CODE of Ethics and Business Conduct

1ST SECURITY BANK

FS BANCORP, INC.

Our Values

Vision
Build a truly great place to work and bank.

Mission
Live our core values and "wow" each other and our customers every day.

Philosophy
Inspired by Geoffrey James

Business is an ecosystem, not a battlefield.
Average companies build armies of "troops" to order about, see competitors as "enemies," and treat customers as territory to be conquered.

We are a relationship driven company that values teamwork, adapts easily to new markets and can quickly form partnerships with each other, customers and even competitors.

A company is a community, not a machine.
Average companies do not see their employees as people. They create "my way or the highway" environments that are rigid and fear driven.

We see team members as a collection of individual hopes and dreams, all connected to a common purpose. We encourage and inspire employees to celebrate individual, team, company and community success.

Leadership is service, not control.
Average companies want employees to do exactly what they are told. They create condescending "Command and Control" environments where personal initiative is unacceptable.

We value leaders who encourage collaboration, diversity of ideas and provide the proper resources to empower their teams to get the job done. We also value humble and patient leaders over arrogant and ill-tempered ones.

We consider each other as peers regardless of job title.
Average companies treat some employees as inferior to others based on organizational charts.

We treat every employee as if they were the most important person at the bank. Excellence is expected everywhere, ideas and suggestions from all are encouraged and "the best idea wins". As a result, employees at all levels take charge of their own destinies.

Motivation comes from vision, not from fear.
Average companies use fear as power to motivate. Employees and managers alike become paralyzed, stagnant and unable to be forward thinking and take risks.

We inspire people to see a better future and how they will be part of it. As a result, employees work harder because they believe in our goals, truly enjoy what they are doing and know they'll share in the rewards.

Change equals growth, not pain.
Average companies see change as both complicated and threatening. They delay necessary changes until they are in a desperate situation and it's too late.

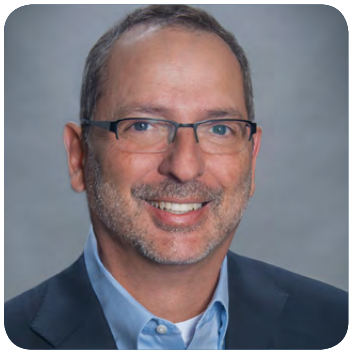
We embrace change and see it as an inevitable part of life. We are aware that change is not always easy but we understand that success is only possible if we all embrace new ideas. It is important for us to work constructively and support each other during change.

Core Values are embraced, they are not just words on a piece of paper.
Average companies talk about the importance of core values, however, management teams at average companies rarely live by them. This leads to the core values becoming a joke for employees.

Our Core Values were developed with input from the Employee Satisfaction Task Force and we expect that every person in every position actively supports them. Our Core Values encourage us to act in a manner that "wows" others and provide us with the opportunity to guide our actions which allow us to become who we want to be. We take pride in our Core Values and strive to live them each day.

Work should be fun, not mere toil.
Average companies believe people only work for a paycheck and discourage camaraderie, job satisfaction and happiness. They fully expect employees to resent having to work, therefore everyone behaves accordingly.

We see work as something that should be enjoyable. We encourage our employees to be happy by embracing their dreams, connecting with teammates and celebrating our successes. It's more than a paycheck; we want our teammates in jobs that can and will make them truly happy.



HONESTY · INTEGRITY · RESPONSIBILITY

A Message from Joe Adams

Our success has been based on hard work and an unwavering commitment to honesty and integrity in everything we do. Today's business environment is complex and much has changed in recent years, but one thing that has never changed is our belief that maintaining our good reputation depends on each of us being personally responsible for our conduct.

An important step in meeting our day-to-day ethics and compliance responsibilities is to be mindful of our commitments to each other, to our customers, our business partners, and to the communities where we work and live. This Code of Ethics and Business Conduct provides information about our personal responsibilities, including complying with the law and applying our good judgment each and every day.

Of course this Code cannot answer all of your questions or address every situation; which is why we have established resources to answer questions and follow-up when problems occur. If you are unsure of what to do in particular circumstances or concerned that the Code, our policies or regulations are being broken, you have a responsibility to speak up. A problem cannot be resolved unless it has first been identified. It's quite simple: if you have a question, or believe there may be a violation, speak up.

I believe the quality of our people, and our commitment to ethics and compliance will not only enable us to succeed today, but will help us to achieve long term success. I am convinced that working together, with the help of this Code, we will not only meet our goals, but we will also continue to be proud of how we achieve success.

Thank you.

Sincerely,

Joe Adams

Joe Adams

CEO, FS Bancorp, Inc. and 1st Security Bank of Washington

Core Values

Relationship Driven – we strive to "wow" (surprise, excite and delight) each other and our customers

Ethical – fair, honest, act with integrity

Lead by Example – maintain a positive attitude, show respect for others, have some fun

Accountable – we take our responsibilities seriously and we meet our commitments with urgency

Team Player – dependable, enthusiastic contributor to team success and to greater good of the Bank

Embrace Dreams – we encourage each other to reach for our dreams

Diversity – we celebrate diversity and support equality for all

Community Oriented – we actively support our communities and the Bank's CRA initiatives

Open and Honest Communication – always professional, responsive and timely

Table of **Contents**

Our Values ..... Inside Front Cover

A Message from Joe Adams 1

Our Commitment to Ethics and Compliance 4

How to Use this Code 4
To Whom this Code Applies 4
Asking Questions – Using the Integrity Line 5
What to expect when you use the Integrity Line 5
Our Non-Retaliation Policy 6
Employee Responsibilities 6
Additional Responsibilities of 1st Security Bank's Leadership 7
Cooperating with Investigations 8
1st Security Bank Integrity Test 9
Accountability and Discipline 9
Waivers and Exceptions 9

Respect and Integrity in the Workplace 10

Diversity and Non-Discrimination 10
Harassment-Free Workplace 11
Employee Privacy 12
Safe and Healthy Work Environment 13
Alcohol and Drug Use Policy 14
Preventing Workplace Violence 14

Maintaining Appropriate Business Relations 15

Conflicts of Interest 15
Corporate Opportunities 16
Friends and Relatives 16
Outside Employment 16
Personal Investments 16
Civic Activities 16
Gifts and Entertainment 17
Gifts and Entertainment of Government Representatives 18

Working with Our Customers and Vendors 19

Honest and Ethical Dealings 19
Marketing and Advertising Standards 19
Protecting the Privacy and Confidential Information of Others 20
Competitive Intelligence 20

Protecting Our Information and Assets 22

Protecting 1st Security Bank Assets 22
Confidential Information 23
Intellectual Property 24
Communicating with the Public 24
Using Social Media 24

Following the Letter and Spirit of the Law 26

Insider Trading 26
Anti-corruption and Bribery 27
Anti-money laundering 28

Our Commitment to ETHICS AND COMPLIANCE

Our Commitment to **Ethics and Compliance**

Protecting 1st Security Bank's reputation is the responsibility of every employee. We must always act with integrity; when we do, others will know they can trust us and have confidence that we will be honest and fair. We want to be known as a company that always honors its commitments and is a reliable business partner. When we do the right thing, we protect our reputation and that will help us to succeed even in today's complex and competitive business environment.

This Code is designed to help when you have questions about what to do in specific situations. It is a summary of how we will do business in accordance with our values, policies, and various laws and regulations.

How to Use This Code

The Code is designed to serve as a resource when you need information about our policies or standards or when you are faced with a difficult ethical situation.

It's impossible to anticipate every question you may have or situation you might face, so in addition to the Code, 1st Security Bank also has other resources that can be of help. These additional resources are listed throughout the Code. As always, the Company relies on you to use good judgment and to seek help when you need it.

To Whom This Code Applies

This Code applies to all employees, officers and directors at any 1st Security Bank branch/department and FS Bancorp, Inc.

Asking Questions – Using the Integrity Line

If you see or suspect any violation of the "Code", including actions or failure to act, illegal or unethical behavior, or you have a question about what to do, talk to your supervisor and ask for help.

Sometimes, you may not be able to talk about an issue with your manager. If that's the case, you have several options. You may contact the Compliance Officer, Enterprise Risk Manager or Human Resource Manager.

In addition any concerns regarding questionable accounting, internal control or auditing matters may be directed to the Chairperson of the Audit Committee by sending a written notice to "Audit Committee Chair, c/o FS Bancorp, Inc. PO Box 97000, Lynnwood, WA 98046. You also have the option to call 1st Security Bank's Ethics Integrity Line 1-888-274-8346 or to make a report via the internet at www.fsbwa.ethicspoint.com.

The Company will make every reasonable attempt to ensure that your concerns are addressed appropriately.

What to Expect When You Use the Integrity Line

The Ethics Integrity Line and the web portal are available 24 hours, seven days a week. Trained specialists from an independent third party provider of corporate compliance services, will answer your call, document your concerns and forward a written report to 1st Security Bank's Compliance Officer for further investigation if necessary. The Company will document the results of the investigation in a report to the Audit Committee Chairperson in order to ensure a fair process is utilized in determining whether a violation of the Code has occurred. No person expressing concerns or complaints will be subject to any disciplinary or other adverse action by the Company, including any kind of retaliation, absent a knowingly false report.

When you contact 1st Security Bank's Ethics Integrity Line or make a report using www.fsbwa.ethicspoint.com you may choose to remain anonymous where allowed by local law. All reports will be treated equally whether they are submitted anonymously or not.

After you make a report, you will receive an identification number so you can follow up on your concern. Following up is especially important if you have submitted a report anonymously, as we may need additional information in order to conduct an effective investigation. This identification number will also enable you to track the resolution of the case; however please note that, out of respect for privacy, the Company will not be able to inform you about individual disciplinary actions.

Any report you make will be kept confidential by all individuals involved with reviewing and, if necessary, investigating it to the degree possible.

1st Security Bank has an opportunity to improve every time you ask a question or raise a concern.

When you take action, speak up and report questionable conduct, you are protecting your colleagues and our reputation. Remember, an issue cannot be addressed unless it is brought to someone's attention.

question **Our supervisor typically does nothing when concerns about potential misconduct are brought to her attention and I believe she has made things difficult for co-workers who have raised issues. Now I have a problem. A co-worker is doing something that I believe to be ethically wrong. What should I do?**

Take action and speak up. You are required to report misconduct. While starting with your supervisor is often the best way to efficiently address concerns, if you do not believe that it is appropriate or do not feel comfortable doing so, you should talk to another member of management, or any of the resources listed in the Code.

question **What if someone misuses the Integrity Line, makes an anonymous call, and falsely accuses someone of wrongdoing?**

Experience has shown that the Integrity Line is rarely used for malicious purposes, but it is important to know that we will follow up on calls and anyone who uses the Integrity Line in bad faith to spread falsehoods or threaten others, or with the intent to unjustly damage another person's reputation, will be subject to disciplinary action up to and including termination.

Our Non-Retaliation Policy

We will not tolerate any retaliation against an employee who in good faith asks questions, makes a report of actions that may be inconsistent with our Code, laws or regulations or who assists in an investigation of suspected wrongdoing.

Reporting "in good faith" means making a genuine attempt to provide honest, complete, and accurate information, even if it later proves to be unsubstantiated or mistaken.

question **I suspect there may be some unethical behavior going on in my business unit involving my supervisor. I know I should report my suspicions, and I'm thinking about using the Integrity Line, but I'm concerned about retaliation.**

You are required to report misconduct and in your situation using the Integrity Line is a good option. We will investigate your suspicions and may need to talk to you to gather additional information. After you make the report, if you believe you are experiencing any retaliation, you should report it. We take claims of retaliation seriously. Reports of retaliation will be thoroughly investigated and, if they are true, retaliators will be disciplined up to and including termination.

Employee Responsibilities

Each of us must take responsibility for acting with integrity, even when this means making difficult choices. Meeting our responsibilities is what enables us to succeed and grow, today – and in the future.

- Always act in a professional, honest, and ethical manner when acting on behalf of the Company.
- Know the information in the Code and written Bank policies, paying particular attention to the topics that pertain to your job responsibilities.
- Complete all required employee training in a timely manner and keep up-to-date on current standards and expectations.
- Report concerns about possible violations of laws, regulations, or the Code to your supervisor, an Executive or any of the resources listed in this Code.

- Cooperate and tell the truth when responding to an investigation or audit and never alter or destroy records in response to an investigation or when an investigation is anticipated.

Remember: no reason, including the desire to meet business goals, should ever be an excuse for violating laws, regulations, the Code or 1st Security Bank policies.

question **I'm a manager and I'm not clear what my obligations are if someone comes to me with an accusation – and what if it involves a senior leader?**

No matter who the allegation involves, you must report it without exception. 1st Security Bank provides several avenues for reporting concerns. If for any reason you are uncomfortable making a report to a particular person, you may talk to any of the other resources listed in the Code or another member of management.

Additional Responsibilities of 1st Security Bank's Leadership

1st Security Bank leaders are expected to meet the following additional responsibilities:

- Lead by example. Managers are expected to exemplify the highest standards of ethical business conduct.
- Help create a work environment that focuses on building relationships, recognizes effort, and values mutual respect and open communication.
- Be a resource for others. Communicate to employees, consultants and vendors about how the Code and policies apply to their daily work.
- Be proactive. Look for opportunities to discuss and address ethics and challenging situations with others.
- Create an environment where everyone feels comfortable asking questions and reporting potential violations of the Code and policies. Respond quickly and effectively to concerns that are brought to your attention.
- Never ask another or pressure anyone to do something that you would be prohibited from doing yourself. Take responsibility for your actions and report inappropriate activities.
- Ensure that Company resources are used properly and productively.
- Be aware of the limits of your authority and do not take any action that exceeds those limits. Delegate authority only where permissible and never delegate authority to any individual who you believe may engage in unlawful conduct or unethical activities.
- If you supervise third parties, ensure that they understand their ethics and compliance obligations.

Managers should not consider ethics concerns as a threat or challenge to their authority - we want an open, honest and trustful dialogue to become a natural part of daily work.

question **I'm a manager. If I observe misconduct in an area not under my supervision, am I still required to report the issue?**

You are chiefly responsible for employees, contractors and third parties under your supervision, but all 1st Security Bank employees are required to report any misconduct they become aware of, and as a leader you are especially obliged to take action. The best approach is to talk first with the supervisor who oversees the area where the problem is occurring, but if this doesn't work, or isn't feasible, you should use other resources listed in the Code.

Cooperating with investigations

All employees are required to cooperate fully and truthfully with investigations. With respect to inquiries from regulators, we must never mislead any investigator and never alter or destroy documents or records in response to an investigation.

All requests for information other than what is provided on a routine basis should be reported to the Compliance Officer and/or the Enterprise Risk Manager immediately. When we are notified of an external investigation, we will take prompt action to preserve documents that may be relevant.

The Compliance Officer, Enterprise Risk Manager or an independent third party will investigate all reports of known or suspected wrongful conduct as 1st Security determines necessary. Any employee found to have engaged in any wrongful conduct will be subject to disciplinary action, up to and including termination of employment, by 1st Security and civil or criminal prosecution when warranted.

Information reported should include the identification of the individual believed to have committed the wrongful conduct, a brief description of the alleged wrongful conduct, and any evidence of the alleged wrongful conduct that is known to you.

Employees are expected to cooperate in the investigation of any report made under this policy. This may include answering questions; providing evidence that is in your possession, custody, or control; or other actions that may be requested. 1st Security will attempt to keep all investigations as confidential as possible.

question **I just learned that a good friend of mine has been accused of sexual harassment and that an investigation is being launched. I can't believe it's true and I think it's only fair that I give my friend an advance warning or a 'heads up' so he can defend himself. Don't I have a responsibility as a friend to tell him?**

Under no circumstances should you give him a 'heads up.' Your friend will be given the opportunity to respond to these allegations as part of the investigation. An allegation of sexual harassment is a very serious matter with implications not only for the individuals involved but also for the Company. Alerting your friend could jeopardize the investigation and expose the Company to additional risk and possible costs.

1st Security Bank
Integrity Test

Making the right decision is not always easy. There will be times when you'll be under pressure or unsure of what to do. Always remember when you have a tough choice to make, you're not alone. Your colleagues and management are available to help, and you have other resources to turn to including the Code, our policies, your supervisor, and the Ethics Integrity Line.

When faced with a tough decision it may help to ask these questions:

- Is it legal?
- Is it consistent with the Code and policies?
- Is it based on a thorough understanding of the risks involved?
- Will I be able to look myself in the mirror and be proud of the decision?
- Would I still be comfortable with the decision if it appeared in the newspaper?

If the answer to any of these questions is no, stop and seek help to identify a better course of action.

question **My department sets various goals that we are asked to achieve. Sometimes I feel pressured to violate the Code and policies to achieve these goals. Is this acceptable?**

No. While successful businesses set high goals and employees strive to achieve them, you should never violate the Code or 1st Security Bank's policies to achieve your goals.

Accountability and Discipline

Violating relevant laws, regulations or the Code, or encouraging others to do so, exposes the Company to liability and puts 1st Security Bank's reputation at risk. If an ethics or compliance problem does occur, you are required to report it so that an effective solution can be developed. You should also understand that violations of laws or regulations may result in legal proceedings and penalties including, in some circumstances, criminal prosecution.

Waivers and Exceptions

Management will regularly reassess this Code and recommend changes to the Board of Directors for approval. In extremely limited circumstances, the Company may find it appropriate to waive a provision of the Code.

Any requests for waivers of the Code for employees who are not executive officers should be directed through your supervisor to the CEO. Requests for waivers for directors and executive officers should be directed to the Board of Directors through the Enterprise Risk Manager or Compliance Officer. Only a majority of the Board of Directors may waive the applicability of the Code for a director or executive officer. All waivers granted to executive officers and directors will be approved by the Board of Directors (with any related party abstaining from voting) and disclosed as required by law and the Nasdaq Stock Market.

Respect and Integrity in **The Workplace**

We owe each other honesty, respect and fair treatment and we need to always treat others as we would want to be treated. This is the basis of our commitment to one another and is the foundation of our success. To maintain our commitment and to attract and keep talented individuals it is vital that we continue to have a supportive, professional and respectful work environment.

Maintaining this environment not only helps 1st Security Bank succeed, it also creates the setting for each of us to thrive and to reach our full potential. What follows are some of the key areas where we must be guided by our commitment to Our Values and to each other.

Diversity and Non-Discrimination

1st Security Bank helps bring together employees with a wide variety of backgrounds, skills and cultures. Combining such a wealth of talent and resources creates the diverse and dynamic teams that consistently drive our results.

Our colleagues, job applicants and business partners are entitled to respect and should be judged on the basis of their qualifications, demonstrated skills and achievements.

We support laws prohibiting discrimination based on a person's race, color, gender, national origin, age, religion, disability, veteran status, marital status, sexual orientation or other protected characteristics.

Make sure you:

- Treat others respectfully and professionally.
- Promote diversity in hiring and other employment decisions.
- Do not discriminate against others on the basis of any other characteristic protected by law or Company policy.

Watch out for:

- Comments, jokes or materials, including emails, which others might consider offensive.
- Inappropriate bias when judging others. If you supervise others, judge them on performance. Avoid introducing unrelated considerations into your decisions. Use objective, quantifiable standards.

To learn more:

- Discuss any questions, concerns about diversity and equal opportunity with your manager or our Human Resources Department.

question **One of my co-workers sends emails containing jokes and derogatory comments about certain nationalities. They make me uncomfortable, but no one else has spoken up about them. What should I do?**

You should notify your immediate supervisor or the Human Resources Department. Sending such jokes violates our values as well as our policies pertaining to the use of email and our standards on diversity, harassment and discrimination. By doing nothing you are condoning discrimination and tolerating beliefs that can seriously erode the team environment that we have all worked to create.

Harassment-Free Workplace

We all have the right to work in an environment that is free of unlawful discrimination and unlawful harassment. Unwelcome actions, words, jokes or comments based on an individual's sex, race, ethnicity, national origin, age, sensory, mental or physical impairment, relation, citizenship, military status, sexual orientation, gender identity or any other legally protected characteristic will not be tolerated.

At 1st Security Bank we do not tolerate:

- Threatening remarks, obscene phone calls, stalking or any other form of harassment.
- Causing physical injury to another.
- Intentionally damaging someone else's property or acting aggressively in a manner that causes someone else to fear injury.
- Threatening, intimidating or coercing others on or off the premises -- at any time, for any purpose.
- Weapons are not permitted in the workplace. This includes not only our facilities, but also parking lots and alternate work locations maintained by the Company.

A common form of harassment is sexual harassment, which in general occurs when:

- Actions that are unwelcome are made a condition of employment or used as the basis for employment decisions such as a request for a date, a sexual favor, or other similar conduct of a sexual nature.
- An intimidating, offensive, or hostile work environment is created by unwelcome sexual advances, insulting jokes, or other offensive verbal or physical behavior of a sexual nature.

Make sure you:

- Help each other by speaking out when a co-worker's conduct makes others uncomfortable.
- Never tolerate sexual harassment including requests for sexual favors, or other unwelcome verbal or physical conduct of a sexual nature.

- Demonstrate professionalism. Do not visit inappropriate internet sites or display sexually explicit or offensive pictures.
- Promote a positive attitude toward policies designed to build a safe, ethical and professional workplace.
- Report all incidents of harassment and intimidation that may compromise our ability to work together and be productive.

Watch out for:

- Unwelcome remarks, gestures or physical contact.
- The display of sexually explicit or offensive pictures or other materials
- Sexual or offensive jokes or comments (explicit or by innuendo) and leering.
- Verbal abuse, threats or taunting.

To learn more:

- Discuss any questions, concerns about harassment with your manager or our Human Resources Department.

question **While on a business trip, a colleague of mine repeatedly asked me out for drinks and made comments about my appearance that made me uncomfortable. I asked him to stop, but he wouldn't. We weren't in the office and it was 'after hours' so I wasn't sure what I should do. Is it harassment?**

Yes it is. This type of conduct is not tolerated, not only during working hours but in all work-related situations including business trips. Tell your colleague such actions are inappropriate and must be stopped, and if they continue you need to report the problem.

Employee Privacy

In recent years, individuals, companies and governments have grown increasingly concerned about the privacy and security of personal information. As a result, laws protecting personal information and how it may be collected, shared, and used are becoming more common.

Many of us have access to personal information related to our colleagues and others. While protecting this information may now be a legal requirement, for us at 1st Security Bank privacy has always been a matter of trust.

Make sure you:

- Learn about the types of information which are given heightened protection by the law and Company policy (such as personally identifiable information, like social security numbers and bank account numbers) and protect them through appropriate means (such as encryption or other types of limited access).
- Protect the confidentiality of personal information of current and former colleagues, as well as job applicants, business partners and customers.
- Never share colleagues' information outside the Company.
- Consult Human Resources if law enforcement or regulatory authority or any other person outside the Company requests employee information.
- Return or destroy personal information that is no longer required by you for business reasons in accordance with our records retention policies.
- Only share confidential employee information within the Company if you have made sure it will be appropriately protected.

- Immediately report to a manager any loss or inadvertent disclosure of employee information.

Watch out for:

- Unintentional exposure of confidential information in public settings such as on phone calls or while working on your laptop.
- The loss of control of confidential information. When sending personal information across borders or to third parties, make sure that the transmissions are for legitimate business reasons and that they comply with local law.

To learn more:

- Discuss any questions, concerns about employee privacy and confidential information with Compliance or Human Resources.

Safe and Healthy Work Environment

1st Security Bank is committed to providing a safe and healthy work environment for colleagues and visitors to our facilities. Each of us is responsible for acting in a way that protects ourselves and others.

Be proactive and speak up. The more we communicate, the better we can respond to any unsafe or unhealthy working conditions.

Situations that may pose a health, safety or environmental hazard must be reported immediately. We can only achieve our goal of a safe and healthy workplace through the active participation and support of everyone.

Make sure you:

- Observe the safety, security and health rules and practices that apply to your job.
- Always display and swipe your personal identification badge when entering and exiting secure areas and do not allow others to enter without properly swiping their personal identification badges.
- Notify your supervisor immediately about any unsafe equipment, or any situation that could pose a threat to health or safety or damage the environment. All employees have the right and responsibility to stop any work they feel may be unsafe.
- Comply with safety and health policies and procedures.
- Maintain a neat, safe working environment by keeping work stations, aisles and other work spaces free from obstacles, wires and other potential hazards.

Watch out for:

- Unsafe practices or work conditions.
- Lax enforcement of security standards, such as facility entry procedures and password protocols.
- Threats, intimidation and violence are unacceptable and have no place at 1st Security Bank, in our workplace or at any off-site work-related activity.
- Possession of a firearm, deadly weapon or explosives is not permitted on the company premises at any time.

To learn more:

- Discuss any questions, concerns about environmental, health and safety with Facilities or Human Resources.

Alcohol and drug-use policy

- While at work or on Company business, you should never be impaired, and always ready to carry out your work duties.

question **I've noticed some practices that we do in my area they don't seem safe. Who can I speak to? I'm new here, and don't want to be considered a troublemaker.**

Discuss your concerns with your supervisor or Human Resources. There may be very good reasons for the practices, but it's important to remember that raising a concern about safety does not cause trouble, it is being responsible.

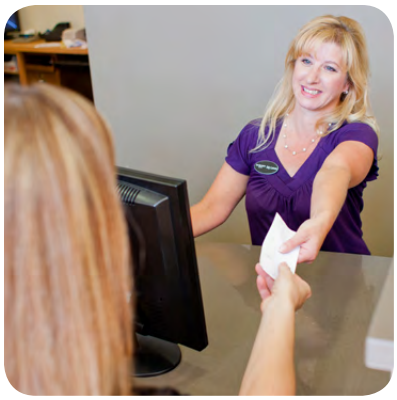
question **Are subcontractors expected to follow the same Health, Safety and Security policies and procedures as employees?**

Absolutely. Managers and supervisors are responsible for ensuring that subcontractors and vendors at work on 1st Security Bank premises understand and comply with all applicable laws, and regulations governing the particular facility, as well as with additional requirements the Company may impose.

Preventing Workplace Violence

Violence of any kind has no place at 1st Security Bank. We won't tolerate the following:

- Physically intimidating, threatening or hostile behavior.
- Causing physical injury to another.
- Acts of vandalism, arson, sabotage or other criminal activities.
- The carrying of weapons on to Company property – unless you are authorized to do so. Possessing a firearm, explosive or other dangerous weapon on 1st Security premises or using an object as a weapon.
- Offensive comments regarding violent events or behavior.
- Inflicting or threatening injury or damage to another person's life, health, well-being, family or property.
- Abusing or damaging 1st Security or employee property.
- Using obscene or abusive language or gestures in a threatening manner.
- Raising voices in a threatening manner.
- Any other act, which, in management's opinion is inappropriate in the workplace.



Maintaining APPROPRIATE BUSINESS RELATIONS

Maintaining Appropriate Business Relations

Conflicts of Interest

A conflict of interest happens whenever you have a competing interest that may interfere with your ability to make an objective decision for 1st Security Bank. Each of us is expected to use good judgment and avoid situations that can lead to even the appearance of a conflict which can undermine the trust others place in us and damage our reputation.

Conflicts of interest may be actual, potential or even just a matter of perception. Since these situations are not always clear-cut, you need to fully disclose them to your supervisor so that we can properly evaluate, monitor and manage them.

Make sure you:

- Avoid conflict of interest situations whenever possible.
- Always make business decisions in the best interest of 1st Security Bank.
- Discuss with your manager full details of any situation that could be perceived as a potential conflict of interest. Your manager may require you to disclose the situation to the Human Resources Department.
- Think ahead and proactively address situations that may put your interests or those of a family member in potential conflict with 1st Security Bank.

Watch out for:

- Situations including the following, which are common examples of potential conflicts of interest:

Corporate opportunities

If you learn about a business opportunity because of your job, it belongs to 1st Security Bank first. This means that you should not take that opportunity for yourself unless you get approval from two of the following individuals CEO, CFO, Enterprise Risk Manager or the Compliance Officer.

Friends and relatives

On occasion, it is possible that you may find yourself in a situation where you are working with a close friend or relative who works for a customer, supplier, competitor, etc. Since it is impossible to anticipate all situations that may create a potential conflict, you should disclose your situation to your supervisor in order to determine if any precautions need to be taken.

Outside employment

To ensure that there are no conflicts and that potential issues are addressed, you always need to disclose and discuss outside employment with your supervisor. If approved, you need to ensure that this outside activity does not interfere or detract from your work. Working for a competitor, supplier, or customer may raise conflicts that will need to be resolved. Also, any approved side or personal business should not compete or do any business with 1st Security Bank. If you have outside employment, please complete the "Request for Outside Employment form" to be signed by our CEO or CFO.

Financial Interests

You should not have a significant investment in, or obligation to, one of 1st Security Bank's competitors, suppliers, customers or business partners unless it is fully disclosed and you have obtained permission from the previously stated positions. "Significant" is hard to define, but as a rule of thumb, it means that your investment should not be big enough for someone to reasonably think that you would do something at 1st Security Bank's expense to help your investment. If you are unsure whether there is a conflict, you should ask for additional guidance.

Civic activities

Unless company management specifically asks you to do so, you shouldn't accept a seat on the board of directors or advisory board of any of our competitors, suppliers, customers or partners, especially if your current job gives you the ability to influence our relationship with them.

To learn more:

- Discuss any questions, concerns about conflicts of interest with your manager and/or the Compliance Officer or Enterprise Risk Manager.

Gifts and Entertainment

In the right circumstances, a modest gift may be a thoughtful "thank you," or a meal may be an appropriate setting for a business discussion which strengthens a professional relationship. However, if not handled carefully, the exchange of gifts and entertainment can look like a conflict of interest, especially if it happens frequently or if the value is large enough that someone could reasonably think it is influencing a business decision.

When it comes to gifts and entertainment, our position is straightforward – we do not accept or provide gifts, favors, or entertainment if the intent is to influence a business decision.

Gifts and entertainment, before you act – think

Gifts and entertainment come in all different forms: shirts, pens, dinners, tickets to sporting events, to name just a few examples. Before you accept or offer gifts or entertainment, think about the situation – Does it legitimately support 1st Security Bank's interest? Is the amount reasonable and customary? Would this embarrass you or the Company if it was on the front page of the newspaper?

Make sure you:

- Only provide and accept gifts and entertainment that are reasonable complements to business relationships.
- Never accept gifts of any kind from a business partner with whom you are involved in contract negotiations.
- Exchange gifts and entertainment that foster goodwill in business relationships, but never provide or accept gifts, and entertainment that obligate or appear to obligate the recipient.
- Do not request or solicit personal gifts, favors, entertainment, or services.
- Accepting gifts of cash or cash equivalents is never allowed.
- Do not accept any single gift worth more than $100, without receiving prior approval from the Human Resource Manager or Enterprise Risk Manager.
- Understand and comply with the policies of the recipient's organization before offering or providing gifts, favors or entertainment.
- Be careful when using agents who represent us or third parties who introduce business partners to us. Monitor them during the duration of any agreement to ensure they live up to our high standards.
- Raise a concern whenever you learn of any sign or "red flag" that a colleague, third party or other agent of the Company may be engaged in any attempt to improperly influence a decision of a customer or government official.
- All gifts with $100 value or greater must be reported to Accounting to be documented in the Federal Deposit Insurance Corporation (FDIC) gift log. All situations will be reviewed by Compliance on a case by case basis.

Watch out for:

- Situations that could embarrass you or the Company, including entertainment at sexually oriented establishments.
- Business partners or customers who may have gift and entertainment standards that are stricter than ours.
- Business partners that appear to be privately held but are actually considered government entities.
- Gifts, favors or entertainment that may be reasonable for a privately owned customer but not for a government official or agency.
- Third parties or agents who are thought to be valuable primarily for their personal ties rather than for the services they are to perform or who request compensation out of proportion to their services.

To learn more:

- Discuss any questions, concerns about gifts and entertainment with your manager, HR Manager or Enterprise Risk Manager.

question **When I was traveling, I received a gift from a business partner that I believe was excessive. What should I do?**

You need to let you manager know or report it to the Human Resource Manager or Enterprise Risk Manager as soon as possible. We may need to return the gift with a letter explaining our policy. If a gift is perishable or impractical to return, another option may be to distribute it to employees or donate it to charity, with a letter of explanation to the donor.

question **During contract negotiations with a potential new supplier, the new supplier mentioned that they had a complimentary registration to a local business seminar. They are unable to attend and asked if I would like to go in their place. I had been thinking of attending the seminar anyhow, since the subject of the seminar applies to my work. There's no personal gain to me, it would be good for 1st Security Bank, and it would be a shame to waste the registration, I planned on saying 'yes.' Now I wonder if that would be the right decision.**

You should decline the offer. If you are involved in contract negotiations, you must never accept any gifts while the negotiation process is on-going. Accepting gifts during negotiations can give the appearance of a 'quid pro quo' and is always inappropriate.

Gifts and entertainment of government representatives

The Company is committed to meeting the many special legal, regulatory and contractual requirements that apply to government-related work. These requirements may apply to bidding, accounting, invoicing, subcontracting, employment practices, contract performance, gifts and entertainment, and other matters.

In addition, 1st Security Bank may be legally obligated to impose these requirements on any agents or subcontractors we bring in to help in the work. You must always make sure you know whether you are dealing with a government-related entity. This is not always obvious. Businesses such as airlines, oil companies and telecommunications providers may be owned or controlled by a government, in whole or in part, and subject to special rules. When in doubt, discuss the situation with your manager, Accounting or the CFO.

Working with
Our Customers and Vendors

Honest and Ethical Dealing

We treat our customers and vendors fairly. We work to understand and meet their needs, while always remaining true to our own ethical standards. We tell the truth about our services and capabilities and we do not make promises we can't keep.

In short, we treat our customers and vendors as we would like to be treated.

Marketing and Advertising Standards

Marketing of 1st Security Bank must be truthful and accurate. Our advertising and promotions must always be tasteful and not offensive to 1st Security Bank, consumers and the general public and always use due diligence when choosing distributors and business partner to ensure they meet our standards. False claims about competitors' products or services are never acceptable.

Make sure you:

- Treat each customer fairly and honestly.
- Speak up and talk to your supervisor if you have concerns about any error, omission, undue delay, or defect in quality or our customer service.
- Promptly raise with a manager any potential conflict of interest between you, customers or the Company.
- Never follow a customer's request to do something that you regard as unethical or unlawful.
- Be responsive to customer requests and questions.
- Promise what you can deliver and deliver on what you promise.

Watch out for:

- Pressures from colleagues or managers to cut corners on quality or delivery standards.
- Temptations to tell customers what you think they want to hear rather than the truth; if a situation is unclear begin by presenting a fair and accurate picture as a basis for decision.

To learn more:

- Discuss any questions or concerns about our products or customer service with the SVP of Retail Banking or SVP of Service and Operations.

Protecting the Privacy and Confidential Information of Others

Our customers and our business partners place their trust in us. We must protect their confidential information.

Make sure you:

- Learn about the types of information which are given heightened protection by the law and Company policy (such as personally identifiable information, like social security numbers and bank account numbers) and protect them through appropriate means (such as encryption or other types of limited access).
- Immediately report any loss or theft of confidential information.

Watch out for:

- Requests by business partners for information about our customers or about our business partners.
- Unintentional exposure of Client information in public settings such as on phone calls or while working on your laptop.

To learn more:

- Discuss any questions, concerns about customer privacy with Compliance or a Leadership Team member.

Competitive Intelligence

Information about competitors is a valuable asset in today's competitive business environment. When collecting business intelligence, 1st Security Bank employees, and others who are working on our behalf, must always live up to the highest ethical standards.

We must never engage in fraud, misrepresentation or deception to obtain information. Nor should we use invasive technology to "spy" on others. We also need to be careful when accepting information from third-parties. You should know and trust their sources and be sure that the knowledge they provide is not protected by trade secret laws, or non-disclosure or confidentiality agreements.

While 1st Security Bank employs former employees of competitors, we recognize and respect the obligations of those employees not to use or disclose the confidential information of their former employers.

Make sure you:

- Obtain competitive information only through legal and ethical means, never through misrepresentation.
- Never contact a competitor regarding their confidential information.
- Respect the obligations of others to keep competitive information known to them as confidential.
- Do not induce or receive confidential information of other companies.
- Make sure that third parties acting on our behalf live up to our standards.
- Do not disclose suppliers' non-public pricing information.

Watch out for:

- Retaining papers or computer records from prior employers in violation of laws or contracts.
- Using anyone else's confidential information without appropriate approvals.
- Using job interviews as a way of collecting confidential information about competitors or others.
- Asking new employees to discuss confidential information from their previous employer.
- Receiving suggestions from third parties for new products, product feature, or services when the source of the original idea is not fully known.
- Obtaining information through any behavior that could be construed as "espionage", "spying" or which you would not be willing to fully disclose.
- Relying, without verification, on third parties' claims that business intelligence was obtained properly.

To learn more:

- Discuss any questions, concerns about collecting business intelligence with the public with your manager or Compliance.

question **I am a manager and one of my team members who recently joined 1st Security Bank from a competitor has with her a customer list and price list of the competitor. She says she plans to use it to our advantage. Should I just ignore this and let her do it?**

No. If an employee retains competitor information it can result in legal action by the competitor. You must report this to Compliance for appropriate action.

Protecting
OUR INFORMATION AND ASSETS

Protecting
Our Information and Assets

Protecting 1st Security Bank Assets

We are entrusted with Company assets and are personally responsible for protecting them and using them with care. Company assets include funds, facilities, equipment, information systems, intellectual property and confidential information.

Make sure you:

- Only use 1st Security Bank assets for legitimate business purposes.
- Personal use of Company assets is discouraged, should be kept to a minimum, and have no adverse effect on productivity and the work environment.
- Do not use 1st Security Bank equipment or information systems to create, store or send content that others might find offensive.
- Do not share passwords or allow other people, including friends and family, to use 1st Security Bank resources.
- Respect the copyrights, trademarks and license agreements of others when dealing with printed or electronic materials, software or other media content.
- If you suspect any fraud or theft of company assets, immediately tell your supervisor or one of the following individuals; Human Resource Manager, Enterprise Risk Manager or the Compliance Officer.

- Only use software that has been properly licensed. The copying or use of unlicensed or "pirated" software on Company computers or other equipment to conduct company business is strictly prohibited. If you have any questions about whether or not a particular use of software is licensed, contact the IT Department.

Watch out for:

- Company property that is not secured when not in use.
- Requests to borrow or use 1st Security Bank equipment without approval.
- Unknown individuals without proper credentials in our facilities.
- Excessive use of 1st Security Bank resources for personal purposes.
- Lax enforcement of electronic access control cards.
- Sharing passwords.

To learn more

- Discuss any questions, concerns about protecting 1st Security Bank assets with the Compliance Officer or the Enterprise Risk Manager.

Confidential Information

One of our most valuable assets is information. Each of us must be vigilant and protect 1st Security Bank's confidential information. This means keeping it secure, limiting access to those who have a need to know in order to do their job, and avoiding discussion of confidential information in public areas.

The obligation to preserve 1st Security Bank's confidential information continues even after employment ends.

Make sure you:

- Use and disclose confidential information only for legitimate business purposes.
- Properly label confidential information to indicate how it should be handled, distributed and destroyed.
- Protect intellectual property and confidential information by sharing it only with authorized parties.
- Only store or communicate Company information using 1st Security Bank's information systems.

Watch out for:

- Never discuss confidential information when others might be able to overhear what is being said – for example on planes, elevators and when using mobile phones.
- Be careful not to send confidential information to unattended fax machines or printers.

To learn more:

- Discuss any questions, concerns about confidential information with any one of the following employees; Compliance Officer, Enterprise Risk Manager or the Human Resources Manager.

Intellectual property

1st Security Bank's intellectual property (IP) is an important asset that must be protected. Some examples of our IP are:

- Business and marketing plans
- Company initiatives (existing, planned, proposed or developing)
- Customer lists
- Trade secrets and discoveries
- Methods, know-how and techniques
- Innovations and designs
- Systems, software and technology
- Patents, trademarks and copyrights.

Promptly disclose to company management any inventions or other IP that you create while you are employed by 1st Security Bank.

Properly label confidential information including IP to indicate how it should be handled, distributed and destroyed.

Protect IP by sharing it only with authorized parties.

Communicating with the Public

1st Security Bank needs a consistent voice when making disclosures or providing information. It is important that only authorized persons speak on behalf of the Company. We must maintain the highest standards of integrity, objectivity and transparency. We are committed to honest, professional and legal communications to colleagues, business partners, and the public.

Make sure you:

- Refer all inquiries about our activities, sales or financial results, or strategic plan to the CFO or CEO.
- Always get prior approval from CEO or Marketing Committee before making public speeches, writing articles for professional journals or other public communication when you are identified with the Company.
- Obtain approval from CEO before distributing any communication intended for a broad employee audience. Communications intended for cross-Company distribution require approval from CEO.
- Never give the impression that you are speaking on behalf of the Company in any personal communication, including user forums, blogs, chat rooms and bulletin boards.

Watch out for:

- Any suggestion you speak for the Company in your personal communications, including in emails, blogs, message boards and social networking sites.
- Temptations to use your Company title or affiliation outside work for 1st Security Bank – such as in charitable or community work – without making clear the fact that the use is for identification only and that you are not representing the Company.
- Invitations to speak "off the record" to reporters or others who ask you for information about the Company.

To learn more:

- Discuss any questions, concerns about communicating with the public with 1st Security Bank's CEO, CFO or Marketing Department Manager.

Using Social Media

Be careful when writing communications that might be published online. If you participate in online forums, blogs, newsgroups, chat rooms, or bulletin boards, never give the impression that you are speaking on behalf of 1st Security Bank and before you hit the 'send' button think carefully.

Don't send emails or post confidential information or material that could be perceived as damaging to the Company's reputation.

Integrity

Following
the Letter and the Spirit of the Law

Insider Trading

Confidential information may not be used for personal benefit. Each of us is prohibited from trading securities or passing information on to others who then trade ('tipping') on the basis of material information before it is made publicly available to ordinary investors.

Material information is the kind of information a reasonable investor would take into consideration when deciding whether to buy or sell a security. Some examples of information about a company that might be material are:

- A proposed acquisition or sale
- A significant expansion or cutback of operations
- A significant product development or important information about a product
- Extraordinary management or business developments
- Changes in strategic direction including entering new markets

Make sure you:

- Do not buy or sell securities of any company when you have material nonpublic information about that company.
- Do not communicate such material nonpublic information to other people.
- Protect material nonpublic information from the general public including securing information both electronic and in paper copy.

Watch out for:

- Requests by friends or family for information about companies that we do business with or have confidential information about. Even casual conversations could be viewed as illegal "tipping" of inside information.

- **TIPPING** - You need to be very careful when you have this type of information to make sure you do not share it with anyone, either on purpose or by accident, unless it is essential for 1st Security Bank-related business. Giving this information to anyone else who might make an investment decision based on your inside information is considered "tipping" and is against the law regardless of whether you benefit from the outcome of their trading.

To learn more:

- Discuss any questions or concerns about insider trading with the CEO, CFO, Compliance Officer and/or the Enterprise Risk Manager.

question **I'm not sure what kind of information is covered by the term 'material information.' What does it include?**

'Material information' includes any information that a reasonable investor would consider important when deciding whether to buy, sell or hold a security. This can include news about acquisitions, financial results, important management changes, as well as news about the financial performance of a company. If you're in doubt about whether certain information is material or has been released to the public, don't trade until you have consulted with the CFO. The general rule of thumb for insider trading is "when in doubt, do NOT trade". If the CFO is not available, consult with the CEO, Compliance Officer or Enterprise Risk Manager.

Anti-corruption and Bribery

All countries prohibit the bribery of their own public officials and many also prohibit the bribery of officials of other countries. We do not pay bribes, kickbacks or facilitation payments, at any time for any reason. This applies equally to any person or firm who represents 1st Security Bank.

Key definitions - bribery, corruption and facilitation payments

Bribery means giving or receiving undue reward (or offering to do so) to influence the behavior of someone in government or business in order to obtain business or financial or commercial advantage.

Corruption is the abuse of an entrusted power for private gain.

Facilitation payments are typically small payments to a low-level government official that are intended to encourage the official to perform his responsibilities.

It is especially important that we carefully monitor third parties acting on our behalf. We must always be sure to perform due diligence and know our business partners, and all those through whom we conduct our business. We must know who they are and what they are doing on our behalf. Third parties must understand that they are required to operate in strict compliance with our standards and to maintain accurate records of all transactions.

Make sure you:

- Never give anything of value inconsistent with local laws and regulations to any governmental official. If you are not sure what the local laws are, the safest course of action is to not give anything of value.
- Understand the standards set forth under anti-bribery laws which apply to your role at 1st Security Bank.
- Accurately and completely record all payments to third parties.

Watch out for:

- Apparent violations of anti-bribery laws by our business partners.

Anti-money laundering

Money laundering is a global problem with far-reaching and serious consequences. It is defined as the process of converting illegal proceeds so that funds are made to appear legitimate, and it is not limited to cash transactions. Involvement in such activities undermines our integrity, damages our reputation, and can expose the Company and individuals to severe sanctions.

Report any suspicious financial transactions and activities to the Compliance Officer and if required, reports would be filed with the appropriate government agencies.

When in doubt or if any cases of irregular payments or money laundering are observed, report the matter to the Compliance Officer.

To learn more:

- Discuss any questions or concerns with the Compliance Officer.

1ST SECURITY BANK

FS BANCORP, INC.