



2024  
CODE OF ETHICS AND  
CONDUCT:  
HOW WE DO BUSINESS

**Letter To Team Members**

Our business at Heritage Bank of Commerce and its subsidiaries (collectively, “the Company”), is built on a foundation of trust that we work hard to earn through every interaction with clients, shareholders, communities, and each other. We are committed to accepting nothing less than the highest level of integrity with honesty and accountability in all our business dealings.

The Code of Ethics and Conduct is designed to guide us to abide by our business principles, values, and standards each and every day. We encourage and empower all team members to speak up when they see something. We have zero tolerance for those who behave unethically.

We require all team members to review and acknowledge our Code of Ethics and Conduct annually to keep the expectations top of mind and as a condition of employment.

Thank you for upholding our commitment to doing what is right so we can continue to earn the trust of everyone we serve.

A handwritten signature in blue ink, appearing to read 'CJ Jones'.

Clay Jones  
President and Chief Executive Officer

# Table of Contents

## About The Code of Ethics and Conduct

- 1.0 [Core Values](#)
- 2.0 [Your Responsibility](#)
- 3.0 [Anti-Retaliation Policy](#)
- 4.0 [Prohibited Conduct and Behavior](#)
  - 4.1 [Discrimination and Harassment](#)
  - 4.2 [Threats and Violent Acts](#)
  - 4.3 [Drugs and Alcohol](#)
  - 4.4 [Falsification of Books and Records](#)
- 5.0 [Conflicts of Interest](#)
  - 5.1 [Business Dealings](#)
  - 5.2 [Outside Employment and Activities](#)
  - 5.3 [Political Contributions and Activities](#)
  - 5.4 [Serving the Community](#)
  - 5.5 [Personal Relationships](#)
- 6.0 [Protecting Proprietary and Confidential Information](#)
  - 6.1 [Safeguarding Client Information](#)
  - 6.2 [Safeguarding Team Member Information](#)
  - 6.3 [Confidentiality of Company Information](#)
- 7.0 [Non-Solicitation](#)
- 8.0 [Information, Data, and Physical Security and Social Media](#)
  - 8.1 [Physical Security and Workplace Safety](#)
  - 8.2 [Electronic Communication and Social Media](#)
- 9.0 [Gifts, Meals, Entertainment and Legacies](#)
- 10.0 [Business Expenses](#)
- 11.0 [Personal Finances and Investment Activities](#)
- 12.0 [Banking and General Business Regulations](#)
  - 12.1 [Insider Trading](#)
  - 12.2 [Anti Money Laundering/Money Laundering Control Act](#)
  - 12.3 [Theft, Embezzlement and Misappropriation of Funds](#)
  - 12.4 [Anti- Corruption and Bribery Policy](#)
  - 12.5 [Whistleblower Policy](#)
  - 12.6 [Principal Officers/Senior Management Code of Ethics](#)
- 13.0 [Complaint Policy](#)



## About The Code of Ethics and Conduct

The Code of Ethics and Conduct (“the Code”) sets forth expectations for directors and team members to conduct themselves in an ethical manner in all their dealings with clients, shareholders, regulators, auditors, fellow team members, and the community. The Code applies to all directors and team members of Heritage Commerce Corp, Heritage Bank of Commerce and its subsidiaries (collectively referred to as “the Company”).

All directors and team members are expected to hold themselves and each other accountable to uphold the Code and are prohibited from improperly influencing or coercing others to violate the Code, Company policies, applicable laws, or regulations.

The Code is not intended to capture every situation that may arise, therefore, when in doubt, team members are encouraged to seek guidance from their immediate manager, Business Unit Executive Vice President, or a member of the People and Culture team.

On an annual basis, without exception, all team members must certify that you have reviewed and will agree to abide by the Code as a condition of employment. The Code does not create any rights for continued employment or create any type of contract or employment obligation as all team members’ employment remains “At-Will.”

### 1.0 Core Values

Although the Code primarily focuses on legal, regulatory, policy, and ethical matters, our core values are based on a set of common shared goals, attitudes, and beliefs which guides our behaviors.

Our collective behaviors define our culture and who we are.

*We act with integrity and transparency...*

*Client, shareholder, and community success is our success...*

*We help each other thrive...*

*We serve with purpose and passion...*

*We continually adapt, learn and grow...*

*We have fun with a healthy sense of humor!*

## 2.0 Your Responsibility

It is our collective responsibility to make sound decisions and act with nothing less than the highest level of ethics and integrity. Our decisions have the potential to impact clients, shareholders, communities, and team members, and may cause unintended negative consequences. To guide you in making sound decisions and to doing the right thing, the following are a set of questions to help you make informed and thoughtful decisions:



- ⇒ *Do I have all the facts?*
- ⇒ *Is this legal? Am I abiding by all laws and regulations?*
- ⇒ *Is this in accordance with our Company's policies and procedures?*
- ⇒ *Could it adversely impact our Company, clients, shareholders, and team members?*
- ⇒ *Could it cause reputational damage to our Company?*
- ⇒ *Could it cause unnecessary risk to our Company?*
- ⇒ *Should I double check with another team member or manager?*
- ⇒ *Am I abiding by a legitimate business "Need to Know" principle?*
- ⇒ *Is it the right thing to do?*

You have a duty and obligation to report situations that you suspect are unethical or illegal whether it directly affects you, someone else, or the Company. You may be held responsible for having knowledge of an unethical or illegal matter and failing to promptly report it through the proper channels outlined below.

Managers must also lead by example for their teams acting with the highest level of integrity at all times. Managers must create an environment where individuals feel safe to speak up and ask questions or report ethical concerns, potential violations of the Company's policy, laws, or regulations without the fear of retaliation. Managers are encouraged to regularly review the Code with their team members throughout the year to ensure understanding of the Code and that appropriate expectations are communicated. As a manager, you are required to report incidents where you are a witness to, or have become aware of, a potential violation of the Code that may have occurred.

If you have questions about the Code or need to report conduct or ethical concerns, you may raise them with your manager or contact the People and Culture Department. You may also submit an anonymous complaint by calling the Company’s third-party Whistleblower and ethics hotline at 855.222.0659 or via email at [reports@lighthouse-services.com](mailto:reports@lighthouse-services.com) (by noting “Heritage Bank of Commerce” in the report).

In order to uphold the Code, you have a duty to fully cooperate in any internal or external investigations as directed by the Company. Failure to do so may result in disciplinary action up to and including termination.

### 3.0 Anti-Retaliation Policy

The Company has a zero-tolerance retaliation policy and violators may be subject to disciplinary action up to and including immediate termination of employment. The Company prohibits retaliation against any person for reporting or threatening to report discrimination, harassment, prohibited behavior, and conduct, or for participating in an investigation of a violation of this Policy or any other Company policies.

**We strive to be the employer of choice in our markets where diversity is celebrated, and every team member has the opportunity to THRIVE.**

### 4.0 Prohibited Conduct and Behavior

We strive to be the employer of choice in our markets where diversity is celebrated, and every team member has the opportunity to thrive. We all have the responsibility to act as good corporate citizens inside and outside of the workplace. When conflicts arise, we must resolve them and do so expeditiously and in a professional, respectful, and constructive manner.

#### 4.1 Discrimination and Harassment

We are an Equal Opportunity Employer and we are committed to providing a work environment that is free from any form of discrimination or harassment on based on race, religious creed, color, national origin or ancestry, physical or mental disability, medical condition, genetic information, marital or domestic partner status, sex, gender, gender identity or expression, age, sexual orientation, military or veteran status, pregnancy, childbirth, breastfeeding, or related medical conditions, or any other characteristic or status made unlawful by federal, state or local laws. This policy also prohibits unlawful discrimination based on the perception that a person has any of those characteristics or is of protected status. All such discrimination is unlawful and will not be tolerated nor permitted.

This policy prohibits directors, team members, clients, independent contractors, vendors, or any person with whom a team member comes in contact with while working from engaging in discrimination or harassment acts.

Prohibited harassment based on a protected status includes, but is not limited to, verbal conduct, such as threats, epithets, derogatory comments, or slurs; visual conduct such as derogatory pictures, cartoons, drawings, gestures, screen savers, e-mail, social media postings, or posters; and physical conduct such as assault, unwanted touching, or blocking or impeding movement.

The Company is committed to enforcing this Discrimination and Harassment Policy. The effectiveness of our efforts depends in part on team members telling us about inappropriate workplace conduct. If you feel that you or someone else may have been subjected to conduct that violates this policy, you should report it immediately. You may speak to, write to, or otherwise contact any of the following resources: your manager, or, if the conduct involves your manager, any member of the People and Culture Department. If team members do not report discriminatory conduct, the Company may not become aware of a possible violation of this Policy and may not be able to take appropriate corrective action.

The Company will ensure that a fair, timely, and thorough investigation is conducted by qualified personnel in an impartial manner that provides all parties with appropriate due process and reaches reasonable conclusions based on the information collected. The Company will maintain appropriate documentation and tracking to ensure reasonable progress is made. At the close of the investigation, the Company will consider appropriate options for remedial actions and resolutions. If misconduct is found, the Company shall take prompt, corrective action, as appropriate. The Company will maintain confidentiality to the extent possible, however, confidentiality cannot be guaranteed if disclosure is required in order to conduct a full and complete investigation. You will not be retaliated against for lodging a complaint or participating in an investigation.

*Supervisors and managers have an obligation to report discriminatory conduct of which they become aware.*

*Supervisors and managers who observe such conduct or who receive any complaints of misconduct must report the conduct or complaint to any member of the People and Culture Department so that an investigation can be made, and corrective action taken, if appropriate.*



## 4.2 Threats and Violent Acts

You deserve to work in an environment that is not only safe, but one that also promotes teamwork and collaboration. We expect you to treat others with courtesy and respect and resolve issues in a professional manner. Threatening or violent acts directed toward a person at work or on duty, including verbal or physical threats, are prohibited, which may include, but are not limited to abusive conduct, intimidation, aggressive behavior, displaying threatening gestures, bullying, cyber bullying, harassment, hitting, kicking, punching, spitting, and throwing of objects.

## 4.3 Drugs and Alcohol

The Company is committed to providing a safe, healthy, and productive workplace that is free from alcohol and unlawful drugs as classified under state, local, or federal laws (including medical or recreational marijuana). As such, the Company prohibits the following activities any time that you are on Company premises or conducting Company business: the use, abuse, or being under the influence of alcohol, illegal drugs, or other impairing substances; the possession, sale, purchase, transfer, or transit of any illegal or unauthorized drug, including prescription medication that is not prescribed to the team member or drug-related paraphernalia; the illegal use or abuse of prescription drugs.

This Policy does not prohibit you from consuming alcohol with moderation at Company and business-related events taking place on or off Company property. However, if you choose to consume alcohol at such events, you must do so responsibly and maintain your obligation to conduct yourself properly and professionally at all times.

While the use of marijuana has been legalized under state law for medical and recreational uses, it remains an illegal drug under federal law and its use as it impacts the workplace is prohibited by Company policy. The Company does not discriminate against team members solely based on their off-duty use of medical and recreational marijuana in compliance with applicable state medical and recreational marijuana laws. However, you may not consume nor be under the influence of marijuana while on duty or at work, even if you have a valid prescription for medical marijuana.

## 4.4 Falsification of Books and Records

We must maintain records and accounts that accurately reflect the Bank's assets, liabilities, receipts and disbursement, and to maintain all books, records, and documents in good order. Directors and team members shall not make any false entries in Company records, create false transactions, alter documents, or sign documents if such person lacks the authority to do so; they shall not direct a team member to make an entry or process a transaction that violates or ignores the Company policy nor make such an entry or process a transaction themselves.

## 5.0 Conflicts of Interest

A conflict of interest is defined as a team member's involvement in activities which may either conflict with the team member's duty to the Company, adversely affect the team member's judgment in the performance of his or her responsibilities, or influence a business decision due to an existing personal relationship.

For example, a conflict of interest would arise in a situation where any director, team member, family member, or acquaintance could have a personal interest, financial or otherwise, or personally benefit from a relationship with a borrower, client, vendor, supplier, person, or company having a business dealing with the Company.

## 5.1 Business Dealings

It is the Company's policy that you do not perform nor approve transactions for friends, family members, or for those with whom you have a personal or financial interest such as cashing checks, issuing cashier's checks, making deposits or withdraws, conducting wire transfers, and/or handling loans. Team members with a personal or financial interest are also prohibited from performing duties that require dual control such as verifying cash counts, deposits, or accessing the vault. It is inappropriate for team members to serve as a conductor on the client's behalf acting as their representative.

You are prohibited from personally borrowing or lending money or personal property to clients or other team members (unless they are family members), vendors, or anyone doing business with our Company.

**It is important to avoid even the appearance of a conflict of interest since the appearance can be just as damaging to the Company's reputation as an actual conflict.**





## 5.2 Outside Employment and Activities



Team members who wish to pursue a second job or other employment opportunities while working at the Company must receive advanced written approval from their immediate manager, their Business Unit's Executive Vice President, and the Chief of People and Diversity to ensure a conflict of interest or an appearance of a conflict of interest does not exist, and to protect the Company's confidential information, trade secrets, and business interests. There are certain key positions which forbid team members from pursuing other paid endeavors due to the nature of their role at the Company. You may speak to someone on the People and Culture team to learn more.

Other types of outside activities, whether for compensation or not, that may raise a conflict of interest include, but are not limited to:

- ⇒ *Preparation of financial or other statements to be presented to our Company to secure a loan*
- ⇒ *Practicing law or providing tax and/or financial investment advice for team members or Company clients*
- ⇒ *Publication of books, articles, or whitepapers relating to our Company or for any Company client*

## 5.3 Political Contributions and Activities

It is the Company's policy to strictly comply with all applicable federal, state, and local political campaign laws. Lobbying activity includes attempts to influence the passage or defeat of legislation directly or indirectly. This activity is subject to applicable regulations, registration, and complex compliance requirements. You may not engage in any lobbying activities including making direct or interest contributions to any state, local, or national campaigns on behalf of the Company without prior written approval of the President and Chief Executive Officer.

Any team member who wishes to run for elective political office or accept a governmental appointment should inform and obtain written approval from the President and Chief Executive Officer to ensure that the duties of that office and possible time away from the job will not create a conflict with the Company's expectations.

Team members of Heritage are prohibited from using Company resources such as worktime, property, personnel time of others, and equipment to assist any candidate for public office in any way without advance approval from the President and Chief Executive Officer.

## 5.4 Serving the Community

We pride ourselves for being a Community Bank and encourage all directors and team members to give back to the community through volunteerism and other outreach efforts. It is our responsibility to ensure that our community engagement efforts do not create a real or perceived conflict by donating to clients, vendors, or others to induce business in exchange for favorable terms on products and services, reduced fees, or other tangible or non-tangible benefits. Team members should consult with their manager and obtain advanced written approval prior to joining a non-profit board or accepting any unpaid board seat. Paid board seats are only permissible with the advanced written approval from the President and Chief Executive Officer.

## 5.5 Personal Relationships



In an attempt to prevent the appearance of a conflict or favoritism, romantic relationships that develop between team members reporting within the same business line leader must be disclosed to their manager and the People and Culture team. Managers are prohibited from having a romantic relationship with subordinates or anyone in their chain of command. It is important that employment decisions like performance evaluations, compensation decisions, granting time off, work assignments, working conditions, and other employment decisions are conducted without the appearance of bias, favoritism, harassment, or unethical conduct. The Company reserves the right to reassign team members to other roles in order to eliminate or reduce the actual or appearance of a conflict.

## 6.0 Protecting Proprietary and Confidential Information

All information obtained by you in connection with your employment at our Company is proprietary information and the exclusive property of the Company and shall not be disclosed to third parties or anyone who does not have a legitimate business to know. Examples of confidential information include, but are not limited to:

- *Client lists*
- *Deposit account information and agreements*
- *Credit information*
- *Plan, policy, procedural documents*
- *Software programs*
- *Contract documents*
- *Vendor agreements*
- *Consumer loan documents and disclosures*
- *Commercial loan documents and disclosures*
- *Team member records*
- *Financial and accounting records*
- *All documents or records used to operate the Company*

Directors and all team members must comply with applicable Information Security Policies designed to safeguard confidential and proprietary information. Examples include, but are not limited to, ensuring emails are sent to the intended recipient, and keeping laptops and physical files and/or confidential information secure while in your care. See Section 8.0 Information and Data Security for more details.

Notwithstanding the foregoing, as provided for by the Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016, a team member will not be held criminally or civilly liable under any federal or state trade secret law for any disclosure of a trade secret that is made: in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, and solely for the purpose of reporting or investigating a suspected violation of law; or in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

If a team member files a lawsuit for retaliation by the Company for reporting a suspected violation of law, the team member may disclose the Company's trade secrets to the team member's attorney and use the trade secret information in the court proceeding if the team member files any document containing the trade secret under seal, and does not disclose the trade secret, except pursuant to court order.

In addition, this Policy (or any policy in the Code), is not intended to preclude or dissuade team members from engaging in legally protected activities/activities protected by state or federal law, including the National Labor Relations Act, such as discussing wages, benefits, or terms and conditions of employment, forming, joining, or supporting labor unions, bargaining collectively through representatives of their choosing, raising complaints about working conditions for their and their fellow team member's mutual aid or protection, or legally required activities.

There are specific privacy laws which govern the banking and financial services industry and our business such as the California Consumer Rights Act. You are expected to follow regulations set forth by the [California Consumer Privacy Act](#), which is applicable to team members and clients. Review the [Consumer Privacy Act Policy](#) for more information.

## 6.1 Safeguarding Client Information

Safeguarding the confidential financial information concerning Company's clients is essential in maintaining public trust. The laws and ethical rules that govern the banking profession impose a responsibility to protect the confidences obtained in the course of client contact from unauthorized disclosure and improper use.

It is the policy that such confidential information acquired by a team member must be held in the strictest confidence. Such information is to be held for Company purposes and not as a basis for personal gain by directors, team members, friends of the Company, shareholders, clients, etc. In limited situations, client information may be released to private persons, organizations, or governmental agencies that request it only with the consent of the client involved and/or upon receipt of legal requests such as subpoena or court order. Confidential client information should never be discussed with anyone outside the Company and can only be shared with those within the Company who have a legitimate business need to know.



Every item of information about a client or related matter, unless this information has been made public, is considered to be confidential. In the event of any doubt as to whether the information has been made public, the information should be regarded as confidential.

The Company requires all team members to follow these guidelines:

- ⇒ *Client Information should never be discussed openly in public places including lobby areas, restrooms, break rooms, hallways, and elevators*
- ⇒ *You should be sensitive to the risk of inadvertent disclosure resulting from open doors, video conferencing, speakerphones or other open communications*
- ⇒ *You should exercise caution when transmitting confidential information through electronic or other means to ensure that disclosure to unauthorized persons does not occur*
- ⇒ *Emails containing confidential and/or sensitive information must be sent secured using the Company's email Encryption feature*

## 6.2 Safeguarding Team Member Information

You must not access or use a team member's information unless there is a legitimate business need to do so. If you possess confidential or sensitive team member information due to your role and/or job function, you are required to treat the information with care and safeguard the information as you would with client information as described in section 6.1.

## 6.3 Confidentiality of Bank Information

When you leave your employment at our Company, you must deliver to your manager any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, equipment, other documents of property, or productions of any aforementioned items accessed or developed during your employment with the Company.

Financial or other information regarding Company is not to be released to any outside person or organization unless it has been published in reports to shareholders, or otherwise made available to the public through authorized news releases.

All news media inquiries must be referred to our head of Investor Relations. Only the President and Chief Executive Officer is permitted to comment on the Company to any news media outlets. This rule should not be construed to restrain any team member from bringing to light a violation of the Code, Company policy, law, or regulation. It is never acceptable to make negative or disparaging comments regarding a competitor of the Company.

Conversely, when you join the Company, you are not allowed to obtain, use, or distribute any information or materials (whether printed or electronic) obtained during your employment at prior companies that are not publicly available.

## 7.0 Non-Solicitation

Solicitation that is non-business related of any form is prohibited on Company premises. Team members may not solicit other team members, clients, or anyone doing business with our Company except with a Company approved or sponsored event. This includes distributing non-business-related materials, announcements, information with or without the request for monetary or other types of donations.



## 8.0 Information and Data Security

The security of our clients, team members, data, assets, and facilities is very important to our Company. As such, the Company has developed an Information Security Policy which covers physical security, cybersecurity, data security, and information security. The [Corporate Security Policy and Handbook](#) has been developed to address all security related policies for team members. In addition, Directors and certain Executives and system administrators also must comply with the Board and Executive Communications and Electronics Access Policy. Please contact the Chief Information Officer for more information.

### 8.1 Physical Security and Workplace Safety

The safety of our team members, clients, and individuals conducting business-related activities on Company property, including parking lots and garages, is of utmost importance. It takes all of us to be alert and report suspicious activities or situations to your manager immediately.

Team members are required to check the credentials of unknown individuals requesting to gain access to secured areas and are prohibited from allowing individuals to gain access to secured or restricted areas prior to confirming the legitimacy of their request.

Any type of weapon, whether licensed or not, or any item having the appearance of bringing harm, or the potential to bring harm, with no common purpose is prohibited in the workplace, and during any period in which you are carrying out business duties on behalf of the Company. For purposes of this Policy, the workplace is defined to include the Company's buildings, outdoor areas, and parking lots.

If you believe there is imminent danger of bodily injury or death, you must dial 9-1-1 to get help. Once you are safe, you must notify the Chief Information Security Officer to report the incident.

## 8.2 Electronic Communications and Social Media

Electronic communications can greatly enhance productivity and efficiency in the workplace. Any information sent between parties or entities over a phone line, through either wired or wireless internet connection is considered electronic communication. This may include information transmitted through emails, printers, Web portals, internet, intranet, chat and messaging apps, audio and video conferencing, text messages, and fax.



The following are examples of prohibited use of electronic communications on Company devices:

- ⇒ *Accessing, downloading, printing, storing or sending information which may be reasonably considered obscene, known to be false, harassing or otherwise abusive or transmitting to others in any location, images, sounds or messages*
- ⇒ *Attempting to forge electronic mail messages or using someone else's electronic mail or systems*
- ⇒ *Creating or willfully disseminating computer viruses*
- ⇒ *Copying copyrighted material (including software), except as permitted by law or by contract of the copyright owner*
- ⇒ *Conducting or sending unauthorized audio or video recordings*

It is the Company's policy to comply with all laws, regulations and related guidance in using social media. While social media accounts are personally owned, any activity whether in the office or outside, on or off Company systems, using a Company email address or not, during business hours or after, that may affect job performance or the Company's reputation and business interests are a proper focus for our Company. You should use good judgement about the content you post on social media as it may have an impact on you personally and our Company brand. You are an extension of our Company brand; therefore, the Company may request you to remove content that is deemed to violate the Company's Code even if the content is posted using your personal social media account.

## 9.0 Gifts, Meal, Entertainment and Legacies

The exchange of business courtesies such as gifts, meals, and entertainment can help strengthen business relationships, foster new relationships, and convey appreciation for business partnerships if practiced appropriately.

Any time there is an exchange of gifts, meal, or entertainment to or from clients, prospects, each other or third parties, a potential conflict may arise. It is your responsibility to ensure that the exchange of gifts, meals, and/or entertainment is reasonable, based on a legitimate business purpose and within guidelines set forth in this Policy.

It is a good practice to consult with your manager prior to giving gifts or extending hospitality and entertainment opportunities. Similarly, when you receive gifts, hospitality, and entertainment offers that appear lavish, excessive or frequent, you must raise these situations to your manager for additional guidance.

The following are examples of acceptable exchange of gifts, meals and entertainment:

- ⇒ *Normal business courtesies, such as a meal or entertainment, involving no more than ordinary amenities or monetary amounts which are available to the general public*
- ⇒ *Non-cash gifts of nominal value (under \$100.00) such as those received at holiday time or for special life moments for instance, weddings, graduations, promotions, birthdays and retirement*
- ⇒ *Unsolicited advertising and promotional material of nominal value (under \$100.00)*
- ⇒ *Discounts or rebates on merchandise or services that do not exceed those available to other clients or the general public*

Directors and team members must refuse to serve personally as executor, trustee, or guardian of an estate or trust of a client or accept legacies or bequests unless the client is a relative or family member.

It is important to recognize that federal law makes it a crime for any director or team member of a federally insured bank, directly or indirectly, to ask, solicit, demand, accept, receive or agree to receive anything of value for themselves that does not fall under the Code without proper approval. This also applies to any other person or entity intending to be influenced, or rewarded, for, or in connection with, any transaction or business of the Company. The penalty for violating this law is a fine, imprisonment, or both.

## 10.0 Business Expenses

Team members will be reimbursed for eligible expenses incurred in connection with approved business activities with submission of appropriate documentation. Team members should exercise good judgment to ensure business expenses are minimized with an emphasis on budgetary controls, discretion and open communications with those who serve in a supervisory capacity. Whenever in doubt about the appropriateness of an expense, team members should consult with their manager and obtain approval. Business expenses must be submitted with all supporting documentation and original receipts with the required description no later than 60 days from the date of the incurred expenditure. In addition, all Directors and team members must abide by the [Luxury Expenditures Policy](#).

If you have been issued a Company corporate credit card, you may only use that card for legitimate business expenses. You are prohibited from performing a cash advance on your corporate card without prior written authorization from your business line Executive Vice President or the Chief Financial Officer. Review the full [Business Expense Policy](#).

## 11.0 Personal Finances and Investment Activities

Since you work at a financial institution, you should manage your personal finances judiciously. Failing to do so may tarnish your professional credibility and negatively impact your job.

Federal and State regulations restrict the types of investments that the Company may choose. Lending personnel, in the course of their loan due diligence, will often obtain information on entities that is highly confidential and privileged. Lending and Investment personnel must be guided by information gathered independently and obey the rules of confidentiality and privacy outlined in this directive.

If a client, or any agent of a client, offers a team member the opportunity to purchase securities of any enterprise, whether in a private round or in a public offering, and those securities would not be available to any member of the general public at the same price and under the same conditions, then such opportunity is a benefit and would be subject to this Policy.



## 12.0 Banking and General Business Regulations



**The banking and financial services industry is heavily regulated and we all have a responsibility to ensure compliance with federal, state, and local laws and regulations. You must deal fairly and responsibly with the public, prospects, clients, suppliers, competitors, and one another at all times and in accordance with ethical business practices.**

### 12.1 Insider Trading

The Company has an Insider Trading Policy for our directors, officers, team members and consultants with respect to the trading of Company's securities, as well as the securities of publicly traded companies with whom we have a business relationship.

Federal and state securities laws prohibit the purchase or sale of a company's securities by persons who are aware of material information about that company that is not generally known or available to the public. These laws also prohibit persons who are aware of such material nonpublic information from disclosing this information to others who may trade. Companies and their controlling persons are also subject to liability if they fail to take reasonable steps to prevent insider trading by company personnel.

It is important that you understand the breadth of activities that constitute illegal insider trading and the consequences, which can be severe. Both the U.S. Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA") investigate and are very effective at detecting insider trading. The SEC, together with the U.S. Attorneys, pursue insider trading violations vigorously. Cases have been successfully prosecuted against trading by team members through foreign accounts, trading by family members and friends, and trading involving only a small number of shares.

This Policy is designed to prevent insider trading, or allegations of insider trading, and to protect the Company's reputation for integrity and ethical conduct. It is your obligation to understand and comply with this Policy. Review the current [Insider Trading Policy](#).

## 12.2 Anti-Money Laundering/Money Laundering Control Act



We comply with all requirements of the Bank Secrecy Act, OFAC, the USA PATRIOT Act, and all regulations of the Department of the Treasury and the Internal Revenue Service relating thereto (collectively referred to as anti-money laundering or AML regulations). We also recognize that the Bank Secrecy Act (BSA), the Office of Foreign Assets Control (OFAC), and The Uniting and Strengthening America by substantial risks and penalties by providing Appropriate Tools Required to Intercept and Obstruct Terrorism (The USA PATRIOT Act) are important tools in federal efforts to combat organized crime, terrorism, and drug trafficking. Noncompliance can expose our Company to substantial risks and penalties.

Certain products, services, clients, and geographic locations may present greater risks to our Company. Various factors, such as the type of account transaction activity, aggregate number and dollar volume of the activity, geographic location of Bank and client, and whether we offer specific products and services to clients and non-clients must be considered in identification and measurement of risk. It is your responsibility to review the full [AML/BSA/USA PATRIOT ACT Policy](#).

## 12.3 Theft, Embezzlement and Misappropriation of Funds

It is every director and team member's responsibility to protect the assets of our Company, shareholders, and clients. Anyone who steals, embezzles, commits fraud, and/or misappropriates money may be subject to a fine, penalty, imprisonment, restitution payment, and other actions as determined by federal, state, local laws, and regulations. Theft may include, but is not limited to, identity, money, Company property, work time, documents, data, and software programs.

## 12.4 Anti-Corruption and Bribery Policy

In accordance with the provisions of the Federal Bank Bribery Law, no Company official, i.e. Director, Officer, team member, agent, or vendor, shall:

*Solicit for themselves or for a third party, other than the Company itself, anything of value from any one in return for any business, service, or confidential information of Heritage Bank of Commerce and Commerce Corp*

*Accept and retain anything of value, including fees or payments, other than normal, authorized compensation, from anyone in connection with the business of the Company either before or after a transaction is discussed or finalized*

Exceptions to the above general prohibitions include acceptance of unsolicited gifts or favors based on family relationship unconnected to the business of Heritage which may be construed as a motivating factor and/or acceptance of loans from other financial institutions on customary terms to finance proper or usual activities and other items of nominal value. Please refer to section 9.0 for more information.

## 12.5 Whistleblower Policy

The Company is committed to high standards of ethical, honest, and legal business conduct. In line with this principle and our commitment to open communication, this Policy provides an avenue for team members to bring to our attention good faith complaints regarding accounting or auditing matters to the Audit Committee of Heritage Commerce Corp and Heritage Bank of Commerce (collectively, the “Audit Committee”). In accordance with Section 301 of the Sarbanes-Oxley Act of 2002, the Audit Committee has established procedures to (1) receive, retain, and treat complaints received by the Company regarding accounting, internal control, or auditing; and (2) receive confidential, anonymous submissions by team members of the company regarding questionable accounting or auditing matters. Review the current [Whistleblower Policy](#).

## 12.6 Principal Officers/Senior Management Code of Ethics

The Principal Officers and Senior Management Code of Ethics supplements the Heritage Commerce Corp’s Code of Ethics and Conduct Policy. Review the current [HCC Principal Officers and Senior Management Code of Ethics Policy](#).

## 13.0 Complaint & Reporting Policy

If you are subjected to any conduct that you believe violates any policy in the Code, or if you witness any such conduct, you should promptly report the conduct, either orally or in writing. You may speak to, write to, or otherwise contact any of the following resources: your manager or any member of the People and Culture Department. You may also submit an anonymous complaint by emailing the Company’s third-party Whistleblower and ethics hotline at 855.222.0659 or via email at [reports@lighthouse-services.com](mailto:reports@lighthouse-services.com) (by noting “Heritage Bank of Commerce” in the report).

The Company is committed to enforcing the policies in the Code. The effectiveness of our efforts depends in part on team members telling us about inappropriate workplace conduct or violations of the Code. If you feel that you or someone else may have been subjected to conduct that violates this Policy, you should report it immediately. If team members do not report such conduct, the Company may not become aware of a possible violation of this Policy and may not be able to take appropriate corrective action.

Supervisors and managers have an obligation to report discriminatory conduct of which they become aware. Supervisors and managers who observe such conduct or who receive any complaints of misconduct must report the conduct or complaint to any member of the People and Culture Department, so that an investigation can be made, and corrective action taken, if appropriate.