Security of Confidential Information: The security of your banking transaction(s) is important to us and it depends on a relationship between you, the customer and us, American Heritage Bank. We ensure protection by putting several security measures in place to keep unauthorized users from accessing any of your confidential information through your online activity, but we need your assistance in maintaining the security of all transaction(s).

What We Will Do: We will maintain state-of-the-art technology measures to ensure your personal information and confidential transactions remain safe, secure, and private. We protect your online activity through a series of account access controls, encryption, screening and filtering routers and firewalls.

We maintain controls for the way you may access your account(s). These controls are maintained through settings on the host software and restrictions may be placed on account access and transfer rights. Other controls in place pertain to password protection. Only customers who have been enabled (signed-up) for Internet Banking will be allowed access to the site. You will be able to access your account with a valid login consisting of your username and a complex alphanumeric password (consisting of upper and lower case letters and numbers) of a minimum of 6 but not to exceed 15 characters. The password may not be the same as the previous 4 passwords and may not contain any spaces. It is highly recommended not to use passwords that could easily be guessed, such as names, pets, addresses, etc. or use words that can found in any dictionary. It will ask you one of your designated security questions, that you set-up when you registered for Internet banking, if you have never logged into Internet banking on that device. If you want the device to remember you and not ask you a security question the next time you log on, click the box by "Remember this Device".

We will limit the number of times you can enter your password incorrectly. After three (3) simultaneous invalid attempts, you will be disabled. Once disabled, only bank personnel may re-set your access rights. We will monitor and record "bad-login" attempts to detect if someone may be trying to guess your password and access your account information. To assist us with the protection of your confidential information, contact us during normal business hours if you cannot remember your password. We will be happy to assist you in resetting it.

You authorize and authenticate your online banking transaction by entering your password, which is encrypted when it is transmitted to us. Encryption is one of the basic tools used for Internet security and it means we will scramble the data entered into the system. You will need to use a browser that is 128-bit secure, JavaScript enabled to log on to your account and perform transactions. When you log on to Internet banking, your browser automatically secures the session using Secure Sockets Layer (SSL). With SSL, the data that travels between the bank and the customer is encrypted so someone else cannot read it. You can determine that encryption is being used and your information is secure if a padlock icon on your browser is locked and you can see the VeriSign Secured icon. If the padlock is unlocked, encryption is not being used and makes your information vulnerable for access by outsiders.

The screening and filtering routers determine who has access to designated Internet banking components by verifying the source and designation of each transmission and determines whether or not to let the transmission pass. The firewall will track each request and verify the source and designation. When you submit your request for a transaction, the information (your username and password) is compared to what you provided to us at the time you signed up for Internet banking. This information is then stored in our secure data center for future references. If the firewall does not recognize your information when it does the comparison, it will reject the request as unauthorized traffic.

Additional security that is provided to you, the customer, is through the use of "cookies". The first time you login, the system puts an encrypted, secure "cookie" on the computer you are using. The "cookie" contains a unique randomly generated number, which when you login at a later date identifies the system as your computer by your IP address and that it is okay to ask for your password. If you try to access your account from a different computer, you will be asked a series of challenge questions to authenticate your identity before you can enter your password.

When you login from the computer you originally used, you will again be asked a series of challenge questions to authenticate your identity. “Cookies” identify the last IP address used.

Your Responsibility: You are responsible for keeping your online banking information confidential. Your password provides entry through the firewall so do not share your password or account numbers, personal identification number (PIN) and other account data with anyone, including other companies or service providers. If you feel your password has been breached, change it immediately online. We recommend that you change your password on a periodic basis and never use passwords that are easy to guess such as birth dates, first names, pet names, addresses, phone numbers, etc.

The following recommended security measures are to help safeguard your personal information:

- We recommend that you memorize your password and not write it down. If you need to write it down for future use, store it in a safe place that is only accessible to you.

- Do not leave your computer unattended while transacting on-line banking activity. Sign off properly before leaving your computer or visiting other sites on the Internet. If anyone else is likely to use your computer, clear your browser cache or close it.

- Keep others from viewing (over your shoulder) your online banking information when you sign on to the system; they can memorize your information and use it to access your account.

- When visiting the website, type the address directly into the browser rather than following a link found from a search engine (such as Google, MSN, Dog Pile, etc). This will help protect you from “logging on” to copycat Web sites that intend to steal and use your personal information.

- Notify us about lost or stolen information (e.g. someone broke into your house; someone went through important papers) or if you suspect fraudulent activity on your account(s) (e.g. your computer has been used by someone other than yourself and you are the only one who is supposed to have access)

You are also responsible for ensuring the information for your transactions are entered into the system correctly. Except as otherwise provided by law, we are not responsible for or will we cover losses due to input errors; misuse of the services; unauthorized access to your account(s) resulting from negligence (such as sharing your password, writing down your password, or entering your password when others may see you); leaving your computer unattended while transacting online banking; and failure to report unauthorized access to your account within two (2) business days from the date it became known to you.

Electronic Mail: You can use electronic mail (e-mail) to contact us about inquires, maintenance and/or problems with the system. We will use reasonable efforts to respond by the next business day. These responses are considered received whether the customer has logged on to the system and read them or not. Messages sent by e-mail are not considered secure methods of communication. Third parties could intercept them; they could be sent to the wrong address, or the appropriate department at the bank may not receive them. We recommend you do not send e-mails that require immediate attention or any that contain confidential information. Be aware that a “receipt” of acknowledgement on an e-mail message means only that the message has routed into the Internet, not that the message has been received by American Heritage Bank. Urgent or confidential matters should be addressed in person or by phoning us at (575) 762-2800 for Clovis and (575) 253-4500 for Melrose. Authorizations that require original signatures should be provided via postal mail or in person.

The bank will not request any personal or financial information by e-mail. If you receive an e-mail from American Heritage Bank requesting confidential information, **DO NOT RESPOND**. Some scammers send e-mails that look legitimate but all they want to do is steal your information if they can. We will **NOT**, at any time, call and ask for your login password. If anyone calls and request this information, contact the bank immediately.