

New

No Changes

Minimal Changes ✓

Substantial Change



Heritage
Financial
CORPORATION

CODE OF ETHICS POLICY

INDIVIDUAL RESPONSIBLE FOR POLICY: Chief Risk Officer

LAST APPROVAL DATE: May 2025

CURRENT APPROVAL DATE: May 2026

COMMITTEE PRESENTED TO: Risk and Technology Committee

Contents (section numbers refer to the online employee handbook)	Page #
Policy Statement (3.1)	2
Corporate Accountability/Whistleblower Policy (3.2) (Separate Board Policy)	
Conflicts of Interest (3.3)	5
Insider Transactions in Company Securities (3.4)	6
Preferential Treatment in Providing Services (3.5)	7
Lending Practices (3.6)	7
Acceptance of Gifts (3.7)	7
Political Activities and Contributions (3.8)	9
Outside Employment (3.9)	9
Personal Finances (3.10)	10
Employee Accounts (3.11)	11
Personal Investment Activity (3.12)	11
Advising Customers (3.13)	12
Serving as an Individual Fiduciary (3.14)	12
Business Opportunities (3.15)	12
Purchase of Bank Assets (3.16)	12
Records and Accounts (3.17)	13
Confidential Information (3.18)	13
Confidential Information Destruction Policy (3.19)	15
Password Keys/Access Security (3.20)	16

3.1 Policy Statement

This Code of Ethics and Conduct Policy ("Code") is intended to deter wrongdoing and promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- Full, fair, accurate, timely and understandable disclosure in documents the Company files with, or submits to, the Securities and Exchange Commission (the "SEC") and in all other public communications made by the Company;
- Compliance with applicable governmental laws, rules and regulations;
- Prompt internal reporting to designated persons of violations of the Code; and
- Accountability for adherence to the Code.

Toward this end, Heritage Financial Corporation and its subsidiaries and affiliates (collectively referred to as the "Company") will seek to operate in accordance with the following principles:

- Conduct its business with integrity;
- Conduct its business with due skill, care and diligence;
- Take reasonable care to organize and control its affairs responsibly and effectively, with adequate systems to promote ethical conduct and compliance with the law, to prevent and detect criminal or unethical conduct, and to manage risks as they arise;
- Pay due regard to the interests of its customers and treat them fairly;
- Avoid, and, where appropriate, address any conflicts of interest in an equitable and appropriate manner, between itself and its directors, officers and employees, between itself and its customers, and between a customer and another client;

- Take reasonable care to ensure that directors, officers and employees are adequately trained and able to conduct their responsibilities including to the standards set forth in this Code, and, where appropriate, to standards specifically required by relevant regulatory and statutory codes;
- Maintain its financial records in compliance with its established accounting policies.
- Encourage prompt internal reporting to designated persons of violations of the Code, the Company's corporate policies, or the law; and
- Accept and promote accountability for adherence to the Code.

Application of the Code

The Code applies to all directors, officers and employees (sometimes collectively referred to below as "participants") of the Company. In addition, standards set out in this Code also apply to all those engaged by the Company, but who are not employees, such as contractors and those engaged through external agencies. The Code applies to all employee decisions and activities within the scope of employment, or when representing the Company in any capacity.

All participants should be familiar with the requirements of the Code apply it to their daily activities and decisions, and to seek guidance from the appropriate individuals when additional information and explanation is needed or requested. Supervising employees are expected to make every reasonable effort to ensure that their staff continues to comply with the provisions of the Code and applicable Company policies.

Obtaining Guidance

If you need additional explanation regarding a particular provision of the Code, or if you need guidance in a specific situation, including whether a potential conflict of interest may exist, please contact your immediate supervisor. If you are uncomfortable speaking to your immediate supervisor, or if you require additional guidance after having consulted with your supervisor, you are encouraged to contact either the Human Resources Department or the Chief Risk Officer.

Reporting Violations of the Code

Any known or suspected violation of the Code, including actions or failures to act, must be promptly reported to your supervisor, the Human Resources Department or the Chief Risk Officer. This includes violations or possible violations involving you or other participants under this code. Any violation of law, rule or regulation applicable to the Company and/or corporate policy is also a violation of this Code. Violations of the Code may result in disciplinary action up to and including termination.

Individuals may report known or suspected violations of the Code anonymously through the Integrity Counts link found on the Heritage Bank intranet home page or by calling the toll free number. Individuals should provide sufficient information to allow a proper investigation of their concerns in a secure and anonymous fashion.

All concerns or complaints will be promptly investigated and appropriate action taken. Results of the investigation will be documented and where appropriate results of the investigation will be reported to the Risk or Audit Committee, as appropriate, 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 absent a knowingly false report. The Company will retain a record of all concerns and complaints, and the results of its investigations, for five years.

Reporting Accounting, Internal Accounting Controls, or Auditing Matters

The Company's policy is to create records and accounts that accurately reflect the Company's financial condition and results of operations. Individuals may anonymously report known or suspected accounting, internal accounting control or auditing concerns through the Integrity Counts link found on the intranet or the toll free number. Individuals should provide sufficient information to allow a proper investigation of their concerns in a secure and anonymous fashion. Any officer or employee falsifying any books, records, or documents of the Company shall be subject to dismissal from employment and may be referred to law enforcement authorities.

Dealings with Auditors, Examiners or Members of Law Enforcement

Participants are required to fully cooperate with internal and external auditing, regulatory examination staff, or members of law enforcement. We expect all participants to honestly and openly answer all questions and respond to documentation requests. Participants are prohibited from destroying any documents that may be necessary for any investigation by a federal or state governmental agency, or the auditors. In addition, insiders may not destroy any document that is required to be kept under the Company's Record Retention Schedule.

Administration

The Board of Directors has established this Code to help foster a strong ethical climate within the Company. The Board of Directors, through the Heritage Financial Corporation Audit Committee, will at least annually review the code and provide final approval of subsequent changes to the policy.

The Human Resources Department provides new employees with employment policies electronically upon hire. The employment policies contain a section called Corporate Code of Ethics and Conduct that mirrors this policy. New employees are required to acknowledge the receipt of the policies electronically. Human Resources monitors to ensure the acknowledgement is completed.

All employees hired before July 1 are required on an annual basis, typically in September, to acknowledge electronic receipt of employment policies and the Code of Ethics, with Human Resources monitoring compliance. Periodically, the Senior Risk Officer may redistribute the Code to all existing employees, in the event that there has been a substantial modification or revision that has been approved by the Board of Directors.

Waivers

Any requests for waivers of this Code for employees who are not executive officers should be directed through your supervisor to the Company's CEO. Requests for waivers for directors and executive officers should be directed to the Heritage Financial Corporation Board of Directors

through the Corporate Secretary. Only the Heritage Financial Corporation Board of Directors may waive the applicability of this Code for a director or executive officer. Any waivers granted to directors or executive officers, including the principal accounting officer, and the reasons for granting the waiver, and any change in this Code applicable to directors and executive officers, including the principal accounting officer, must be promptly disclosed to the public as required by applicable law, regulation or listing requirements.

3.3 Conflicts of Interest

A conflict of interest is defined as an employee's involvement in outside businesses and/or activities which might either conflict with the employee's duty to the Company or adversely affect the individual's judgment in the performance of their responsibilities. Our policy prohibits employees from engaging in personal conduct that will conflict with the interests of the Company. In addition, we believe it is important to avoid even the appearance of a conflict of interest since this may damage the Company's reputation.

All employees must disclose to their manager if a relative or business associate of the employee is seeking to provide goods or services to the Company. If you are unsure whether a particular situation creates a conflict of interest, you should consult with your manager or the Bank's Chief Risk Officer.

Officers and employees are prohibited from acting on behalf of or otherwise performing any transaction, loan, or business activity involving themselves, family members, members of their household, business partners, or close personal friends. You are not to handle transactions where a personal interest might take, or appear to take, precedence over the best interests of the Bank. Nor should you handle any part of an account where you have a personal interest or serve as a signer.

"Transactions" include, but are not limited to: loans, changing any information on bank systems, cashing checks, rate changes, processing deposits or payments, approval of overdrafts, accepting checks on uncollected funds, waiving of NSF (overdraft) or late charges (*see Policy 4.4: Financial Responsibility/NSF Policy*), and waiving the requirement for financial statements or collateral documents.

Additionally, you should not sign on customer's accounts, act as deputy or co-renter of customer's safe deposit boxes, or otherwise represent customers, except when the customer is related to you by blood or marriage.

In order to avoid any potential or perceived conflicts of interest, the Company will not actively solicit or recruit accounting firm employees who are participating in an active or ongoing audit for the Company or who are known to be employed by the accounting firms currently performing audit services for the Company. All employment inquiries by employees of the accounting firm employed to perform audit services should be referred to Human Resources Management.

3.4 Insider Transactions in Company Securities (a.k.a. Insider Trading)

The federal securities laws prohibit the purchase or sale of Company securities, directly or indirectly, by any employee, or by any member of such employee's household, while the employee possesses material non-public information concerning the Company.

The Company, its employees, and third parties with knowledge of material inside information may be subject to severe penalties under federal and state securities laws for trading in the

Company's securities while aware of material inside information or disclosing this information to others who then trade in Company securities.

"Material" information includes any information that a reasonable investor would consider important in making a decision to buy, hold, or sell Company securities. Both positive and negative information can be considered material. Examples of information that the courts have held to be material are:

- A material change in annual or quarterly earnings of the Company or a change in dividends.
- A proposed material acquisition of another corporation by the Company or other merger or acquisition transactions involving the Company.
- Significant write-off of loans.
- Material change in loan loss reserves or policy for funding reserves.
- Purchase or sale of significant assets.
- Major litigation, adverse regulatory proceeding or material threat of either event.
- A significant change in management.
- A significant expansion of operations, whether geographic or otherwise, or the curtailment of current or future planned operations.

"Nonpublic" information is information which has not been disclosed to the public generally, such as through a press release to a news wire service, public report filed with the Securities and Exchange Commission (SEC), or other means of widespread dissemination.

An employee of the Company who becomes aware of any such information concerning the Company cannot legally buy or sell Company stock (unless the transaction is done pursuant to a pre-arranged trading plan in compliance with SEC Rule 10b5-1 or payroll deduction to purchase securities as part of the 401(k) Plan entered into at a time when the employee is not aware of material non-public information); or communicate such information to other persons (sometimes referred to as "tipping").

To help minimize risks of liability under the insider trading laws employees must comply with the following guidelines. You may not purchase or sell Company securities, including those securities owned within the 401(k) Plan, if:

- You have knowledge of material nonpublic information (see definition above).
- For Directors and Executive Officers, if the Company is in a blackout period. A blackout period is defined as the period beginning two weeks prior to the end of the fiscal quarter or the fiscal year end and continuing until 48 hours after the public release of the Company's earnings for such a period; and
- You have a question whether nonpublic information is material (see definition above).

You may purchase or sell Company securities pursuant to a pre-arranged trading plan in compliance with SEC Rule 10b5-1 approved by the Company and entered into at a time when you are not aware of material non-public information. You may purchase Company securities pursuant to a pre-arranged payroll deduction for investment election purposes in the 401(k) Plan.

Any employee who engages in such illegal conduct will be subject to immediate dismissal. Any director who engages in such illegal conduct may be subject to removal by the other directors and/or the stockholders. For more detail on insider trading restrictions please contact the Corporate Secretary.

For Directors and Executive Officers, please see the Heritage Financial Corporation Insider Trading Policy for Directors & Executive Officers.

3.5 Preferential Treatment in Providing Services

Every customer and employee is entitled to respect, courtesy and equality. Employees must provide the highest level of professionalism and service on a consistent and equal basis. The following are guidelines on how to avoid preferential treatment:

- Employees must avoid unlawfully favoring the interests of certain customers, suppliers, government officials, or other employees. All standard practices, policies and procedures apply to all similarly situated individuals and the general public.
- Employees must avoid giving unlawful preferential treatment to a director, employee, customer, supplier, government official, or others because of a personal relationship.
- Employees must avoid the appearance of, or actual preferential treatment for themselves, relatives, friends, business associates, or government officials.
- Employees may not be involved in Company matters regarding their own business or the business of their relatives, friends or business associates. In these situations, employees should have an unrelated employee that does not report to them handle the matter.

3.6 Lending Practices

The Bank's lending officers must use prudent lending guidelines as detailed in the Bank's Loan Policy in making loans to Bank customers. The lending officer must justify any interest rate concessions based on the borrower's creditworthiness and overall business relationship with the Bank. Lending officers may not grant direct or indirect accommodations or make credit recommendations for:

- Members of their families,
- Any individual or organization to which the officer or employee or their immediate family is indebted, or
- Any organization, which the employee or their immediate family is associated or hold a material financial interest.

We do not require that a customer purchase other services from our Bank or prohibit the customer from dealing with our competitors as a condition to obtaining a loan or other banking services from our Bank.

Bank employees may not grant any loan or gratuity to any federal or state bank examiner or employee working for the Bank's independent auditing firm.

3.7 Acceptance of Gifts

Employees and their immediate family shall not solicit, accept, or retain a personal benefit from:

- Any Bank customer,
- Any individual or organization doing or seeking to do business with the Bank, or

- Any other individual or organization based on a relationship with the Bank or Company.

A personal benefit shall include any type of gift, gratuity, favor, service, loan, legacy (except from a relative), fee, compensation, or anything of monetary value.

Certain exceptions to this general rule may be acceptable if there is not, and there appears not to be, a reasonable likelihood of improper influence on the participant's performance of their duties for the Company. The personal benefit may not exceed the value of the following:

- Normal business courtesies, such as a meal or entertainment, involving no more than ordinary amenities;
- Non-cash gifts of nominal value such as those received at holiday time or special occasions that represent expressions of friendship;
- Gifts based upon kinship, marriage, or social relationships entirely beyond and apart from any business relationship;
- Unsolicited advertising and promotional material of nominal value; and
- Awards given by charitable, educational, civic or religious organizations for meritorious contributions or service.

For the purposes of this policy, nominal value is defined as an item having a value of less than \$100.00; however, nominal gifts which, when combined, total more than \$250.00 in a twelve month period from the same customer, vendor and/or business may not be considered nominal.

Any participant receiving a personal benefit, other than for the exceptions listed above, must report the benefit to the Human Resources Department or other appropriate official. Failure to timely report such a gift is subject to disciplinary action, up to and including termination.

Bank Bribery Act (18 USC 215©)

The federal government recognizes that a serious threat to the integrity of an insured state nonmember bank occurs when its officials become involved in outside business interests or employment that gives rise to a conflict of interest. Such conflicts of interest may evolve into corrupt transactions that are covered under the bank bribery statute. The Bank Bribery Act prohibits any employee, officer, director, agent or attorney of an insured state nonmember bank from (1) soliciting for themselves or for a third party (other than the bank itself) anything of value from anyone in return for any business, service or confidential information of the bank and (2) accepting anything of value (other than bona fide salary, wages and fees referred to in 18 U.S.C. 215(c)) from anyone in connection with the business of the bank, either before or after a transaction is discussed or consummated.

Accordingly, all participants are prohibited from self-dealing or otherwise trading on their positions with the bank or accepting from one doing or seeking to do business with the bank a business opportunity not available to other persons or that is made available because of such participant's position with the bank. Therefore, the Company expects all participants to disclose all potential conflicts of interest, including those in which they have been inadvertently placed due to either business or personal relationships with customers, suppliers, business associates, or competitors of the bank.

3.8 Political Activities and Contributions

Although the Company endorses participation in community and public activities, employees may not accept candidacies for political offices without the prior approval of Human Resources Management, CEO and/or President/COO. In addition to major offices, this restriction includes council and school board memberships, municipal treasurer, and other quasi-governmental positions. Employees elected to political positions may hold such positions only if they do not violate the guidelines on outside employment (*see Policy 3.9: Outside Employment*).

Additionally, while the Company recognizes your right to become personally involved in political or social actions, opinions are not to be stated and/or mailed on Company or Bank letterhead. Nor are you to wear campaign buttons or display similar items within the Company.

Except upon express written authorization by the CEO, President/COO, or vote of the Board of Directors, no employee of the Company may act as a representative of the Company with respect to influencing the passage or defeat of any legislation by the Legislature of the State of Washington or other states, or the adoption or rejection of any rule, standard, rate or other legislative enactment of any state agency.

Contributions

The Company is prohibited from making a contribution or expenditure in any federal or state election to political office. However, the Company may choose to belong to certain banking and industry organizations for which portions of the membership fees are allocated towards lobbying on behalf of the banking industry. The Company may make a loan to a candidate for political office or a political action committee if the loan is made in the ordinary course of business and complies with the Bank's Loan Policy.

You may make personal contributions to candidates or political action committees as you so desire; however, you are prohibited from making any direct or indirect contribution of Company funds or other Company property for the election of any candidate for any political office. This prohibition includes the use of our Company's email, corporate facilities and equipment for any political activity.

3.9 Outside Employment

To adequately protect the Company's interests, you are expected to avoid working for any other person, firm, or employer where such work represents a conflict of interest or will interfere with your job responsibilities or work schedules at the Company. In those cases where an employee believes outside employment is justified, the employee should present a written request to Human Resources for prior approval. Human Resources may not approve any outside employment activity that might:

- Encroach upon regular working hours,
- Interfere with the employee's regular duties, or
- Be with a customer with whom the employee has any operational or credit responsibility.

No Officer or employee may be employed by any other financial institution or competing business (e.g. lending or investment/brokerage firm) except the holding Company.

Officers and employees may not become or continue to serve as directors of outside corporations regardless of whether the corporations are Bank customers. Human Resources Management may make an exception to this policy if there is an overriding business reason to do so. Officers and employees must obtain prior approval from Human Resources Management before accepting any offer to be a director of an outside corporation. These restrictions, however, do not apply to corporations that are closely held by the Officer's or employee's family or involve a non-profit social, civic, religious or philanthropic institution.

Real Estate Licenses

To prevent both actual conflicts of interest and the potential for the appearance of such conflicts, Heritage Bank prohibits employees from maintaining an active real estate license. If you have been a real estate agent or broker, you may retain an inactive license. New employees with an active real estate license will be given thirty (30) days from hire in which to deactivate their license.

This restriction applies without exception to employees directly involved with consumer or commercial real estate lending (including Home Loan and Commercial) as well as to any other employees who interact with Heritage Bank borrowers or deposit customers as a regular part of their jobs.

If you do not work in those areas and your job with Heritage Bank does not involve regular customer contact, you may be permitted to maintain an active real estate license for the purpose of buying and selling real estate, but only on the following conditions:

- You may not use any Heritage Bank resources for the purpose of conducting your business (such as, for example, Heritage Bank stationery, photocopy machines/scanners, or its telephone or computer system, including email.)
- No real estate business may be conducted at Heritage Bank facilities or during your work hours.
- You may not indicate to your real estate customers you are associated with Heritage Bank and may not wear Heritage Bank logo clothing when meeting with real estate customers.
- You may not indicate to Heritage Bank customers with whom you interact as an employee that you sell real estate.
- The ultimate decision of whether such an outside business is permissible rests with senior management and requires the approval of Human Resources Management.

Notwithstanding the general prohibition set forth above, you may activate the license, for a limited period, for the purpose of facilitating the purchase or sale of your personal residence (or that of an immediate family member, which would include the parent, child, or sibling of you or your spouse or domestic partner) so you may benefit from avoiding a portion of commissions in the case of the sale of your personal residence, or to allow you to pass along such savings to the family member. If you have been an agent, such temporary activation means that you can "hang" your license with a broker. If you were a broker, such temporary activation means you can establish a main office business address in which to conduct the licensed activities. In either case, once the transaction is complete, you must deactivate the license.

3.10 Personal Finances

Each employee should conduct their personal financial affairs in a responsible manner. Employees and their immediate families should borrow only from reputable organizations that regularly lend money, provided that such persons may borrow money without restriction from relatives. Borrowing from other banks and lending to employees of other banks must be free of any reciprocity regarding terms or interest rates received or given. Bank executive officers who borrow from another bank or financial institution must comply with regulatory reporting requirements. For this purpose, Bank executive officers are only those policy-making officers specifically appointed by Board Resolution.

Employees may not borrow from or extend credit to any customer or supplier of the Bank unless the customer or supplier is a recognized lending institution. Employees should not cosign, endorse, or otherwise assume liability for the borrowings of any customer or prospective customer. You should discuss any financial emergency with your immediate supervisor or Human Resources Management.

3.11 Employee Accounts

As with any customer, employee accounts and account activity are regularly monitored by external regulators/auditors as well as Internal Audit and Risk personnel. Therefore, you should have no expectations of privacy with regard to any of your account relationships at Heritage Bank. The Company reserves its right to review this information with the appropriate Bank personnel and/or outside government agencies. If suspicious or unusual activity occurs on any of your employee accounts, you may be required to provide an explanation to auditors, Human Resources and/or appropriate management personnel. Misuse of an employee account may result in corrective action up to, and including, termination of employment.

3.12 Personal Investment Activity

Participants may not engage in any investment transactions which create, or give the appearance of creating, a conflict of interest between the participant and the Bank or between the Bank and any customer. We do not believe it is possible to specifically list all of the possible conflicts of interest. However, we require that the following situations be avoided:

- Buying securities of a customer, supplier, borrower, or competitor where it may be construed as affecting the participant's judgment that is exercised on the Company's behalf;
- Investing in a company where the participant, as a representative of Heritage Financial Corporation or its subsidiaries has access to non-public information concerning the company;
- Permitting a customer to arrange investments for the account of the participant or his or her immediate family;
- Investing in customer-sponsored businesses under circumstances that might create a conflict of interest or the appearance of a conflict; and
- Making investments that parallel or anticipate investment action by the Bank.

Any named executive officer who has a margin account with a broker or dealer in securities or commodities must report that information to the Company's CEO, Corporate Secretary or other appropriate official.

If the Company enters into discussions to acquire a target company (including, but not limited to, any bank, savings bank, holding company or other type of entity), all Heritage participants

aware of the transaction have an obligation to disclose as soon as possible their respective investment in such target company.

3.13 Advising Customers

You are expected to exercise care in discussing transactions with customers since the Bank may not practice law or give legal or tax advice. Consequently, you must not say anything that may be interpreted as legal or tax advice.

You should avoid specifically recommending any one individual or firm if a customer asks for advice regarding professional services, including attorneys, accountants, insurance agents, etc.

You must observe fair and ethical conduct in dealing with our competitors. We believe it is inappropriate and unethical for our employees to make disparaging remarks concerning our competitors. Our strategy is to emphasize the quality and competence of our directors, officers, and employees in soliciting new customers. In addition, you are prohibited from working with competitors to set or control interest rates, prices or marketing practices.

Bank employees cannot personally earn fees from arranging third party transactions.

If you speak a foreign language, you may choose to update your language preferences on the intranet directory, offering to assist customers with interpretation in a general context. Being bilingual does not always translate into professional translation services. It may work in a general context, but in the financial industry it is important to remember proper translation can require certain specialization. Review the Foreign Language Guidance document for guidelines and what to avoid.

3.14 Serving as an Individual Fiduciary

Employees must request prior approval from the Bank's CEO or other appropriate official before accepting an appointment as a fiduciary or a co-fiduciary for a customer's account. The only exception to this rule is that an employee may serve as a fiduciary for a member of their immediate family without obtaining prior approval of the CEO or other appropriate official. Employees may not receive a fee for acting as a co-fiduciary with the Bank unless specific prior approval is received.

You should not sign on customer's accounts, act as deputy or co-renter of customer's safe deposit boxes, or otherwise represent customers, except when the customer is related to you by blood or marriage.

3.15 Business Opportunities

You may not acquire or derive personal gain or profit from any business opportunity or investment that comes to your attention as a result of employment or association with Heritage Financial Corporation or Heritage Bank. You may not take or divert business opportunities to yourself or others that rightfully belong to the Company, without first disclosing to the Company all relevant facts pertaining to the opportunity. The opportunity rightfully belongs to the Company or its subsidiaries in any case where the Company or its subsidiaries have been seeking a particular business opportunity, or in any case in which the Company might reasonably be expected to participate (such as referral fees, etc.).

3.16 Purchase of Bank Assets

Whether acting individually or in a fiduciary capacity, you are not permitted to sell or purchase assets to or from the Bank or any estate being administered by the Bank without obtaining prior approval of the Bank's CEO or CFO. You are not required to obtain prior approval for purchase of any assets the Bank is selling at a public sale or auction.

3.17 Records and Accounts

All Company records shall be maintained in accordance with the Company Accounting procedures and with other applicable accounting policies, procedures and controls. All transactions shall be recorded timely, accurately, completely, and truthfully. Company policies are intended to promote full, fair, accurate, timely and understandable disclosure in reports and documents filed with or submitted to the SEC and in the Company's other public statements. Efforts by any employee to conceal or distort information will be considered unacceptable conduct. No undisclosed or unrecorded corporate funds or assets shall be established for any purpose. No payments from corporate funds or other assets shall be approved or be made with the intention or understanding that any part of such payment will be used for any purpose other than that described by the documents supporting the payment.

Embezzlement, misappropriation of funds or property, or the falsification of any record, account or document may result in immediate dismissal and will be referred to the appropriate law enforcement agencies.

3.18 Confidential Information

All client data and much of Heritage Bank's internal data is considered confidential. Never access confidential data (including account numbers, Social Security numbers, HIPAA data, driver's license, credit card, Bank or other account numbers, etc.) without a valid business reason. See below for further details.

Confidential Customer Information

We believe it is essential to safeguard the confidential nature of customer financial information to maintain our Bank's reputation and the trust of the general public. Our policy is that customers' confidential information acquired by any employee as a result of their activities on the Bank's behalf must be held in the strictest confidence.

Employees using a Bank-issued, or their personal, laptop which contains confidential customer and/or Bank information must follow all standard security measures such as password protection and/or encryption of the confidential information. Failure to properly protect confidential information, especially if the laptop is lost, stolen or left where unauthorized access could occur, will result in corrective action up to, and including, termination of employment.

Confidential information includes account balances and credit extensions, the financial condition of a customer, and the anticipated changes in management or in the conduct of the affairs of a business customer. An employee may only use this information for Bank-related purposes and not for personal gain.

Do not use client data for development (including AI), testing, training presentations or any purpose. Properly sanitized data that cannot be traced to a client, client employee or customer may be used for testing and similar purposes. Any situation that requires the use of client data

for non-client specific development or testing requires the express approval of Heritage Bank's CEO.

You may not discuss confidential customer information with anyone outside the Bank. In addition, you may only discuss confidential customer information with employees that have a legitimate business need to know. You should refrain from sending confidential customer information via text message or other unsecured lines of communication, including unencrypted email.

If contacted by another employee to provide confidential customer information over the phone, you must request the Security Code of the Day, located on the Bank's Intranet home page. The Security Code of the Day must **always** be provided by the person requesting the confidential information, and never by the person to whom the request is being made. Immediately report all social engineering attempts to your manager or the Information Security department.

You may only release information regarding a customer to private persons, organizations, or governmental entities with the customer's written consent or appropriate legal process, such as a subpoena or court order. The Bank's CEO or Human Resources Management is responsible for reviewing any request for such information.

Employees who gain unauthorized access to other employees' salaries or private financial data (including accessing employee accounts or loan information without a business reason to do so) will be subject to corrective action up to, and including, termination of employment.

Notice of Immunity pursuant to the Defend Trade Secrets Act of 2016

An individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that is made: 1) in confidence to a federal, state, or local government official, either directly or indirectly, solely for the purpose of reporting or investigating a suspected violation of law; 2) in confidence to an attorney, solely for the purpose of reporting or investigating a suspected violation of law; or 3) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. Furthermore, an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual: 1) files any document containing the trade secret under seal; and 2) does not disclose the trade secret except pursuant to court order.

Annual Customer Information Security training is provided to all employees.

Confidential Business Information

Confidential business information may include details regarding operations and finances, audit and or regulatory exam results, information obtained from regulatory bodies (such as the FDIC or SEC), merger and/or acquisition targets or plans, business opportunities customer identities and accounts, computer programs and systems, employees, policy and procedure manuals, and other proprietary information.

You may not release financial or other information regarding the Company to any outside person or organization unless it has been published in reports to stockholders or otherwise made available to the public through authorized news releases, SEC filings or regulatory reports.

You are prohibited from attempting to obtain confidential information from Bank systems or departments for which you have not received appropriate authorization.

You are prohibited from taking photographs, videos, or recordings of Bank employees, equipment, information, or premises without specific approval from your manager and the Risk Department.

Nothing in this policy is intended to interfere with employees' rights under Section 7 of the National Labor Relations Act. Furthermore, nothing in this policy prevents employees from disclosing or discussing conduct, including conduct as defined by RCW 49.44 et seq. and the Oregon Workplace Fairness Act, that they reasonably believe, under federal, state, or common law, constitutes a violation of a clear mandate of public policy, discrimination, harassment, retaliation, or a wage or hour infraction.

3.19 Confidential Information Destruction Policy

You have a responsibility to protect the Bank's and customers' personal and confidential information and abide by the specific laws that govern the release and disposal of confidential information. You can mitigate the risk of confidential information falling into the wrong hands through careful handling and disposal of confidential materials.

Garbage/Trash

Garbage/Trash is anything not of a confidential nature, such as newspapers, magazines, fliers, junk mail, cans, plastics, food, gum, liquids, rubber bands and staples. Dispose of garbage/trash in a regular wastebasket or recycling container; garbage/trash should not be included in shred receptacles.

Confidential Materials

The following documents must be shredded:

- Documents such as internal reports, lists, screen-prints, voided transaction slips or receipts, or loan documents that contain customer information such as name, social security number and any other personal identification information, account number and/or balances.
- Any document that contains confidential bank information, such as lists of employees, emergency contact lists, phone lists, employee information, internal reports, e-mails, Company financial statements and reports.
- Any document which contains confidential employee information including, but not limited to: social security numbers, home addresses, phone numbers and medical information (such as doctor's notes and requests for leave).

Disposal Methods

Janitorial staff will dispose of garbage/trash. You are responsible for emptying the shred bin at your workstation daily into the large locking shred receptacle available at your location. The janitors will not dump these containers. If you haven't been issued a shred bin, clearly mark a wastebasket or box as "Shred – Do not empty". In the event your shred bin is not emptied daily, it must be secured in a locked office, vault, or cabinet until such time that it can be emptied into the larger locking receptacle.

"Teller garbage" should be placed into the employee's shred bin and emptied into a locking shred receptacle daily. If an employee has a cash offage that warrants further research, all teller garbage is retained in a secure location (i.e. locked inside the vault) until the completion of the investigation. "Teller Garbage" refers specifically to any item containing confidential information that is prepared by an employee related to balancing activities or transactions.

The large shred receptacles are periodically emptied into mobile shred trucks. A bank employee is required to accompany the driver to the truck to verify the destruction of materials, verify that no materials are left in the parking lot, sidewalk or street, and to sign the destruction certificate. Signed destruction certificates should be sent to the Accounting Department.

Microfilm, fiche, disks, and plastic customer deposit bags are to be destroyed by incineration by contacting the appropriate waste disposal service provider.

3.20 Password/Keys/Access Security

Heritage Bank recognizes the importance of accountability and the protection of data stored in the Bank's various systems. Authority to use a system is determined by your job title and/or job description; access is assigned on a need to know and need to use basis. For these reasons, employees must keep user passwords in strict confidence. Asking for someone's password, and/or allowing someone else to know and/or use your password may be grounds for corrective action up to, and including, termination of employment.

Your network password is to be a minimum of fifteen (15) characters, must contain at least 1 blank space (not at the beginning or end of password), and must not begin with the words "A", "An", or "The". The IT Security team may request random third party password audits, and if the third party is able to crack your password, you will be required to change it. You are required to lock or log off your computer when leaving it unattended. Employees are responsible for any unauthorized transactions performed under their password.

All doors into secured work areas must be locked. Keys, building access cards, and access codes are assigned as necessary for entry into buildings. It is the responsibility of the employee to whom they are assigned to ensure keys and codes are kept secure and confidential. Keys or access codes that have been compromised or lost must be reported to your direct supervisor or Compliance. Lost or compromised keys or access codes may be grounds for corrective action up to, and including, termination of employment.

All visitors to Heritage Bank secured areas must present appropriate picture identification, sign a visitor's log, and be escorted at all times. A visitor's log entry must accurately provide the following information: visitor's name and signature, organization represented, the purpose of the visit, entrance time, exit time and sponsoring Heritage Bank manager or delegate. If you see someone in a secured Heritage Bank secured area you don't recognize, not sure who they are, or they look suspicious, every employee has the responsibility and authority to politely inquire as to the nature of that person's business and who they are there to see. However, if you are uncomfortable with approaching a stranger simply notify your supervisor ASAP and make them aware of the situation.