Department:	Compliance
Policy For:	Website Privacy Policy
Bank Approved:	December 15, 2022
Prior Revision Date:	October 26, 2021

WEBSITE PRIVACY POLICY

At Summit State Bank, the basis of each customer relationship is trust. We respect the privacy of our customers and are committed to treating customer information responsibly. We believe the confidentiality and protection of customer information is one of our fundamental responsibilities. While information is critical to providing quality service, we recognize that one of our most important assets is our customers' trust. Thus, the safekeeping of customer information is of the highest priority to Summit State Bank.

Collection, Use, and Retention of Your Information:

When you visit our website, we may collect certain categories of information from you, such as personal information that may be needed or requested from you in order for you to access online banking or other services. Personal information means personally identifiable information such as first and last name, physical address, email address, or other identifier that permits us to contact you physically or online. The only information we collect through this website is information that is necessary to interact with you or to accomplish transactions you request. This may result in sharing of personal information with third parties (such as data processors or service bureaus) as part of servicing your accounts or transactions. We use the information to provide personal service to you and to help us design or improve our products and services to meet your financial needs. When you send us a secure online message or a conventional e-mail, we retain the contents of the message and our response.

Our Web Server may collect generic information about you such as the pages you visit, the date and time of access, the actions that you tried to perform, and whether or not you were successful. Our Web Server may use "cookies" which is a small file stored on your computer to give you a unique ID. Cookies may be used to monitor your use of our Website, to deliver content specific to your interests, and for other identification purposes. You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Online Banking:

Ensuring the security of your personal information is important to us. When you log in to Online Banking through our login page, your login information is protected using a minimum of 128-bit SSL encryption.

User Name and Password:

Summit State Bank provides additional security for your financial information by the mandatory use of a User Name and Password to access account information. It is important that your User Name and Password are kept

confidential. Your User Name and Password should be unique, difficult to guess, and ideally should have both lowercase and uppercase letters and numbers. For example, do not create a User Name that is similar to your email address.

Security Tips for Online Banking:

- Memorize your User Name and Password. Your online User Name and Password authenticate you when you begin an Online Banking session. You should memorize your Password and never write it down, save it to your computer, or reveal it to anyone.
- Create a complex password that:
    - Is 12 – 32 characters in length. A longer password is better.
    - Is not a word that is found in a dictionary.
    - Is a paraphrase or small sentence, rather than a word.
    - Is not the name of a person or pet.
    - Includes upper- and lower-case letters and numbers.
    - Has at least four different characters (no repeats).
    - Has at least one special character.
    - Looks like a sequence of random letters and numbers.
    - Is not obvious or easily obtainable information.
    - Is a password that is unique to this website and not used for any other websites.
- Change your password regularly.
- Remember to sign out of Online Banking and close all browsing sessions for security. You may not always be at your own computer when you bank online. Therefore, it is important to sign off when you are finished with your online session and close all open browsers. For your security, Online Banking will automatically end your banking session after twenty minutes of inactivity. There is a twenty minute maximum time out limit.
- Always use your browser's built-in security features.
- Make sure the computer(s) you use have current software security patches and anti-virus software. Antivirus software requires frequent updates to guard against new viruses.
- Install a personal firewall to help prevent unauthorized access to your home computer.
- Wireless Wi-Fi access should be secured with strong encryption. WPA2 security with a strong password is recommended. WEP and WPA (first generation WPA encryption, which is different than WPA2) can be easily cracked. Use of public Wi-Fi is not recommended.
- Be suspicious of unsolicited email from a "business" that asks for your password, Social Security number, or highly sensitive information. Legitimate businesses typically do not ask for this type of information over the Internet. Contact the business directly to verify the authenticity of the email. Do not reply to or click on any links or pictures in unsolicited emails, especially those asking for personal information. **Summit State Bank will never email you or phone you to request private information such as account number, social security number, card number, or password.**
- Do not give out personal or financial information online, via text message, or on the phone unless you initiated the contact and know the party you are dealing with is legitimate.
- Promptly and carefully review your account statements such as bank statements, credit card statements, as well as mobile phone and home telephone bills for unauthorized charges or activity. Regularly check your statements and account activity online to spot questionable transactions.

Security Tips for Mobile Devices:

Mobile devices can contain very personal and confidential information, i.e. email, pictures, contact information for friends and family, etc. You must permit cookies in order to use mobile banking. Take the following steps to help secure your mobile device from unauthorized access in case your phone is lost or stolen:

- Configure your mobile device to automatically lock after 15 minutes or less of inactivity.
- Configure your mobile device to require a complex password in order to unlock the device (see ***Security Tips for Online Banking*** above, for complex password suggestions).
- If possible, configure your device to automatically wipe all information after 10 or fewer invalid password attempts.
- If possible, configure your device to work with remote tracking or remote wipe software, such as a Microsoft Exchange server.
- If the mobile device you use for ezBanking or Business ebanking is lost or stolen, log in to your online banking from a PC as soon as possible and remove the device from the mobile banking service so your accounts cannot be accessed. You should also contact Summit State Bank to make us aware that your mobile device has been lost or stolen. If needed, we can assist you during our regular business hours with deactivating access to your account from the lost or stolen device.

Notify Summit State Bank immediately by phone if you notice any unusual account activity or if your mobile device has been lost or stolen. Call your local branch between 9:00 a.m. and 5:00 p.m. Monday through Friday.

Links to Other Websites:

Our website may contain links to other websites of interest. However, if you use these links to leave our site, you should note that we do not have any control over that other website. Therefore, we are not responsible for the protection and privacy of any information which you provide while visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Children's Privacy:

Protecting the privacy of children is especially important to us and we do not knowingly solicit or collect personal information from children on our website. For more information about the Children's Online Privacy Protection Act (COPPA), visit the Federal Trade Commission website at www.ftc.gov.

Our Privacy Commitment to You:

At Summit State Bank, we value our relationship with you. We want you to understand how we use the information that you provide and our commitment to ensuring your personal privacy. If you have any questions about how Summit State Bank protects your confidential information, we invite you to contact Summit State Bank's Compliance Officer at (707) 568-6000.

Changes to this Website Privacy Policy:

If it is necessary to make changes to our Website Privacy Policy, we will update this Website Privacy Policy with the changes and new effective date.