

SEACOAST NATIONAL BANK

CODE OF CONDUCT

Introduction

At Seacoast National Bank (SNB), we strive to provide quality products and service within the confines of ethical business practices. The strength of our company lies in maintaining mutual respect between, and within, the company and our various stakeholders, and in preserving our reputation for integrity. Our customers, shareholders and communities expect us to meet very high standards. They entrust us with their money, confidential information and important aspects of their lives.

This Code of Conduct reflects our commitment to live up to those expectations. Many of these policies are based on laws and regulations. Others are based on philosophical and ethical principles that enhance our ability to work together cooperatively and conduct our business effectively. We are all responsible for complying with both the letter and spirit of applicable laws and regulations, as well as with company policies designed to guide us in maintaining our principles. We are expected to avoid illegal, dishonest, or unethical conduct, or any other actions that might reflect unfavorably on either our own integrity or that of our company.

The provisions of this Code of Conduct will be enforced, and all employees are responsible for knowing and complying with these, as well as with the Associates Handbook and with any additional standards set by the division and respective department in which you work. Failure to do so, or conduct in violation of any law or regulation, may lead to discipline, up to and including dismissal. We may be periodically required to attest to our compliance with the Code of Conduct.

We should all work to create an atmosphere that supports respect, integrity, teamwork, and excellence, and we should be proud of our company. Employees who become aware of any behavior by another employee that is in conflict with either the spirit and letter of the Code of Conduct are urged to discuss the matter either with their manager, Compliance Officer, Human Resources Department, or report the occurrence to the Chief Risk Officer. The situations will be appropriately and confidentially investigated, to the extent possible. There will be no retaliation against employees who report information in good faith.

Social Conduct and Bank Commitments

As bankers, employees are required to conduct themselves in a manner that will not damage the reputation of the Bank, or the employee, through the perceptions of our shareholders, coworkers, community and our families. At times, the Bank

will sponsor events, including after-hour meetings and employee celebration events, management retreats, customer dinners or socials, private banking events, and community/civic functions, where the social nature of the event may include the serving of alcohol. Employees who participate in these events, and choose to drink alcohol, do so with the expectation that they will drink in moderation and will be accountable for their actions under the Code of Conduct.

Employee participation in off-hour events is seen as a very important leadership activity that builds relationships with customers and employees. At times, the scheduling of these events can come into conflict with the employee's responsibilities and commitments to their family. As a family-first workplace, the employee's commitment to their family obligations will be the priority. Should a schedule conflict arise that creates difficulty at home, the employee has the right to not participate or shorten their attendance at this function. In these cases the employee should notify their manager in advance of the conflict, so a substitute bank representative can be identified.

Relationship With Customers

Confidence

Confidential information with respect to customers obtained through employment with SNB is considered privileged and is to be held in strictest confidence. It is to be used solely for corporate purposes. Confidential information shall not be given to persons outside SNB, including family or associates, or even to other associates of SNB who have no need for the information in discharging their duties. (See Customer Financial Records Privacy Policy). "Confidential information" generally consists of financial and personal information learned about customers through their accounts, records on file with the bank or personal conversations with customers."

Confidential information concerning customers may in some instances be considered "inside information", which, if used or disclosed, could subject the associate, SNB and a person outside the corporation to whom the information is communicated, liable under federal and state securities laws.

Associates who end their employment with the Bank are strictly prohibited from removing or disclosing any customer information, materials or documents that are consider the Bank's property, as these are considered proprietary resources and are not the property of the associate. Should it be discovered that the associate has committed a breach of this policy, the Bank will take remedial action, up to an including legal measures to recover any form of proprietary information and property. To protect customer relationships with the Bank, specific Bank Officers may be placed under specified non-competition/non-disclosure rules, where this policy has a definitive effective period from the date of termination.

Gifts

It is a federal criminal offense for anyone to give, offer or promise anything of value to another with the intent to influence or reward an employee of a financial institution in connection with any specific business or transaction which benefits the Bank, customer or third party.

It is illegal for any financial institution associate to solicit or demand, for themselves or for any other person, or to accept anything of value with the intent to be influenced or rewarded in connection with any specific business or transaction which benefits the Bank, customer or third party.

An individual or employee representing SNB shall not provide any gift of more than nominal value to any individual or company in consideration for doing business with SNB as a customer or supplier of services. However, normal business entertainment of customers and suppliers is appropriate. Premiums such as those offered for opening new accounts may be provided in conjunction with a new business campaign, and promotional materials of reasonable value may occasionally be given to customers or others.

No individual representing SNB shall accept any gift of more than nominal value (\$50) or any fee from an actual or potential customer or supplier in connection with any specific transaction or business with SNB. Normal business entertainment and meals, refreshments, travel arrangements or accommodations offered in connection with business meetings or to foster better business relations or goodwill may be accepted if reasonable in amount. Gifts or favors based on obvious personal or family relationships are permissible when circumstances make it clear that it is the personal relationship, rather than the business of SNB that is the motivating factor. Gifts of reasonable value may also be accepted in connection with commonly recognized events, such as promotions, Christmas, weddings, births, or retirements. Discounts or rebates on merchandise or services should not be accepted from SNB customers or suppliers except to the extent they are available to all employees or to other customers. In no instance shall any gifts, offers of entertainment or favor be accepted if acceptance could jeopardize public confidence in the bank or create undesirable obligations. When in doubt, consult with your supervisor.

Whenever any individual representing SNB is offered or receives something of value beyond what is permitted by the preceding, the gift or favor shall be reported to the Chief Risk Officer or an Executive Officer. Such disclosure helps to show the individual's good faith and will help protect the individual from being implicated in circumstances that may suggest corrupt intentions or breach of trust. Any gift of more than reasonable value should be returned. When an individual is in doubt as to whether a particular gift or favor may be accepted or retained, the Chief Risk Officer may be consulted for a written determination.

An associate should not accept a bequest or legacy from a customer unless the customer is a relative of the employee.

Business and Family Relationships

An associate, who individually holds, or holds through members of their immediate family, a financial management interest in a corporation, trust or business unrelated to SNB shall not in his/her capacity as an associate, exercise any discretionary authority whatsoever with respect to any loan or other transaction between that business and SNB. (see Related Party Transaction Policy)

When acting for SNB an associate shall not exercise any discretionary authority whatsoever with respect to any loan, sale or other transaction between SNB and his/her immediate family.

Fiduciary Appointment

Fiduciary appointments, such as executor, administrator, guardian, trustee, testamentary trustee, etc., may only be accepted for family members. An exception to this policy requires written approval from an associate's manager and the Executive Officer.

Associates may not accept appointments as attorney-in-fact under general powers of attorney if a power of attorney is as general as to allow them to use their own discretion in handling customer funds. Exceptions to this policy may only be made if appointment as attorney-in-fact is part of a formal company product offering or business transaction, if it is necessary to enable Trust Department employees to exercise their responsibilities in the normal course of business, or if it is for family members.

Associates may carry out customer instructions that specify handling of the customer's accounts when authorization to do so has been obtained from the customer.

Personal Loans

Associates shall not borrow from any customer of SNB (except for normal credit purchases) unless the customer is a recognized lending institution.

Rendering Non-Banking Advice to Customers

Giving legal and tax advice is the province and responsibility of practicing attorneys and tax accountants. Associates should avoid making statements which could be construed as offering advice which might have legal or tax implications. Likewise, associates should avoid telling customers how to run their businesses since liability may accrue from controlling or interfering with a customer's business affairs. Referral of customers to professionals for specific advice may be made, provided several names are given and the customer understands the bank does not endorse any one of the references.

Responsibility to Investors

Disclosure; Purchase and Sale of Seacoast Stock or Other Securities

Inside information is material, non-public information relating to securities issued by any corporation. Information is considered "material" if it is important enough (1) to affect the judgment of investors about whether to buy, sell, or hold stock; or (2) to influence the market price of the stock. Examples of "material non-public information" typically would include, but not be limited to, advance information on earnings and dividend changes, equity or debt offerings, major bank credits, stock splits, mergers, significant developments regarding litigation or governmental proceedings, major impending corporate initiatives and impending significant changes in company management.

It is both a requirement of the law and company policy that no associate may use "material non-public information" in connection with any decision to purchase or sell or to recommend the purchase or sale of any security, whether on behalf of the company or for his or her own account, or to pass along such information to any other person for the purpose of enabling that person to use it. Even if there is no actual misuse of material non-public information, employees should avoid circumstances in which it might appear that such information is being misused.

Seacoast Banking Corporation of Florida
Anti-Hedging Policy

Approved by Board of Directors on 03/18/14

Purpose:

This document sets forth:

- Seacoast's policy prohibiting its Employees and Directors from engaging in hedging transactions related to common stock and other securities of the Company (the "Anti-Hedging Policy").

Scope:

- The Anti-Hedging Policy applies to all Employees and Directors of Seacoast.

Defined Terms:

For purposes of this policy, the following terms have the following meanings:

"Bank" means Seacoast National Bank.

"Board" means the Boards of Directors of the Company and the Bank.

"CEO" means the chief executive officer of the Company.

"Company" means Seacoast Banking Corporation of Florida.

"Compensation Committee" means the Compensation and Governance Committee of the Board of the Company.

"Covered Person" means (a) with respect to the Anti-Hedging Policy, any person who is an Employee or a Director, and (b) with respect to the Pledging Policy, any person who is an Executive Officer or a Director.

"Covered Securities" means common stock or other equity securities of the Company.

"Director" means a member of the Board.

"Dodd-Frank Act" means the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

"Effective Date" means the effective date of these policies, which shall be upon adoption by the Board.

"Employee" means any full-time employee of Seacoast, and shall include Executive Officers.

“Executive Officer” means an officer of Seacoast designated as an “executive officer” of Seacoast for the purposes of federal securities laws.

“Seacoast” means both the Company and the Bank.

Anti-Hedging Policy:

The Board believes that ownership of Covered Securities by Executive Officers and Directors promotes alignment of the interests of Seacoast’s shareholders with those of its leadership. The Board recognizes that transactions that are designed to hedge or offset declines in the market value of Covered Securities can disrupt this alignment, interfere with Seacoast’s compensation programs and philosophies, and undermine policies regarding equity ownership. The Board further believes that it is contrary to Seacoast’s best interests for non-executive Employees to engage in hedging strategies involving Covered Securities. Consequently, it is the policy of Seacoast that no Covered Person, or any designee of such Covered Person, is permitted to purchase financial instruments (including, without limitation, prepaid variable forward contracts, equity swaps, collars, forward sale contracts, exchange funds or put and call options) that are designed to hedge or offset any decrease in the market value of Covered Securities held, directly or indirectly, by such Covered Person. Nothing in this policy shall prohibit any Covered Person from holding or exercising options on Company common stock that were granted to him or her as compensation for services.

Covered Persons shall be afforded a reasonable opportunity to unwind or otherwise terminate any transaction existing as of the time he or she becomes subject to this Anti-Hedging Policy that would otherwise violate this policy. Each Executive Officer and Director will be expected to certify compliance with this Anti-Hedging Policy in connection with Seacoast’s annual securities questionnaires, and otherwise from time to time upon request by the Board. Each non-executive Employee will be expected to certify compliance with this Anti-Hedging Policy as determined by the Board from time to time.

Miscellaneous Provisions:

- It is intended that this policy be administered in a manner that will comply with applicable law and securities exchange listing requirements, such as Section 955 of the Dodd-Frank Act and the listing standards of Nasdaq. The Board shall amend this policy to the extent required to comply with final regulations issued by the Securities and Exchange Commission under Section 955 of the Dodd-Frank Act and any listing standards of Nasdaq.
- Seacoast shall take appropriate steps to inform Covered Persons of this Anti-Hedging

Responsibility to Associates and Officers

Management Accessibility

SNB has an open door policy which allows every associate who has a problem, complaint or is simply looking for advice to feel free to go to any level of management where they feel the problem can be solved, up to and including the Chief Executive Officer or an Executive Officer.

Privacy of Records/Removal of Documents

The protection of Seacoast National Bank business information, property and all other Company assets are vital to the interests and success of Seacoast National Bank. No Seacoast National Bank related information or property, including without limitation, documents, files, records, computer files, equipment, office supplies or similar materials (except in the ordinary course of performing duties on behalf of the Bank may be removed from the Company's premises. In addition, when an employee leaves Seacoast National Bank, the employee must return to the Company all Seacoast National Bank related information and property that the employee has in his/her possession, including without limitation, documents, files, records, manuals, information stored on a personal computer or on a computer disc, supplies, and equipment or office supplies.

Violation of this policy is a serious offense and will result in appropriate disciplinary action, up to and including discharge.

Code of Conduct/Confidentiality

SNB will endeavor to safeguard the privacy of its associates and confidentiality of associate records by advising associates of all personnel records maintained on them, collecting only data related to the purpose for which the files were established and allowing those authorized to use a file to do so only for legitimate SNB purposes. Associates will be allowed to inspect, and challenge for correction as necessary, information in their personnel files, excluding confidential letters of recommendation, material relating to other employees, investigator materials and audit documentation. Removal of official documents or equipment from bank premises, without the express consent of a supervisor or department head, is prohibited.

Banking Services

As part of their total compensation, associates may be provided certain banking services at less than the standard charges for such services to the public, and loans may be granted to them at employee rates to meet normal credit needs. However, the credit criteria for the granting of such loans shall be the standard criteria for loans to regular SNB customers.

Responsibility of Associates, Officers and Directors

Treatment of Employees

SNB's policy is that the workplace should be free of harassment and discrimination based on race, color, religion, sex, national origin, age, or any other basis provided by law.

Specifically, all forms of harassment are prohibited by this company and it is against the law. Everyone associated with the bank should be aware of the following:

- what harassment is;
- what steps to take if harassment occurs; and
- no retaliation for reporting what is believed to be harassment is allowed.

Please refer to the Sexual and Other Forms of Harassment section of the Associates Handbook, which provides details on the bank's policy on Sexual Harassment.

Outside Activities

Participation by associates in civic, cultural, religious and charitable activities is encouraged.

Associates should not have outside interests that materially encroach on the time or attention which should be devoted to their duties, adversely affect the quality of work performed, compete with the activities of the bank, imply sponsorship or support of SNB on behalf of the outside employment or organization or adversely affect the reputation of SNB.

It is important for every citizen to take an active interest in the political and governmental process. Associates are encouraged to keep themselves well informed concerning political issues and candidates and to take an active interest

in all such matters. In all cases, associates participating in political and civic activities do so as individuals and not as representatives of SNB. In addition, campaigning for oneself or for other candidates should not impair the associate's time commitment to performing their job. Associates may hold part-time elected positions with management approval if such positions do not conflict with the performance of their jobs.

Approval from the Executive Officer is required prior to an associate accepting any fiduciary responsibility for any firm, corporation or person (other than a member of the employee's immediate family). The Executive Officer would need prior approval from the Board of Directors.

Prior approval of speeches or articles is required if the material reflects, discusses or discloses company policy, in which case the material should be reviewed and approved by the Senior Executive Officer and/or the Chief Executive Officer or his designee.

No associate may use his or her position with SNB to advance personal business or financial interest. All potential conflicts of interest, including those in which an associate has been inadvertently placed because of business or personal relationships with customers, suppliers or competitors, should be reported immediately to an Executive Officer. Their Executive Officer shall maintain a record of such report for the protection of SNB and the associate.

Other Employment

SNB's policy on other employment follows the general guidelines involving outside activities which basically prohibits outside employment that conflict with an associate's duties and responsibilities to the bank. Although outside employment is not encouraged, management may grant an associate approval prior to undertaking outside employment on a case by case basis.

Membership on Boards of Directors of Other Organizations

From time to time associates of SNB are privileged to serve on public and quasi-public organizations - such as housing or industrial development authorities. This service is beneficial to our reputation, is beneficial to our business and, more importantly, is beneficial to the public interest involved. It is our policy to support such activities.

Occasionally, however, the interests of those public bodies and of SNB become involved with one another, as for example, when the public body seeks bank financing. Under such circumstances SNB should be available as sources of credit and other financial services on an objective, competitive basis. To avoid any appearance of a conflict, however, the associate should not participate in

negotiating or consummating the transaction with respect to either party, and the records of other parties should clearly reflect that abstinence. Associates should be vigilant to avoid any conflict that could arise by membership in such organizations.

Additionally, associates of SNB should not serve on the Board of Directors of a profit making organization unless they have received the prior written consent of the Executive Officer. The Executive Officer would need prior written consent of the Senior Executive Officer and/or the Board of Directors in order to serve on the Board of Directors of a profit making organization.

Finally, an Officer of account should not serve on the Board of Directors of his or her customer without the prior written consent of an Executive Officer.

Speeches, Teaching Activities

It is entirely appropriate that associates represent the bank by giving speeches, making presentations or teaching. In many cases the organization involved will pay expenses. If, however, the bank is to bear the expenses for such an activity, then the employee should secure the permission of their department manager before accepting such an engagement.

If teaching or speaking activities are undertaken as a representative of the bank, associates should make their Executive Officer aware of these activities in advance. Associates should not request honoraria or payment if the service is provided on company time. If, however, an honorarium or payment is made, associates may accept it.

Appropriation of Business Opportunities

No associate shall take for himself or give to another, an opportunity which belongs to SNB. This would violate the associate's duty of loyalty to the Bank. Whenever the bank has been seeking a particular business opportunity, or the opportunity has been offered to it, SNB funds or personnel have been used in developing the opportunity, the opportunity shall rightfully be that of SNB.

Personal Finances

Associates are expected to maintain their personal financial affairs in a manner which will favorably reflect on the reputation of SNB. Associates that experience problems in maintaining their bank accounts or personal finances in good standing should make their manager aware of these difficulties, and seek assistance from the appropriate Bank Officer(s) who may be able to guide decision making or create solutions that would correct the problem. Bank Officers, who experience financial

problems and are in positions to advise customers in their financial matters and/or manage customer accounts through their assigned authorities, are required to notify their Executive Officer of their problems and action plans to resolve these issues. Financial problems that would create operational and/or financial risk to the Bank, or reputation risk with Bank customers are to be raised to the Chief Talent Officer for review. Any exceptions to this policy, where circumstances are out of the employees control and any risk can be mitigated, can be approved by the Executive Officer.

Associates shall maintain their personal accounts responsibly and keep them in good standing. Associates shall not process any transactions or account maintenance on their own personal accounts, or on the accounts of immediate family members.

Associates shall not invest for themselves or members of their immediate family, in the stock or business of a customer, unless such investment has been approved by an Executive Officer. Participation in partnerships, joint ventures or other joint business enterprises in which an SNB customer is a general partner also requires the prior approval of an Executive Officer.

Each major policy-making officer of SNB is required to be familiar with the reporting requirements of Regulation "O" and with reporting requirements with respect to outside business interests.

Purchase of SNB Property

Associates and their immediate families, whether acting individually or in a fiduciary capacity, are not permitted to sell assets or to purchase assets from SNB or any trust account being administered by SNB, unless such sale or purchase has been approved in advance by the Executive Officer, or unless such assets are being offered at public sale or public auction, or the purchase or sale has been approved by a court having jurisdiction over the transaction. Sale or purchase of SNB assets by the Executive Officer requires prior approval by the Chief Executive Officer and/or the Board of Directors.

False or Misleading Remarks

False malicious or misleading remarks must not be made about vendors, customers, competitors or others associated with the bank. False statements regarding the banks financial condition is strictly prohibited. False, misleading or incomplete statements to auditors, examiners or other investigators are considered the same as falsification of records.

Corporate Information Security

Information about SNB's business operations is a valuable company asset. Great care must be exercised to ensure that such information is safe, confidential and accessible only to authorized users. It is the responsibility of all associates of the bank to protect the confidentiality of the bank's, customers' and vendors' financial, technical and other trade secret information. Financial, personal and other sensitive information about current or former customers and individuals associated with the bank should receive the same care and security as funds or valuable physical property. (see Information Security & Technology Program Policy)

All individuals associated with SNB must not use their positions to obtain information or services for unauthorized purposes. Those who knowingly access, disclose, modify, copy or destroy bank or other protected information without prior approval or for improper purposes are in violation of the bank's information security policies.

The Customer Financial Records Privacy Policy provides details on the policy and procedures on safeguarding customer data.

Internet E-Mail

The internet is a portal to a vast audience. Communications on the Internet, whether directly or indirectly, can influence the public's attitude toward SNB. E-mail on the internet should be considered a public, visible postcard, without any security. Therefore, only correspondence suitable for review by the public may be distributed outside SNB via e-mail on the internet. Usage of internet e-mail through the bank is restricted to work-related functions. Questions about internet security should be addressed to the Chief Risk Officer or the Compliance Risk Manager. (see Social Media Policy; Information Security & Technology Program Policy)

Accounting, Record keeping and Investigation

SNB complies with the relevant accounting, record keeping and internal control requirements of the Securities and Exchange Act of 1934, as amended; the Foreign Corrupt Practices Act of 1977; the financial reporting requirements of generally accepted accounting principles and regulatory requirements. The bank is required to maintain books and records that accurately and fairly reflect, in reasonable detail, transactions and dispositions of assets.

To assure the integrity of the bank's accounting records, all entries to the company's books must be prepared with care and must be supported by adequate documentation to provide a complete, accurate and auditable, record of transactions they describe. Associates are responsible for implementing SNB's accounting, record keeping and internal control policies.

Bank policy prohibits any arrangement that results in making knowingly false or misleading entries in company books or records. Under no circumstances should funds, assets or liabilities of the organization be concealed or hidden. Associates having information or knowledge of any unrecorded or miss-recorded funds, assets or liabilities or any prohibited act must promptly report the activity to the Chief Risk Officer.

Use of SNB Name

Unless authorized by Executive Management, no associate shall, through activities, statements or otherwise represent or imply SNB sponsorship or approval of any political, social, religious or business activity or cause.

Internal Disclosure of SNB Activities

Each associate must ensure that the established procedures for reporting activities concerning the business of SNB are followed so that the Chief Executive Officer and/or the Chief Risk Officer will be aware at all times of all material matters pertaining to or impacting the operation of the bank. Additionally, each associate is obligated to see that the necessary information concerning any activity within the organization reaches the appropriate level, and exceptions to policy as well as management overrides are properly approved and reported.

Social Networking Policy

Seacoast National Bank takes no position on your decision to start or maintain a blog or participate in other social networking activities. However, it is the right and duty of the company to protect itself from unauthorized disclosure of information concerning the Bank. Seacoast National Bank's social networking policy includes rules and guidelines for company-authorized social networking and personal social networking and applies to all executive officers, board members, management and associates.

Definition

For the purposes of this discussion and these policies, social media are online tools used to publish and discuss user content with others. Included are Social networks (i.e. Facebook, LinkedIn, Twitter), blogs (i.e. BankRate), forums (i.e. Yahoo Finance), Multimedia sites (i.e. You Tube, Flickr, Photobucket), Q & A sites (i.e. Yahoo! Answers), review sites, communities, social classified sites (i.e. Craigslist) and internal media too.

Technology changes quickly, so the aforementioned list is meant to be representative, but by no means all inclusive. When reading the policies and procedures below, they apply to all forms of online social communication.

The internet is a public channel and acts as a conduit to the public at large, which is why our online presence will be carefully monitored and managed.

Social media is a valuable tool that can help to engage customers, prospects and community partners and educate the public about company news, community events and initiatives.

All individual and/or departments that have a business need to develop and maintain a company sponsored social media site or presence must submit a request to the Marketing department for approval.

General Provisions

Unless specifically instructed, employees are not authorized and may not speak on behalf of Seacoast National Bank or attribute any personal statement to the bank. Employees may not publicly discuss clients, products, employees or any work-related matters, whether confidential or not. Employees are expected to protect the privacy of Seacoast National Bank, its employees and clients and are prohibited from disclosing personal employee and non-employee information and any other proprietary and nonpublic information to which employees have access. Such information includes but is not limited to customer information, trade secrets, financial information and strategic business plans. Employee are expressly prohibited from engaging in any harassing, threatening, and/or otherwise inappropriate behavior that impacts the bank's business reputation, confidential information, employees and/or customers while using any social media sites.

Promotion or mention of specific types of bank products and services must be preapproved by both the Marketing and Compliance departments.

Authorized Social Networking

The goal of authorized and permissible social networking and blogging is to become a part of the industry conversation and promote web-based sharing of ideas and exchange information. Authorized social networking and blogging is used to convey information about company products and services, promote and raise awareness of the Seacoast National Bank brand, search for potential new markets, communicate with employees and customers to “brainstorm”, issues or respond to breaking news or negative publicity, and discuss corporate, business-unit and department-specific activities and events.

When social networking, blogging or using other forms of web-based forums, Seacoast National Bank must ensure that use of these communications maintain our brand identity, integrity and reputation while minimizing actual or potential legal risks, whether used inside or outside of the workplace.

Employer Monitoring

Employees are cautioned that they should have no expectation of privacy while using the Internet. Your postings-can be reviewed by anyone, including Seacoast National Bank. Seacoast National Bank reserves to right to monitor comments or discussions about the company, its employees, clients and the industry, including products and competitors, posted on the Internet by anyone, including employees and non-employees. Seacoast National Bank uses blog-search tools and software to monitor forums such as blogs and other types of personal journals, diaries, personal and business discussion forums, and social networking sites.

Employees are also cautioned that they have no expectation of privacy while using company equipment, computers, phones or facilities for any purpose, including authorized blogging. Such devices may be monitored by the Bank.

Seacoast National Bank reserves the right to use content management tools to monitor, review or block content on company blogs that violate company blogging rules and guidelines.

Responding to Social Media questions, complaints or comments regarding Seacoast National Bank.

The following rules and guidelines apply to social networking and blogging when authorized by the employer and done on company time. The rules and guidelines apply to all employer-related blogs and social networking entries, including employer subsidiaries or affiliates. This includes Officers designated by the CEO, Chief Risk Officer and /or Chief Marketing Officer to serve as a spokesperson to a specific subject or inquiry.

Only authorized employees can prepare and modify content for Seacoast National Bank's social media sites, intranet site and websites. Entries. Content must be relevant, add value and meet at least one of the specific goals or purposes developed by Seacoast National Bank.

All employees must identify themselves as employees of Seacoast National Bank when posting comments or responses on the employer's blog or on the social networking site. **Under no circumstances should an employee ever post on anything involving Seacoast National Bank posing as a non-employee.**

Any copyrighted information (logos and trademarks) where written reprinted information has not been obtained in advance cannot be posted on Seacoast National Bank's social sites or website.

Business units and departments are responsible for ensuring all blogging and social networking information complies with Seacoast National Bank's written policies. Department managers are authorized to remove any content that does not meet the rules and guidelines of this policy or may be illegal or offensive. Removal of such content will be done without permission of the blogger or advance warning.

Seacoast National Bank expects all guest bloggers to abide by all rules and guidelines of this policy. Company reserves the right to remove, without advance notice or permission, all guest bloggers' content considered inaccurate or offensive. Seacoast National Bank also reserves the right to take legal action against guests who engage in prohibited or unlawful conduct.

Social Media Response Procedures

All responses on behalf of Seacoast National Bank will be approved by the Marketing department in partnership with our agency, our compliance area and the areas involved in the discussion topic. Pre-positioned responses will be developed for common discussion topics.

Responses will be timely,

All responses on behalf of Seacoast National Bank will be transparent, concise and helpful. Negative comments should not be engaged online, but whenever possible dealt with directly with the poster offline.

Any comments or questions involving customer service issues or specific account information should be referred to the telephone banking center or other specific appropriate division if discernible from the post.

Individuals who are registered or affiliated with a Securities Broker-Dealer or Registered investment Advisor, or who hold an Insurance License, are

prohibited from using any social media sites for business purposes. Specifically included in this prohibition is any use of, or participation in, interactive content social networks (including; Blog posts, Tweets, Facebook status updates, LinkedIn updates, Comments, instant messaging and Webinars). Any reference to employment by any dual employee of a Seacoast affiliated Registered Broker-Dealer or Registered Investment Advisor within personal use social networking profiles must be updated to reflect the employer as only Seacoast National Bank. There may not be any reference to the dual-employee status as a Registered Broker-Dealer or Registered Investment Advisor.

Personal Blogs

Employees are expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as the employee:

- Seacoast National Bank respects the right of employees to use blogs and social networking sites as a medium of self-expression and public conversation and does not discriminate against employees who use these media for personal interests and affiliations or other lawful purposes.
- Bloggers and commenters are personally responsible for their commentary on blogs and social networking sites. Bloggers and commenter's can be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous by any offended party, not just Seacoast National Bank.
- Employees cannot use employer-owned equipment, including computers, company-licensed software or other electronic equipment, or facilities on company time, to conduct personal blogging or social networking activities. This activity should be done off hours and off site.
- Employees cannot use blogs or social networking sites to harass, threaten, discriminate or maliciously disparage any Bank employees or anyone associated with or doing business with Seacoast National Bank.
- If employees choose to identify themselves as a Seacoast National Bank employee, please understand that some readers may view you as a spokesperson for Seacoast National Bank. Because of this possibility, we ask that you state that your views expressed in your blog or social networking area are your own and not those of the company, nor any person or organization affiliated or doing business with Seacoast National Bank.
- Employees cannot post on personal blogs or other sites the name, trademark or logo of Seacoast National Bank or any business with a

connection to Seacoast National Bank. Employees cannot post company-privileged information, including copyrighted information or company-issued documents.

- Employees cannot post on personal blogs or social networking sites photographs of other employees, clients, vendors or suppliers, nor can employees post photographs of persons engaged in company business or at company events.
- Employees cannot post on personal blogs and social networking sites any advertisements or photographs of company products, nor sell company products and services.
- Employees cannot link from a personal blog or social networking site to Seacoast National Bank's internal or external web site.
- If contacted by the media or press about their post that relates to Seacoast National Bank business, employees are required to speak with their manager first. Any response to the media will be approved by the Executive Officer and Marketing Director, both in terms of approving the need to respond and the content of the response.
- If you have questions relating to this policy, your personal blog or social networking, ask your manager or supervisor.

Reporting Violations

All Seacoast National Bank employees are responsible for reporting any violations or possible or perceived violations to supervisors, managers or the HR department. Violations include improper discussions of Seacoast National Bank and its employees and clients, any discussion of proprietary information and any unlawful activity related to blogging or social networking.

Discipline for Violations

Seacoast National Bank investigates and responds to *all* reports of violations of the social networking policy and other related policies. Violation of the company's social networking policy, as part of the Bank's code of conduct, will result in disciplinary action up to and including termination. Discipline or termination will be determined based on the nature, severity and other relevant factors of any blog or social networking posted. Seacoast National Bank reserves the right to take legal action where necessary against employees who engage in prohibited or unlawful conduct.

Relationship With The Community

The following provisions of the code cover general guidelines on some of the more significant laws and regulations which SNB strongly adheres to in its relationship with the community.

Compliance with Laws

SNB and its associates will comply with all applicable laws, rules and regulations. In instances where the proper and ethical course of action is unclear, counsel from attorneys and others will be sought. In no instance shall anyone engage in a course of action which, if it were made public, would be of embarrassment to SNB. The integrity of each staff member is of utmost importance.

Americans with Disabilities Act

SNB is committed to serving the needs of all customers and employees and fully supports compliance with the Americans with Disabilities Act (ADA). The goals and objectives of the ADA enhance the quality of our society and strengthen the American economy through businesses reaching out to and including all segments of the population.

Although even the best efforts of the business community will not remove every barrier faced by all people with disabilities, meaningful efforts to do so will offer many more opportunities to participate fully in the economic and social mainstream.

Any concerns in this area may be directed towards the Chief Talent Officer or the Compliance Risk Officer for further information.

Affirmative Action Policy: Fair Lending and Equal Employment

In accordance with SNB's Loan Policy, all credit decisions are to be made without regard to race, color, national origin, religion, sex, age, marital status, sexual orientation, disability, or any other factors prohibited by law. This commitment is fulfilled while maintaining prudent credit discipline and achieving acceptable return for the shareholders.

SNB recognizes that affirmative steps must be taken to ensure that this principle is applied consistently and continuously throughout all aspects of our credit operation, including product design, marketing and advertising, underwriting, appraisal, training, compensation and performance evaluation. Procedures have

been established to ensure that bank wide operations reflect SNB's commitment to fair lending and that employees are duly informed of this commitment.

An essential element in building a diverse, inclusive environment is the bank's equal employment opportunity policy. It prohibits discrimination and harassment in all business activities on the same basis as its fair lending policy. Details of the bank's policy on equal employment are discussed in the Associates Handbook.

SNB believes that diversity in perspective, experiences and ideas brings strength. Fostering an environment that recognizes and respects differences has a direct effect on the bottom line; it motivates people, promotes innovation, encourages risk-taking, creates additional revenue opportunities, and increases productivity; all of which link to the company's business goals. Through diversity, the bank is able to better understand and meet the business needs of its customers in an increasingly diverse world.

Purchase of Favored Treatment/Political Contributions

The intent of the Anti-Kickback Act of 1986 is to eliminate the use of kickbacks or other fees or benefits by or between contractors or subcontractors or their employees in connection with the award or performance of contracts and subcontracts involving the federal government. In the same light, bank policy prohibits offering, giving, soliciting or accepting bribes, kickbacks, extraordinary commissions, or other things of value for the purchase of favored treatment or regard of favored treatment by governments, other businesses or individuals.

Fees or commissions must be paid only for clearly stated business purposes. Hospitality of meals, business meetings and social events may be extended by bank employees if it is appropriate to the situation and would not compromise the company, the employee or the recipient.

Political Contributions

Federal law prohibits all corporations from making federal political contributions and prohibits national banks from making contributions to federal, state or local candidates for election. In addition, various state laws further limit the ability of corporations to make political contributions. Where lawful, the company may make contributions concerning civic or governmental issues in which the company has a particular interest only after receiving both an opinion of legal counsel that the contribution is lawful and the prior approval of the Chief Executive Officer or the Chief Risk Officer.

Selection of Vendors

The services of brokers, dealers, lawyers, consultants and other professionals are to be chosen on the basis of qualifications, quality, price and benefit to SNB, and not merely on personal or customer relationships. Accordingly, the use of family members and relatives to perform services for the company without prior management approval is prohibited

Bribes

It is SNB's policy to fully comply with the anti-bribery provisions of the Foreign Corrupt Practices Act which makes it a criminal offense for any U. S. enterprise to offer a bribe to a foreign official, foreign political party, party official or candidate for political office for the purpose of obtaining, retaining or directing business to any person, whether or not that person is the one making the bribe. A bribe may take the form of an offer, payment, promise to pay or authorization of the payment of money or anything of value.

Antitrust Consideration

Activities that violate or appear to violate antitrust laws must be avoided. Tie-ins and exclusive dealings involving bank and non-bank products need to be carefully reviewed with Executive Management and the Compliance Risk Officer to prevent violations of the anti-tying laws and regulations for national banks. Also, antitrust laws prohibit discussing rates, costs and market information with competitors or making arrangements with them that affect prices, services or other competitive policies and procedures.

Community Reinvestment Act

Corporate responsibility to its communities has been an integral part of SNB's business. The bank's commitment is a strategic, integrated effort that involves business units throughout the organization. A significant amount of time and effort is spent assessing the composition and needs of the bank's community, particularly those in the low to moderate income levels.

In addition, SNB, and its associates, actively participates in a variety of socio-civic organizations that give back to the community.

SNB's long-term goal is to enrich the quality of life in the communities where it does business and build relationships of value by providing economic opportunities.

Environmental Commitment

The protection and enhancement of the environment is a responsibility shared by individuals, institutions, governments and the private sector. SNB is committed to weighing environmental considerations in its business decisions and striving to integrate the environmental and economic concerns of its constituents. SNB seeks to conduct business in a manner consistent with its environmental principles. These principles are designed to bring an environmental ethic to various areas of the organization - recycling, real estate management, and different forms of community involvement.

Relationship With Bank Regulators

In order to merit the confidence of the public and of those agencies which regulate SNB, there must be complete candor in our dealings with the regulatory agencies. Each associate must respond completely and accurately to all questions by the regulatory agencies, the bank's outside independent auditors, members of the internal audit department or any internal control/review committees. No adverse data in response to any question should be concealed.

Administration of Code

Compliance Guidance

If an individual is unsure whether a situation or certain conduct may constitute a violation of this code, the Chief Executive Officer and/or the Chief Risk Officer and/or an Executive Officer should be consulted for guidance. Additionally, the Chief Talent Officer or the Compliance Risk Officer may also be consulted.

Penalties for Non-compliance

Violations of this code are grounds for disciplinary action up to and including termination, even for a first time offense.

Reporting Unethical Practices and Possible Crimes

Associates are encouraged to report, without fear of reprisal, suspected illegal or unethical activities. Under federal law, any company can be held criminally liable when one of its employees, directors or agents commits a crime. Accordingly, any SNB associate who has knowledge or information about conduct by another employee, director or agent of the bank that he or she believes, in good faith

might be a crime or is unethical - whether or not the bank is victimized - must promptly report the relevant facts to any of the following who is not a party to the act: Department Manager, Executive Manager, Chief Talent Officer, Compliance Risk Officer, Chief Risk Officer, Chief Executive Officer or the Board of Directors/Chairman, Audit Committee.

Associates are, however, cautioned against making frivolous or unfounded accusations. Employees may seek additional information on this subject by contacting the Chief Talent Officer.

Any associate who is asked to perform or witness a banking transaction, recordkeeping practice, or decision making event that could be considered unethical or a violation of bank policy or procedure, is required to report this as a complaint. Such reporting will be handled with the highest confidentiality, where employees have the right to report any findings on an anonymous basis, and can do so without concern of any retaliation. The complaint must be made in writing and addressed to both of the following parties:

Maria Frias
Chief Risk Officer
Seacoast National Bank
PO Box 394
Stuart, FL 34995

Christopher Fogal
Chairman, Audit Committee
Seacoast Banking Corporation
c/o Christopher Fogal, CPA
603 N. Indian River Dr.
Suite 300
Fort Pierce, FL 34950

Complaints received by the Chief Risk Officer and Chairman of the Audit Committee will be promptly investigated and resolved.

Associates who do not feel comfortable discussing a business ethics issues with their supervisor, or the Bank's Chief Risk Officer or Audit Committee Chairman; you may call **The Network**, an independent company which provides an anonymous reporting service for hundreds of companies worldwide. This service is toll-free; 24 hours a day; 7 days a week. It's an option that is always available to associates that want to help, but prefer not to give their name.

“THE NETWORK”

Seacoast National Bank’s confidential hotline to report
accounting and auditing related complaints

1-866-908-7247

Some common examples of business conduct issues where associates are required to report the incident to their supervisor:

- Accounting and auditing irregularities
- Theft and fraud
- Conflicts of interest
- Securities matters
- Insider trading
- Destroying, altering, or falsifying company records
- Disclosure of proprietary information

Here’s what happens when you call *The Network*:

- 1) Associates are greeted by a friendly Interviewer, who documents the situation in detail. Associates don’t have to give their name and the call is not recorded.
- 2) The Interviewer assigns a report number to the associate and asks them make one call back.
- 3) The information is then relayed to the Bank’s management to investigate the concern. This information will first be received by the Chief Risk Officer.
- 4) Using the report number and scheduled call back date given to the associate by the Interviewer, the associate calls for the follow-up. You may be asked additional questions or ask to add any additional information at this time.

Why is ethical business conduct so important?

High standards are more than a slogan or catch phrase – they are a way of doing business; Seacoast banking business!

Maintaining high standards means conducting business ethically and legally. Our adherence to these standards is a key component in building a reputation for excellence and integrity.

Why care about business ethic issues?

Business conduct violations can result in serious consequences for individuals – even imprisonment under some circumstances. The Bank may also be financially penalized through lawsuits or claims, resulting in fines and/or restrictions placed on our business activities. But most importantly, associates should care because violations of business conduct make everyone a victim. The negative impact on our professional reputation can be severe, and affect our relationships with our community and customers.

How can I help maintain high standards of business conduct?

Think before you act.

Ask yourself: Is it illegal? Does it violate company standards or the Bank's Code of Conduct? Could it cause loss or harm to you, co-workers, the Bank, shareholders, customers or companies you are doing business with? Would you feel uncomfortable if everyone knew what you did?

If you answer “yes” to any of these questions, the action is very likely wrong, and you should avoid it. If the answers are not clear, don't take a chance. Talk with your supervisor immediately. When you think before you act, and make the right decision, you uphold high standards and serve as a good example for others to follow!

Speak up!

Use Peer Influence. If you see or suspect business conduct violations, don't ignore the situation. Say something to express your concern. Your influence could help prevent a friend from making a big mistake. If the situation does not improve after this; talking to your supervisors is the next step. Ignoring business conduct violations only allows for the problem to grow more costly and frustrating.

Employee Investigations

Seacoast National Bank will conduct prompt, thorough and confidential investigations when reported regarding employees who are alleged to be involved in matters dealing with violations of bank policy and procedure involving loss or possible theft of money or proprietary information, breaches in confidentiality and/or security that create liability for the bank, harassment

allegations and any matter that represent a significant violation of bank code of conduct and business ethics.

Associates who are determined to be relevant parties or witnesses in the matter under investigation are required to fully participate and offer assistance in the process. Any employee refusing to do so, or who take deliberate action to undermine the investigation, provides false information, or who breach confidentiality will be subject to disciplinary action, including termination. Exceptions to breaches in confidentiality will be granted to employees who obtain legal council during the investigation (where information can be shared with the attorney when client/attorney confidentiality priviledges exist.)

Associates who work in departments or positions with significant high risk for fraud or theft, will have periodic financial and criminal background checks performed as part of a regular security protocol for that area. Notification of these security checks to the Associate is not required. Findings of the security check will be confidential. Any finding that could be interpreted as conditions for risk of fraud or theft will be addressed with the Associate as part of the regular security audit.

Seacoast Banking Corporation of Florida

Code of Ethics for Financial Professionals

This Code of Ethics for Financial Professionals applies to the principal executive officers of Seacoast Banking Corporation of Florida (the "Company") and its reporting subsidiaries and all professionals serving in a finance, accounting, treasury, and tax or investor relations role. In addition, the Company expects all of its employees to act in accordance with the highest standards of personal and professional integrity in all aspects of their activities, to comply with all applicable laws, rules and regulations, to deter wrongdoing and abide by the Company's Code of Conduct and other policies and procedures adopted by the Company that govern the conduct of its employees. This Code of Ethics is intended to supplement the Company's Code of Conduct.

Employees in specific decision making and reporting positions are required to perform their jobs in accordance with the Code of Ethics, including:

- a. Engage in and promote honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- b. Avoid conflicts of interest and to disclose to the Board of Directors or Audit Committee of the Company any material transaction or relationship that reasonably could be expected to give rise to such a conflict;
- c. Take all reasonable measures to protect the confidentiality of non-public information about the Company or its subsidiaries and their customers obtained or created in connection with your activities, and to prevent the unauthorized disclosure of such
- d. information unless required by applicable law or regulation or legal or regulatory process;
- e. Produce full, fair, accurate, timely, and understandable disclosure in reports and documents that the Company or its subsidiaries files with, or submits to, the Securities and Exchange Commission and other regulators and in other public communications made by the Company or its subsidiaries;
- f. Comply with applicable governmental laws, rules and regulations, as well as the rules and regulations of self-regulatory organizations of which the Company or its subsidiaries is a member; and
- g. Promptly report any possible violation of this Code of Ethics to the Company's Audit Committee.

Employees are prohibited from directly or indirectly taking any action to fraudulently influence, coerce, manipulate or mislead the Company or its subsidiaries' independent public auditors for the purpose of rendering the financial statements of the Company or its subsidiaries misleading. Employees understand that they will be held accountable for their adherence to this Code of Ethics. An employee's failure to observe the terms of this Code of Ethics may result in disciplinary action, up to and including termination of employment. Violations of this Code of Ethics may also constitute violations of law and may result in civil and criminal penalties for the employee, their supervisors and/or the Company.

Any questions an employee may have regarding the best course of action in a particular situation, should promptly contact the Chairman of the Audit Committee. Employees may choose to remain anonymous in reporting any possible violation of this Code of Ethics.

Limitation on Luxury Expenditures Policy (Effective June 21, 2009)

Expenditures for excessive entertainment or events are prohibited. This includes both foreign and domestic junkets or travel that does not serve a demonstrated business purpose. Excessive entertainment or an excessive event is defined as any single occurrence or event where the per participant expenditure by the bank exceeds \$2,000. Recognized trade association conferences, conventions and training, off-site planning meetings and off-site board of directors meetings are considered a normal part of the successful operation of the bank and the company and are not considered excessive events. In addition client focused entertainment or events that do not exceed the above limit are considered an important component of our private banking program and are not considered excessive events.

Office and facility renovations should be designed to, enhance operational efficiency, comply with applicable fire codes and ADA requirements, maintain a safe, sanitary and clean working environment, enhance the public image of the organization, improve employee morale, or such other worthwhile purpose as may be identified by the organization. Office and facility renovations may be deemed excessive if the total cost of the renovation exceeds \$200 per square foot. Relocating or adding to movable worker stations, improving the air flow or temperature, altering the wall, ceiling or lighting configuration of a work or storage space, establishing a new branch office or sales office are not considered excessive by their very nature.

Excessive aviation or other transportation services expenditures are prohibited. The bank will not purchase or enter into a lease for any fixed wing aircraft, rotary-wing aircraft, watercraft, or over the road vehicle with seating for eight or more individuals without prior board approval. The uses of commercial airlines for

business related travel, and the occasional use of daily chartered aircraft when time constraints and destinations make this the more economically feasible mode of travel, are not considered excessive.

Reasonable expenditures for ordinary entertainment activities or bank events for the purpose of enhancing staff development, providing performance incentives for employees, or otherwise in the normal course of the operation of the bank are permissible and are not intended to be covered by this policy. Expenditures of this type are at the sole discretion of the chief executive officer, the president or their designees and by their nature are not considered excessive.

This luxury expenditures policy is intended to supplement the Company's Code of Conduct and corporate governance program. The Chief Executive Officer, Chief Risk Officer and/or Chief Financial Officer must ensure adherence to this policy. Any violation of this policy will be promptly reported to the Board of Directors or its designated committee.

Customer Financial Records Privacy Policy

The directors, management, and staff of Seacoast National Bank respect the privacy of every customer's personal financial information. Customers furnish sensitive information to the bank in the normal course of business, and the bank is committed to treating such information responsibly. Our customers expect privacy and security for their personal and financial affairs.

The following privacy policy summarizes the bank's practice regarding its customers' personal financial information.

Categories of Information the Bank Collects:

At Seacoast National Bank, we collect, retain, and use nonpublic personal financial information about our customers only when we believe doing so will help administer our business, provide products and services, create new products or improve existing products, services and delivery systems. In addition, the bank collects and retains information about its customers to comply with pertinent laws and regulations.

The bank collects nonpublic personal information from many sources. The majority of this type of information comes directly from customers who complete various applications and forms, for example, loan applications, deposit account applications, and requests for information about accounts or products and services.

The bank also collects nonpublic personal financial information as a result of transactions between the bank and its customers. This includes transaction information from checks, debit cards, credit cards, automated teller machine (ATM) cards, and electronic transfers (e.g., pc and internet banking or automated clearinghouse (ACH) transactions). Nonpublic personal information does not include that which the bank obtains from government records, widely distributed media, or government-mandated disclosures.

Categories of Information the Bank Discloses:

By law, the bank may disclose certain personal financial information without allowing consumers the right to opt out:

- * To companies that perform transaction processing for the bank in the following circumstances:
 - If the transaction, service, or product is requested or authorized by the consumer
 - To maintain or service a consumer's account as part of a private label credit card or other loan extension program
 - In connection with a securitization, secondary market sale (including servicing rights), or other similar transactions.
- * To companies that perform services for the bank or functions on the bank's behalf if the customers have been provided with a copy of the bank's privacy policy and the bank entered into a contractual agreement with the companies that prohibits the companies from disclosing or using the information other than to carry out the purposes for which the bank disclosed the information;
- * To protect the confidentiality or security of the bank's records pertaining to the consumer, service, product, or transaction;
- * To disclose information necessary to enforce the bank's legal or contractual rights or the rights of any other person who is engaged in the financial transaction;
- * To disclose information required in the ordinary course of banking business, such as in the settlement of claims or benefits, the confirmation of information to the consumer or the consumer's agent, and the billing, processing, or clearing of items in the normal course of business;

- * To provide information to consumer reporting agencies, insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating the bank, persons that are assessing the bank's compliance with industry standards, and the bank's attorneys, accountants, and auditors;
- * To share customer identification, transactions and account experience information with the bank's affiliates as permitted by the Fair Credit Reporting Act;
- * To the extent permissible under the Right to Financial Privacy Act, which establishes specific procedures that federal government authorities must follow when seeking customer records?
- * To comply with federal, state, or local laws, rules, and other applicable legal requirements.

Safeguarding Customer Information:

At Seacoast National Bank, we protect consumer privacy by requiring that only employees who have a business reason for knowing information have access to it. The bank has appointed its Compliance Risk Officer as the financial privacy coordinator who will be responsible for assisting management in maintaining internal processes and procedures that protect the confidentiality of customer information.

The bank has procedures in place to maintain the accuracy and completeness of customer financial information. Should the bank become aware of other personal information, such as medical information, the bank will strive to maintain the confidentiality of such information. In addition, the bank will abide by customer preferences regarding direct mail and telephone solicitations.

Bank management is responsible for maintaining security standards and procedures to help prevent unauthorized access to confidential information about customers. The bank will update and test technology on an ongoing basis to ensure the protection and integrity of customer information.

Customers will be provided with a copy of the bank's privacy policy at account opening and on an annual basis. Employees will be provided with a copy of this policy and will be trained at least annually regarding the importance of safeguarding customer information. Appropriate disciplinary action will be taken against any employee who violates the bank's privacy policy and procedures.

If the bank changes its policy or practice by, for example, adding a category of information that will be disclosed to a third party, the bank will notify existing customers and give them an appropriate time period to opt out of the disclosure.

Information Security and Technology Program Policy:

Seacoast National Bank has implemented a Privacy Program that protects customer non-public or sensitive information for our compliance with Gramm-Leach-Bliley (GLBA) Privacy Act, and has appointed the Information Security Officer as the responsible person for this program who creates, an annual Privacy Risk assessment and reports GLBA compliance efforts to the Board of Directors, annually. Employees are required to take annual training for GLBA Privacy and HR will notify you by email when the training will be conducted.

Sensitive Customer Information is defined in Seacoast Policy as:

A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. In addition, this could include any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

As an employee of Seacoast National, you will treat sensitive customer information as follows:

- Communication of sensitive customer information to other Seacoast employees or authorized Seacoast service providers is done only when there is a business need.
- You will not use email to communicate sensitive customer information or put account numbers or Social Security numbers in the text of an email. You may communicate this information in an email attachment to a @Seacoastnational email address or to an authorized service provider at their email address, with your managers approval, but you **must** encrypt the attachment to the service provider prior to sending the email.
- You agree to file and store all sensitive customer information in secure areas created for this purpose, and shred any hard copy that does not need to be retained.
- You will participate in annual Privacy training, and read and agree to abide by our Information Security Program Policy.
- You will commit your User ID and password to memory, not write it down or share it with anyone.

The purchase of all computer equipment and software must be authorized by Seacoast management and obtained, installed, configured and maintained by the Information Systems Department (ISD).

Computers, whether PCs, Laptops, IPads or terminals attached to the network are only for Bank operations with the exception that the Bank permits a

reasonable amount of personal use of e-mail. Remote access to the Seacoast network is limited to email access, unless otherwise authorized by management. Modems or other non-standard communication devices are prohibited on any Seacoast National Bank workstation connected to the internal network or for use by end users.

Downloads, or any inappropriate content from the Internet are prohibited unless specifically approved by ISD. All Internet and network activity is monitored. Avoid the following email categories, including but not limited to:

- Jokes, no matter how harmless they may seem.
- Opening or forwarding any form of a "chain" letter.
- Sexually suggestive material, particularly explicit and pornographic material that violates applicable law.
- Material that expresses or promotes discriminatory attitudes towards religion, gender, age, nationality or other groups.
- Software used for "hacking or cracking" internal or external computer systems, such as viruses, executable programs, software, screensavers, games, etc.
- Harassment or threats.
- Business activities unrelated to Seacoast National Bank.
- Messages that intentionally misrepresent the identity of the sender.
- Material that is illegal in any other way.

Abuse of E-mail, Internet and network privileges can result in disciplinary action up to and including termination. Unauthorized access to another employee's files or use of company facilities to gain unauthorized access to another company's computing facilities is prohibited and is grounds for disciplinary action up to and including termination.

All data maintained on PC's, Laptops, Ipads, Terminals etc. remains the property of the Bank and must be held in strict confidence. Each person using these devices is responsible for the confidentiality of the data and the data is to be protected from all unauthorized persons both on and off the Bank premises. **Users MUST NOT leave an area with any sensitive customer data displayed on a PC monitor or data terminal screen, nor print hard copy or store data on a USB drive unless authorized by Bank management.** Privacy of information must be protected at all times.

It is incumbent upon each user to protect their individual passwords and keep them as secure as possible. Each user should comply with the below password policies.

- Use a unique User id and password
- Change passwords every 90 days
- Make password length a minimum of eight characters
- Use numbers and letters in passwords, with at least one capital letter
- Report any possible password breaches, and reset your password
- Logout or lock terminals that are left unattended.