United Security Bancshares

United Security Bank

Code of Business Conduct and Ethics

Letter from the Chief Executive Officer

Dear Fellow Employees:

We have prepared this Code of Business Conduct and Ethics (the "Code") to help you understand the standards of ethical business practice at United Security Bancshares and it subsidiary, United Security Bank (collectively referred to as the "Company"). This Code applies not only to all employees, officers and directors of the Company, but also to all consultants, agents and other representatives working for the Company, unless expressly excluded.

The principles set forth in this Code describe how we should behave. The Company will conduct its respective operations consistent with the highest business, legal and ethical considerations. Compliance with these principles is mandatory. Personal responsibility is at the core of our principles and culture. We expect everyone associated with the Company not only to know right from wrong, but also to always choose right over wrong. In every business decision we make, we must act and do business in strict compliance with the law and the principles set forth in this Code. It is also our responsibility to report anything we observe or know about that might violate the principles in this Code.

No Code can ever anticipate every ethical decision we may face in business. So whenever you are in doubt about any matter that may have ethical implications, you should seek guidance from the Company. This Code identifies the channels and procedures that we have established to help answer your questions.

Violation of this Code is a serious matter and could subject you and/or the Company to civil liability or even criminal prosecution. It is important that you read this Code carefully and ask questions about anything you do not understand. Each of us must understand and accept our personal responsibility in preserving and enhancing the Company's established reputation for integrity. I know you and our colleagues will take pride in always doing the right thing.

_____

Dennis Woods, Chief Executive Officer

ACKNOWLEDGEMENT
OF THE
CODE OF BUSINESS CONDUCT AND ETHICS

The undersigned having received a copy of the Company's Code of Business Conduct and Ethics ("Code") acknowledges that he or she has read it and understands the importance of good faith compliance with the Code. The undersigned agrees to fully comply with the Code and understands that the failure to comply with the Code may result in disciplinary action including termination of employment.

Dated:_____

_____
Signature

_____
Print your Name

Acknowledged By:

_____
Supervisor's Signature

POLICY STATEMENT

It is the policy of the Board of Directors of United Security Bancshares and United Security Bank (hereafter "Board") to conduct business in accordance with the highest ethical standards, in order to merit and maintain the complete confidence and trust of our customers, shareholders, staff members, and vendors. Staff members of United Security Bancshares ("Bancshares") and United Security Bank ("Bank")(both the Bancshares and Bank on a consolidated basis shall be referred to as the "Company") must conduct their personal affairs and manage their business transactions in a manner that does not result in adverse comments or criticism from the public, or in any way damage the Company's reputation as a responsible financial services organization. This policy addresses both business and social relationships, which may present legal and ethical concerns, and also sets forth a Code of Conduct to guide staff members. The term "staff members" refers to all officers and employees of the Company.

Compliance with Laws and Regulations

It is the policy of Bancshares and the Bank to fully comply with the spirit and intent of all applicable laws and regulations. We expect our staff members to comply with all applicable laws, rules and regulations in accomplishing their assigned duties, while using good judgment and ethical standards.

Administration of the Code of Conduct

It is the responsibility of each director and staff member to be familiar with the Company's *Code of Business Conduct and Ethics* (the "Code"). Supervising officers are expected to make every reasonable effort to ensure that their subordinate staffs continue to comply with the provisions of the Code.

On behalf of the Board of Directors of Bancshares and the Bank, the Audit Committee of Bancshares will periodically review the Code, advising the Boards in matters of administration and updates.

Senior management shall implement the Code, and determine matters of interpretation. Monitoring of adherence to the Code shall be accomplished by audit, examination, and human resource procedures.

Staff members are encouraged to seek the advice of the appropriate supervisor regarding questions of interpretation, and of the applicability of the provisions of the Code to a particular situation.

All staff and Directors shall sign a written acknowledgement of receipt of a copy of the Company's Code of Business Conduct and Ethics and any subsequent changes thereto.

Staff members who violate the provisions of the Code may be subject to dismissal may be subject to corrective action, including termination of employment. Staff members must promptly report any known or suspected violations of the Company's Code of Business Conduct and Ethics.

Waivers of the Code

IMPORTANT. In certain circumstances, it may be appropriate to grant a waiver of a provision of the Code, including waivers to the Bancshares' or Bank's Chief Executive Officer, Chief Financial Officer, other executive officers, or directors. **Any such waiver of the Code must be made in writing, and receive the prior consent of the *independent members* of the Board of Directors of United Security Bancshares. Any waiver must be promptly disclosed to shareholders via the Bank's website, filing of the appropriate form, or other expeditious and efficient method that is in accordance with legal and regulatory requirements.**

Enforcement Responsibilities and Procedures

The Board proactively promotes the highest level of ethical behavior and personal performance, including meeting the requirements of this Code. All staff members and directors should ensure prompt and consistent reporting of violations of the Code, as well as any actual or potential violation of applicable laws, regulations or Bank policies. Because it may be unclear whether a violation has occurred, staff members are encouraged to talk to managers about behavior that may violate the Code, and may raise any questions relating to the Code.

Complaint Procedure; Whistleblower; Communicating with Directors

The Sarbanes-Oxley Act, along with Nasdaq Rules, requires that the Bancshares' Audit Committees establish and maintain procedures to receive, retain and treat complaints received relating to accounting, internal control, or auditing matters.

This process is also called "Whistleblowing", and the bank's full policy is available as Corporate Procedure Manual (CPM) 1004 Whistleblower Complaint Policy".

For Whistleblowing purposes, a complaint is a serious concern that could have a large impact on the bank, such as actions that:

- May lead to incorrect financial reporting;
- Are unlawful;
- Are not in line with company policy, including the Code of Business Conduct; or
- Otherwise amount to serious improper conduct such as fraud against bank shareholders.

These procedures relate to employee concerns or complaints regarding questionable accounting or auditing matters, more specifically including, without limitation, the following:

(i) fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Company;

(ii) fraud or deliberate error in the recording and maintaining of financial records of the Company;

(iii) deficiencies in or noncompliance with the Company's internal accounting controls;

(iv) misrepresentation or false statement to or by a senior officer or accountant regarding a matter contained in the financial records, financial reports or audit reports of the Company;

(v) deviation from full and fair reporting of the Company's financial condition;

(vi) mail fraud, wire fraud, bank fraud, securities fraud, violation of any SEC rule or regulation or violation of any federal law relating to fraud against shareholders; and

(vii) Attorney Reports.

Moreover, these procedures must allow for confidential and anonymous submission of their concerns, by employees. Such procedures are currently in place and provided below. Our Board of Directors Audit Committee may be contacted by email, mail or Fax. A report form, with instructions for confidential delivery is available to all staff members on the bank's intranet portal.

Additionally, the bank utilizes an independent third party resource to accept whistleblowing complaints in an on-line portal, by phone, e-mail or fax 24 hours a day, 7 days a week, 365 days a year. These complaints may be made anonymously if desired, and will be routed to the Audit Committee Chairman for appropriate addressing and resolution..

Complaints lodged by the public about a bank product or service or similar complaints that are not related to financial reporting are to be made in accordance with General Compliance Policy (GCP) 1114 Complaint Policy.

Safeguards

Harassment or Victimization

Harassment or victimization of individuals submitting hotline reports will not be tolerated. In compliance with Section 806 of the Sarbanes-Oxley Act of 2002, the Company will not discharge, demote, suspend, threaten, harass or in any manner discriminate against any employee in the terms and conditions of his/her employment based upon any lawful actions of any such employee with respect to good faith reporting of a matter covered by these procedures. Contact the Audit Committee of Bancshares, in the same manner prescribed above, to report alleged retaliation.

Confidentiality

Every effort will be made to protect the reporter's identity by our hotline vendor. Please note

that the information provided in a hotline report may be the basis of an internal and/or external investigation by our company into the issue being reported. It is possible that as a result of the information provided in a report the reporter's identity may become known to us during the course of our investigation.

Anonymous Allegations
The policy allows employees to remain anonymous at their option. Concerns expressed anonymously will be investigated, but consideration will be given to:

- The seriousness of the issue raised;
- The credibility of the concern; and
- The likelihood of confirming the allegation from attributable sources.

Malicious Allegations
Malicious allegations may result in disciplinary action.

Procedure for Handling Complaints

Reporting
The whistleblowing procedure is intended to be used for serious and sensitive issues. Serious concerns relating to financial reporting, unethical or illegal conduct, should be reported in either of the following ways:

- **Website: www.lighthouse-services.com/unitedsecuritybank**
- **Toll-Free Telephone:**
  - **English speaking USA and Canada: 833-490-0007**
  - Spanish speaking USA and Canada: **800-216-1288**
  - Spanish speaking Mexico: **01-800-681-5340**
  - French speaking Canada: **855-725-0002**
  - Contact us if you need a toll-free # for North American callers speaking languages other than English, Spanish or French

- **E-mail:** reports@lighthouse-services.com (must include company name with report)

- **Fax:** (215) 689-3885 (must include company name with report)

Reporters to the hotline will have the ability to remain anonymous if they choose. Please note that the information provided by you may be the basis of an internal and/or external investigation into the issue you are reporting and your anonymity will be protected to the extent possible by law. However, your identity may become known during the course of the investigation because of the information you have provided. Reports are submitted by Lighthouse to United Security Bank or its designee, and may or may not be investigated at the sole discretion of our company.

Employment-related concerns should continue to be reported through your normal channels such as your supervisor, or Vice President Human Resources Officer (559-248-5089).

Timing
The earlier a concern is expressed, the easier it is for us to take action.

Evidence
Although you are not expected to prove the truth of an allegation, the employee submitting a report needs to demonstrate in their hotline report that there are sufficient grounds for concern.

HOW THE REPORT WILL BE HANDLED:

The action taken will depend on the nature of the concern. The Audit Committee of the United Security Bank Board of Directors receives a copy of each report and follow-up reports on actions taken by the company.

Initial Inquiries
Initial inquiries will be made to determine whether an investigation is appropriate, and the form that it should take. Some concerns may be resolved by agreed upon action without the need for an investigation.

Feedback to Reporter
Whether reported directly to United Security Bank personnel or through the hotline, the individual submitting a report will be given the opportunity to receive follow-up on their concern:

* Acknowledging that the concern was received;
* Indicating how the matter will be dealt with;
* Giving an estimate of the time that it will take for a final response;
* Telling them whether initial inquiries have been made;
* Telling them whether further investigations will follow, and if not, why not.

Further Information
The amount of contact between the individual submitting a report and the body investigating the concern will depend on the nature of the issue, the clarity of information provided, and whether the employee remains accessible for follow-up. Further information may be sought from the reporter.

Outcome of an Investigation
At the discretion of the company and subject to legal and other constraints the reporter may be entitled to receive information about the outcome of an investigation. Copies of all complaints

and investigation records will be maintained in accordance with the Company's document retention policy.

United Security Bank reserves the right to modify or amend this policy at any time as it may deem necessary.

CONFLICTS OF INTEREST

Policy

A conflict of interest is defined as a staff member's involvement in outside interests that might either conflict with the staff member's duty to the Company or adversely affects the staff member's judgment in the performance of their responsibilities.

It is the Company's policy that staff members do not engage in personal conduct that will conflict with the interests of the Company. All staff members are required to disclose any potential conflict of interest, including one in which they have been inadvertently placed as a result of a business or personal relationship with a Company customer, supplier, business associate or competitor.

Disclosure of potential conflicts of interest should be made, in writing, with a full account of the circumstances, to the staff member's supervisor who will review the situation and instruct the staff member as to the appropriate action. Contemporaneous written records of all such disclosures are retained.

Bank Bribery Act

Federal banking law generally prohibits any employee, officer, director, agent or attorney of United Security Bank (hereinafter "bank official(s)") 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.

Acceptance of Gifts

Staff members and their immediate families shall not solicit, accept or retain a benefit for themselves or for any third party from any customer of the Company, any individual or organization doing or seeking to do business with the Company, or from any other individual or organization based on a banking relationship other than normal authorized compensation, with the intent to be influenced or rewarded in connection with any business or transaction of the Company. In this context, a benefit is regarded as any type of gift, gratuity, favor, service, loan, legacy (except from a relative), fee or compensation, or anything of monetary value.

Specific exceptions to this prohibition are made if there is, and appears to be, no reasonable likelihood of improper influence in the staff member's performance of duties on behalf of the Company. The personal benefit, however, must be one of the following:

- Normal business courtesies, such as a meal, refreshment or other reasonably valued entertainment involving ordinary amenities, in the course of a meeting or other occasion, the purpose of which is to hold bona fide business discussions.

- Non-cash gifts of reasonable value (under $100) such as received at holiday time or special occasions, such as a new job, promotion, wedding, or retirement, representing an expression of friendship.

- Gifts based upon obvious family or personal relationships, when the circumstances make it clear that it is those relationships, rather than the business of the Company, which are the motivating factors.

- Unsolicited advertising and promotional material of nominal value, such as pens, pencils, note pads, and key chains.

- Awards given by charitable, educational, civic, or religious organizations for meritorious contributions or service.

- Loans from other banks or financial institutions on customary terms to finance proper and usual activities, such as home mortgage loans, except where prohibited by law.

- Discounts or rebates on merchandise or services that do not exceed those available to other customers.

Any personal benefit(s) received, other than the exceptions noted above, is to be reported by the staff member to their supervisor, in writing, with a full account of the circumstances. The supervisor will review the situation with the Risk Manager/BSA Officer and instruct the staff member as to the appropriate action. The Company retains contemporaneous written records of all such disclosures.

Cash gifts (which include gift cards) in any dollar amount may not be accepted by an employee. It is important to recognize that federal law makes it a crime for any officer, director or employee of a federally insured bank or bank holding company, directly or indirectly, to ask, solicit, accept, receive or agree to receive anything of value, for himself or for any other person or entity, for or in connection with any transaction or business of the Company, including making loans. The penalty for violating this law is a fine, imprisonment, or both. Any offer of such an improper payment should be immediately reported to the staff member's supervisor.

Giving Gifts

Any business gift given (where appropriate and legal) must not exceed in the aggregate $100 in value per calendar year unless prior of the Company's CFO approval is received. Sales or marketing representatives may make business gifts of their regular Company products or promotional items valued under $25 for the purpose of generating business goodwill. Moreover.

Political Contributions

It is the policy of the Company to strictly comply with all applicable federal and state political campaign laws.

The Company is prohibited from making any contribution or expenditure in connection with any federal election or campaign. The approval by legal counsel for the Company and the Board is required for other political contributions.

In accordance with federal law, no staff member shall make any direct or indirect contribution of funds or other property of the Company in connection with the election of a candidate to any federal office. For these purposes, use of the corporate facilities and equipment for political activities is deemed to be a contribution. Loans to a candidate for political office or to a political committee are not prohibited so long as the loan is made in the ordinary course of business and meets the Bank's usual credit criteria and approval procedures for the particular type of loan.

The Bank's policy regarding corporate political contributions is not intended to discourage staff members from making personal contributions to candidates or political parties of their choice.

Outside Activities

The Bank discourages staff members from holding outside employment. In those instances where it is justified, written approval from the Personnel Department is required. No outside employment or activity will be approved which might subject the Company to criticism or which will encroach upon regular working hours, interfere with regular duties, or necessitate such long hours that the staff member's productivity is affected.

Staff members are not to act, without prior written approval of management, as executor, administrator, trustee, guardian or conservator, or in any other fiduciary capacity, whether or not it is related to the business of the Company. Approval, except in unusual cases, will normally be granted to act as fiduciary for a family member.

Soliciting others. Staff members may not contact other Company employees during work hours or on firm premises to solicit political contributions or volunteer political activity (including "grassroots" activity such as encouraging others to contact elected representatives regarding specific legislation). Staff members may not use firm resources (stationery, e-mail or phones, facilities, client or employees lists, etc.) to contact anyone, including employees, customers and vendors, for these purposes at any time.

Personal Finances

Personal finances should be managed in a manner consistent with employment in a financial institution. Staff members and their immediate families should borrow only from reputable organizations that regularly lend money, and such borrowings must carry the prevailing rate of interest and not involve favored treatment of any kind. Staff members may not borrow money (other than nominal amounts) from or lend money to other employees, customers or suppliers, or act as a guarantor, co-signer, or surety or in any other similar capacity for customers, suppliers, or other employees, except in the limited case set forth in the next paragraph.

In general, staff members may not participate in any other personal financial transactions with fellow employees, customers, or suppliers. This prohibition includes shared investments (unless they are either widely held or held pursuant to firm sponsored co-investment plans) and investment clubs. The foregoing limitations do not apply to: (a) borrowing from, or acting as guarantor, co-signer, or surety for, relatives or close personal friends (generally, friendships formed outside the context of any Company business relationship), (b) borrowing on non-preferential terms from a customer that is in the financial services business. (c) making consumer credit purchases on non-preferential terms from a customer or supplier in the normal course of that customer/supplier's business.

Except as approved by the Board with the nondisapproval of legal counsel, staff members are not permitted to purchase "Real Estate Owned" or REO properties owned by the Company, or by a third party lender where the loan was serviced by the Bank, as a result of mortgage foreclosure proceedings or deeds in lieu of foreclosure.

Staff members should not sign on customers' accounts, act as deputy or co-renter of customers' safe deposit boxes, or otherwise represent customers. This does not include customers related to the staff member by blood or marriage.

Personal Investment Activity

While the Company does not intend to unreasonably limit staff members in their personal investment activities, it is the Company's policy that no staff member enter into investment transactions which would create, or give the appearance of creating, a conflict of interest between the staff member and the Company, or between the Company and any customer.

Lending Practices

(1) It is the policy of the Bank to maintain prudent lending services to adequately supply the credit needs of its customers. Any rate concessions shall be based solely upon a borrower's creditworthiness and overall business relationship with the Bank and in accordance with the Bank's lending policy.

(2) Staff members are not in any way to represent or exercise authority on behalf of the Company, grant direct or indirect accommodations or make credit recommendations with respect to: members of their families; any individual or organization to which the staff member or his or her immediate family is indebted; or any organization to which the staff

member, or his or her immediate family, is associated or in which a material financial interest is held.

(3) Federal law prohibits any director, officer or employee of the Company from granting any loan or gratuity to any public bank examiner or assistant bank examiner, who examines the Bank or has authority to examine the Bank.

Advice to Customers

Staff members may occasionally be asked by customers to comment upon the legality of a particular transaction. Since the Company cannot practice law or give legal or tax advice, staff members must exercise care in discussing transactions with customers, and nothing should be said that might be interpreted as the giving of legal or tax advice.

Corporate Opportunities

Employees, officers and directors owe a duty to the Company to advance its legitimate interest when the opportunity to do so arises. Employees, officers and directors are prohibited from:

- Taking for themselves personal opportunities that are discovered through the use of corporate property, information or position;
- Using corporate property, information or position for personal gain; and
- Competing with the Company, without the prior consent of the Board of Directors.

Use of Company Resources

General

Telephones, electronic mail (e-mail) systems and other electronic communications devices provided by the Company, whether in the workplace or elsewhere, are the property of the firm and should be used for business purposes; however, reasonable personal use is permitted, consistent with this Code and all other policies of the Company. You are expected to use common sense and good judgment in determining what is and what is not "reasonable personal use". The use of e-mail, the firm's intranet and the internet must conform to the policies of the Company. E-mail and internet systems may be used to transmit or provide access to confidential information only when such information is adequately protected and transmitting such information is necessary for business purposes.

Among other things, the following are prohibited in electronic communications: (a) statements, which, if made in any other forum, would violate any of our policies, including policies against discrimination and harassment; participation in impermissible or illegal activities (such as gambling or the use and sale of controlled substances); and the misuse of confidential

information. (b) accessing, downloading, uploading, saving, or sending sexually oriented or other offensive materials.

The Company considers all data and communications transmitted through, received by, or contained in the firm's electronic or telephonic equipment and systems to be the Company's property. Subject to applicable laws and regulations, the Company reserves the right to monitor, review, and disclose all such data and communications as it deems appropriate. You should have no expectation of privacy when using such resource.

Staff members should keep in mind the provisions of the Code as to what a staff member can say or post on the internet about the Company and information derived from the Company (including networking sites like Facebook, Twitter and LinkedIn). You should be familiar with these rules if you engage in internet communications from the office, home or elsewhere.

E-mail and Internet

E-mail systems are not entirely secure and may be susceptible to interception. Unlike a spoken conversation, e-mail creates a permanent record. Any e-mail you send may be printed by the recipient and forwarded by the recipient to others, and is probably retained on company computers for a substantial period of time. Therefore, Company's employees should exercise the same care, caution and etiquette in sending an e-mail message as they would in normal written business communications.

Make sure your Company e-mail is professional and appropriate to the circumstances. Specifically, the Company will not tolerate abusive, obscene, offensive or profane e-mail. In addition, because the e-mail system is a Company resource, the Company reserves the right to read all e-mail communications.

Anyone who has been provided a connection to the Internet is provided such connection primarily for business use. Employees are allowed limited personal use of Company communications systems, so long as it does not interfere with work responsibilities or result in inappropriate costs or violate the law or this Code. In connection with such limited personal use, employees shall not visit any Web site or download any data from any site that is not in the public domain or that is unprofessional, obscene, inflammatory or inappropriate for business use as determined in the sole discretion of the Company. The Company may maintain logs and records as to an employee's personal use of communications systems for evidence of abuse of Company-provided systems. Violation of the Code regarding an employee's personal use of communications systems will result in disciplinary action including termination of employment.

Software

Copyrights protect most computer programs. Our policy is to respect such copyrights and to strictly adhere to all relevant laws and regulations regarding the use and copying of computer software. Therefore, do not make copies of any part of a third-party computer program unless the copy is an authorized back-up copy or the computer software license specifically permits the copy to be made. If you are uncertain about this, you may consult with the Company's legal

counsel. If you are engaged in writing computer programs, do not copy or refer to any lines of code written by a third party without the advice of the Company's legal counsel or the written consent of the third party.

CONFIDENTIALITY

Customer Information

Safeguarding the confidential financial information concerning the Bank's customers is essential in maintaining the public trust. It is the policy of the Company that such confidential information acquired by a staff member through his or her employment must be held in the strictest confidence. Such information is to be held for Bank purposes and not as a basis for personal gain by any staff member. Aside from routine credit inquiries, information regarding a customer may generally only be released to private persons, organizations or governmental bodies that request it with the consent of the customer involved or upon receipt of legal process, such as a subpoena or court order.

Confidential customer information should never be discussed with anyone outside the Company, and only with those within the Company who have a legitimate business need to know. Confidential customer information should never be discussed in public places, even within the Company's offices. Staff members should be sensitive to the risk of inadvertent disclosure resulting from open doors, speakerphones, cellular phones, and when transmitting confidential information by fax or other electronic media.

Information Regarding the Bank

Financial or other information regarding the Company is not to be released to any outside person or organization unless it has been published in reports to shareholders, or otherwise made available to the public through authorized news releases. All news media inquiries must be referred to the President and CEO. The Company expects every employee to treat information concerning the Company and its personnel with the same confidentiality as information concerning customers of the Bank and to observe, with respect to the Company, the same guidelines set forth under the Caption, "Customer Information".

Material Inside Information

The disclosure of "material inside information" subjects staff members, the Company and third parties to whom the information is communicated to severe penalties under federal and state securities laws. Information is "material" when there is a significant likelihood possessing such material inside information must not trade in or recommend the purchase or sale of the securities involved until the information is actually disseminated to the public. See INSIDER TRADING below.

Lending personnel must not disclose confidential information on existing or proposed loan customers to outside persons or organizations.

INSIDER TRANSACTIONS

Loans and Extensions of Credit

All loans and extensions of credit made to or for the benefit of directors, executive officers and principal shareholders of the Company and their related interests shall comply with Regulation O (12 CFR §215 Part A and §337.3).

All loans and extensions of credit by the United Security Bank in excess of $100,000 made to other officers, employees, agents, consultants, and representatives of the Company shall comply with all applicable laws and shall be approved by the loan committee of the board of directors of United Security Bank.

Deposits and Bank Charges

All deposits made by any director, executive officer or employee of the Company and their related interests (as defined in Regulation O) with United Security Bank shall be on the same terms and conditions as if the deposit were made in an arm's length transaction by a third party customer of United Security Bank. All banking fees and charges for bank products and services provided to any director, executive officer or employee of the Company and their related interests (as defined in Regulation O) with United Security Bank shall be on the same terms and conditions as if the banking product or service were provided in an arm's length transaction to a third party customer of United Security Bank, except that the basic normal monthly banking charges for a standard checking account may be waived.

Other Investments and Investment Accounts

Investment transactions by and for the account of any director, executive officer or employee of the Company and their related interests shall be priced and charged the same fees, commissions, discounts, and on the same terms and conditions as if the investment were made in an arm's length transaction by a third party customer of United Security Bank.

INSIDER TRADING

Employees and directors of the Company are frequently entrusted with possession of confidential and highly sensitive information concerning the Company, its clients or other businesses with which the Company has material contractual relationships or with which the Company may be in the process of negotiating material transactions ("Confidential Parties"). As long as an employee or director of the Company is aware of material non-public information relating to the Company,

any of its clients or any Confidential Party, it is the Company's policy that such employee or director may not buy or sell the securities of the Bank, the client or the Confidential Party, as applicable, regardless of how that information was obtained.

Equally important, the employee or director must maintain such information in the strictest confidences.

An employee or director of the Company must also not permit any member of his or her immediate family or anyone acting on his or her behalf, or anyone to whom he or she has disclosed such information, to purchase or sell such securities.

After the information has been publicly disclosed through appropriate channels, employees and directors of the Company should nevertheless allow a reasonable time to elapse (usually three business days) before trading in the security, to allow for broad public dissemination and evaluation of the information.

In view of the foregoing, it is the policy of the Company that employees and directors of the Company must not purchase or sell securities of the Company, any client of the Company or any Confidential Party, if the employee or director has, or believes he or she may have, material non-public information relating to the Company, such client or such Confidential Party, as applicable. All inquiries in this regard, including, without limitation, inquiries as to whether information is material non-public information or whether a company or person is a client of the Company or a Confidential Party, should be directed to the Chief Financial Officer.

PRIVACY

In order to assure access at all times to Company property, and because employees may not always be available to produce various documents, records, files or other items in their possession in the ordinary course of business, the Company reserves the right to conduct a routine inspection or search of the Company's premises at any time, without the consent of the employee.

The Company's premises include all locations owned or leased by the Company or under the control of the Company, including office space, parking lots, closets, storage areas and lockers. Company property includes all tangible and intangible personal property of the Company, including, without limitation, all furniture, equipment, file cabinets, computer hardware and software, licenses and copyrights. The foregoing includes all communications and transmissions of any kind, including all information stored on any hardware, software, electronic disk, voice mail, e-mail and all other electronic communication media.

Routine searches and inspections may include an employee's office, desk, file cabinets, closet, locker, computer files, whether contained on a hard drive or floppy disk, including past and present e-mail communications, and similar places where Company property may be located, whether or not such places are locked.

All system pass codes must be available to the Company at all times. Employees may not use pass codes that are unknown to the Company. Employees are prohibited from the using the code of another employee to gain access to that individual's e-mail, voice mail or computer system.

Employees are prohibited from using the Company's information systems in any way that might be considered disruptive or offensive to others, including customers and vendors. Personal or inappropriate use of the Company's information systems may result in disciplinary action, up to and including termination. Inappropriate transmission includes, but is not limited to, sexually explicit messages, offensive language and ethnic, racial and gender-specific slurs.

ACCURACY OF RECORDS

We rely on our employees to maintain accurate books and records to efficiently manage our business. As in all other aspects of our business, we expect our employees to adhere to the highest standards of honesty. We do not engage in inaccurate, false or misleading record keeping. If you are ever tempted or asked to make a representation, either in a document or in oral communication, that is other than fully accurate, do not do it. This applies to each and every detail of our business. It applies even in circumstances where one might believe that the consequences of the inaccuracy would be harmless.

The Company's funds or assets will be utilized solely for a lawful and proper purpose and no transfer or expenditure of such funds or assets will be undertaken unless the stated purpose is, in fact, the actual purpose, and the transfer or expenditure is authorized in writing and within the Company's policy. No undisclosed or unrecorded fund (e.g. slush fund) or asset of the Company shall be established for any purpose.

No false or artificial entries shall be made in the books and records of the Company or any of its subsidiaries for any reason, and no employee shall engage in any arrangement that results in such a prohibited act.

It is also the Company's policy that no employee shall take or approve actions that result in incurring, or paying, the cost of anything from corporate funds if such an expenditure, when properly and accurately reported, is not authorized or not reimbursable to the employee under the Company's rules.

Questions regarding this policy should be addressed to the Company's Chief Financial Officer.

CONSULTANTS

Consulting agreements shall be controlled to protect the Company's confidential information. No consultant may be retained to perform work for the Company without a formal written agreement prepared by the Company's legal counsel. These agreements must contain a detailed statement of work, a clear description of all amounts to be paid, and all specific provisions required by the legal counsel covering conflicts of interest, standards of conduct, government

business ethics, confidentiality obligations, ownership of intellectual property and special provisions in foreign agency agreements.

Unless specifically approved by the Company's legal counsel, all payment for services or products must be paid in the name of the consultant, agent or representative named as a party on the agreement and paid in the location where the services are performed. All consultants must be informed about and agree to follow the Company's Code of Business Conduct and Ethics with respect to activities that affect the Company's businesses.

DRUG & ALCOHOL POLICY AND EMPLOYEE ASSISTANCE

To remain competitive, it is essential that we make the sound decisions. We expect that all our employees' judgments will be clear and unimpaired by drugs or alcohol.

Specific Guidelines

(1) Employees shall not distribute, possess or use illegal or unauthorized drugs or alcohol on the Company's property, on the Company's time, in connection with business or in a manner that may affect performance of employee's responsibilities and duties to the Company.

(2) Employees whose behavior, judgment or performance is impaired by drugs or alcohol should not go to or return to work and will be prohibited from entering the Company's premises or engaging in Company business. Violations of this policy are serious and will result in appropriate discipline, including termination.

EMPLOYMENT AND MEDICAL RECORDS

Employment records of Company employees can only be disclosed to those Company employees having a substantial and legitimate need to know the information in an employee's file or in response to appropriate legal process as required under the **Health Insurance Portability and Accountability Act (HIPAA) of 1996**. Company employees with access to these files have the responsibility and duty to keep them confidential as breaches of confidentiality will subject the Company to penalties and fines under HIPAA.

The Company's employees' medical records are confidential and private. These medical records are kept separate from all other employee records and will not be released to any person unless required by law or based upon a written release from the employee concerned.

EMPLOYMENT OF CLOSELY RELATED PERSONS

The Company wants to make sure that our workplace is fair and untainted by any possible perception of favoritism. We encourage the tradition of family service but have certain rules

about employing closely related persons. Our policy is not to employ persons closely related to a Company officer without required approvals.

Other closely related persons cannot be employed in jobs where one Company employee has effective control over any aspect of the related Company employee's job. Related Company employees may not share responsibility for control or audit of significant Company assets.

RELATIONSHIPS WITH DEPARTING AND FORMER EMPLOYEES

Your obligation to abide by certain company standards exists even after your employment ends. For example, absent vice president level or above approval, you may not accept a job with another company if your new duties would cause you to:

- Breach any employment condition or agreement you have with the Company; or
- Use or disclose Company nonpublic information in the new position.

In addition, when leaving or retiring from the company you must ensure that you return all Company property in your possession, including all records and equipment. You may not provide any Company nonpublic company information to former employees. If a former employee solicits this information from you, you must notify the Company's Chief Executive Officer or the Company's legal counsel.

You may not purchase products or services on the Company's behalf from former employees without prior Board approval unless they have been separated from the Company for more than a year.. Certain former employees may have information from which they can still unfairly benefit even after a year. If you suspect this is the case, you should consult with Company's Chief Executive Officer for appropriate action.

Employees of the Company should be careful in speaking with former employees of the Company and not disclose confidential information about the Company, even if it is something that the former employee may already know. A casual conversation with a former employee could result in the unintentional leak of a material secret of the Company.

ENVIRONMENT, SAFETY AND HEALTH

The Company is committed to maintaining a leadership role in protecting human health and the environment. We will promote and protect the health and safety of our employees, the environment and the communities in which we operate. Therefore, we will strictly adhere to all applicable laws and regulations relating to environmental protection and workplace health and safety.

Many environmental, safety and health laws and regulations are complex. If your work involves these fields, it is your responsibility to familiarize yourself with the requirements of relevant laws and regulations, including record keeping.

EQUAL OPPORTUNITY

It is the Company's policy to ensure equal employment and advancement opportunity for all qualified individuals without distinction or discrimination because of age, color, national origin, race, religion, sex, physical or mental disability or veteran status.

This policy applies to all employees and applicants for employment and to all aspects of the employment relationship, including recruitment, hiring, compensation, benefits, training, transfer, and any other terms and conditions of employment. Equal employment opportunity principles must be communicated periodically to all employees and reaffirmed each year.

The Company's Chief Operations Officer is responsible for implementing our equal opportunity policy. The Human Resources senior officer is the one to whom you can address any concerns regarding any potential violations of this policy.

FRAUDS AND THEFTS

It is the Company's policy to ensure that incidents of fraud and theft relating to the Company are promptly investigated, reported and, where appropriate, prosecuted.

Any suspected incident should be immediately reported to the Chief Executive Officer of the Company or the Company's Audit Committee Chairman. The Committee will review the incident and advise regarding prosecution, if appropriate. No one may sign a criminal complaint on behalf of the Company or complete a criminal or other investigative report without prior written approval of the Company's Chief Financial Officer or Company's Audit Committee Chairman. These two positions have jurisdiction over related personnel actions and civil litigation. To report an incident, please contact the Director of Human Resources or the legal counsel.

REGULATORY EXAMINATIONS AND INVESTIGATIONS

It is our policy to fully cooperate with any appropriate government investigation. If you or someone you supervise learns about a possible government investigation or inquiry other than a regularly scheduled bank or securities regulatory examination, inform the Company's Chief Executive Officer or legal counsel immediately.

Specific Guidelines

(1) Never destroy any Company documents in anticipation of a request for those documents from the Company or any of the Company's investigators, any government, bank or securities regulatory agency, opposing party in a legal matter or a court. Documents include electronic media such as disks, computer-stored information and e-mail transmissions.

(2) Never alter any historical Company document or record. Any corrections or amendments to a Company historical document or record should be set forth in a separate document that also refers to the original historical document so that an audit trail is maintained.

(3) Never make any untrue or misleading statement to any government, bank or securities regulatory investigator.

(4) Never try to influence any other Company employee or any other person to provide untruthful information to any Company investigator, government or bank or securities regulatory investigator, or to provide any incomplete, false or misleading information.

(5) If any government, bank or securities regulatory agency inquiry arises through a written subpoena or a written request for information (such as a Civil Investigative Demand), you must submit the subpoena or written request to the Company's legal counsel immediately, before any action is taken or promised.

(6) If you are approached outside the workplace by a government investigator or bank or securities regulatory investigator, you have the right, if you wish, to consult with the Company's legal counsel (or, if you prefer, your own private legal counsel) before speaking with the investigator.

PUBLIC STATEMENTS

Generally, employees must refrain from making public statements regarding issues or matters about which they are not authorized spokespersons. If an employee is contacted by the media about a Company matter, the employee should refer the media contact to the Chief Executive Officer of the Company.

SEXUAL HARASSMENT

The Company will not tolerate sexual harassment, which involves the solicitation of sexual favors or the initiation of any unwelcome sexual advance by one employee toward another. It may also involve other sexually related physical or verbal conduct. The creation of a work environment that is hostile, intimidating or offensive to an individual or group because of gender may also constitute sexual harassment.

Men and women throughout the Company should treat one another with courtesy, dignity and respect, regardless of gender. All employees should recognize that there has been rapid social

change as to appropriate conduct in the workplace, and workplace behavior should always reflect our principles of **courtesy**, **dignity** and **respect**.

The Company's officers, managers, supervisors and executives must be alert to the possible presence of sexual harassment in the workplace. Appropriate steps must be taken to prevent sexual harassment. Complaints about sexual harassment can be made to your supervisor, the Human Resources Department or the Chairman of the Audit Committee. Any complaints must be promptly, fairly and thoroughly investigated. There will be no retaliation for truthfully reporting sexual harassment or participating in the Company's investigation of a complaint.

If sexual harassment occurs, there will be a prompt disciplinary consequence ranging from a warning to dismissal.

WORKPLACE VIOLENCE

Employees should have a safe place in which to work. Workplace violence, including threats, threatening behavior, harassment, intimidation, assaults and similar conduct, will not be tolerated. Any threats or concerns about your safety or the safety of others should be immediately reported to your manager. Firearms are not permitted on any Company facility without prior written approval from the Company's Chief Executive Officer and the Company's legal counsel.