively to subordinates;

- ***Ask questions*** if a policy or the action to take in a specific situation is unclear;

- ***Be alert*** to indications and/or evidence of possible wrongdoing; and

- ***Report*** violations and suspected violations of this Code of Ethics and Business Conduct to the appropriate person as described in "How to Report a Violation" below, and elsewhere in this Code.

The Bank's managers have a particular responsibility to notice and question incidents, circumstances and behaviors that point to a reasonable possibility that a violation of this Code has occurred. A manager's failure to follow up on reasonable questions is itself a violation of Bank policy.

How to Ask a Question
Whenever possible, an employee should work with his or her immediate supervisor to get answers to routine questions.

If a supervisor's answer does not resolve a question, or if an employee has a question that he or she cannot comfortably address to his or her supervisor, he or she should go to the President and Chief Executive Officer of the Bank.

Executive officers and directors may bring any questions to the Chairman of the Board or the Chairman of the Audit Committee.

How to Report a Violation
Any employee having information about a violation (or suspected violation) of this Code should report the violation in writing to the President and Chief Executive Officer of the Bank. Executive officers and directors may submit any reports of violations (or suspected violations) of this Code in writing to the President and Chief Executive Officer of the Bank.

If the violation involves the President and Chief Executive Officer of the Bank, then the employee should report the violation by informing the Chairman of the Board or the Chairman of the Audit Committee.

Follow-up to the Report of a Violation
The President and Chief Executive Officer of the Bank may arrange a meeting with the employee to allow the employee to present a complete description of the situation. The President and Chief Executive Officer of the Bank will take the matter under consideration, including undertaking any necessary investigation or evaluation of the facts related to the situation and, after consultation with the appropriate individual, shall render a written decision, response or explanation as expeditiously as possible. Individuals who are alleged to be involved in a violation will not participate in its investigation.

Determining Whether a Violation Has Occurred
If the alleged violation of this Code concerns an executive officer or director, the determination of whether a violation has occurred shall be made by the Audit Committee of the Board of Directors, in consultation with the President and Chief Executive Officer of the Bank and/or such external legal counsel as the Audit Committee deems appropriate.

If the alleged violation concerns any other employee, the determination of whether a violation has occurred shall be made by the President and Chief Executive Officer of the Bank and/or such external legal counsel as the President and Chief Executive Officer deems appropriate.

In determining whether a violation of this Code has occurred, the committee or person making such determination may take into account the extent to which the violation was intentional, the materiality of the violation from the perspective of either the detriment to the Bank or the benefit to the director, executive officer or employee, the policy behind the provision violated and such other facts and circumstances as they shall deem advisable.

Acts or omissions determined to be violations of this Code by other than the Audit Committee under the process set forth above shall be promptly reported by the President and Chief Executive Officer of the Bank to the Audit Committee and by the Audit Committee to the Board.

Confidentiality
Reports of suspected violations will be kept confidential to the extent possible and consistent with the conduct of an appropriate investigation.

No Retaliation
Retaliation in any form against an employee who has, in good faith, reported a violation of this Code will not be tolerated.

Consequences of a Violation
Employees who violate this Code, or who fail to report violations of which they are aware or should be aware, will subject themselves to disciplinary action up to and including dismissal. Some violations may also result in civil liability and/or lead to criminal prosecution.

Prior Approvals
Whenever the requirement for prior approval appears in this Code, it means that a writing setting forth the pertinent facts of the situation under consideration shall be submitted according to the following process:

- If a request for prior approval relates to an executive officer or director, the determination with respect to the approval shall be made by the Audit Committee of the Board of Directors, in consultation with the President and Chief Executive Officer of the Bank and/or such external legal counsel as the Audit Committee deems appropriate.

- If a request for prior approval relates to any other employee, the determination shall be made by the President and Chief Executive Officer of the Bank, unless the matter is quantitatively or qualitatively material or outside the ordinary course of business, in which case such determination shall be made by the Audit Committee.

All approvals (other than those approved by the Audit Committee) shall be promptly reported to the Audit Committee.

Waivers
Employees must request a waiver of a provision of this Code if there is a reasonable likelihood that their contemplated action will violate this Code.

If a waiver request relates to an executive officer or director, the determination with respect to the waiver shall be made by the Audit Committee of the Board of Directors, in consultation with the President and Chief Executive Officer of the Bank and/or such external legal counsel as the Audit Committee deems appropriate. Any waivers granted by such committee shall be submitted to the Board for ratification.

If a waiver relates to any other employee, the determination shall be made by the Chief Executive Officer unless the matter is quantitatively or qualitatively material or outside the ordinary course of business; in which case the determination shall be made by the Audit Committee.

All waivers of the Code (other than those approved by the Audit Committee) shall be promptly reported to the Audit Committee.

Waivers will not be granted except under extraordinary or special circumstances.

Updates and Changes
This Code will be reissued periodically to remind employees, officers and directors of its specifics and to make changes and clarifications based on experience and suggestions.

CONTACTS

To Ask Questions and/or to Report Violations:

William W. Harrod, President and Chief Executive Officer

Key Contact

Carolyn Wallace, Chairwoman of the Audit Committee