

## **PRIVACY POLICY STATEMENT FOR ONLINE BANKING**

We, at Gulf Coast Bank & Trust Co., place a great deal of importance in the relationships we work so hard to build. We understand that privacy is important. We are committed to safeguarding your confidential information with the same care that we use to protect information obtained from transactions through any other methods of delivery.

As a general policy Gulf Coast Bank does not automatically collect and store website user's personally identifiable information, such as the user's name, address, telephone number, email address, social security number, bank account number or credit card number.

Our online services and website are not intended for children under the age of 13. If you are a child under the age of 13 please seek permission by a parent or guardian before using this website. We will not knowingly collect personal information from children under 13 without parental consent. In the event we learn that we have collected information from a child under 13 without parental consent, we will delete the information as soon as reasonably possible.

Our web site privacy policy is described below. It has been approved by our board of directors and is included in the training of our staff.

### **Recognition of Expectation of Privacy**

Gulf Coast Bank recognizes that our customers have a reasonable expectation of privacy, and we recognize the importance of protecting that privacy. We are committed to safeguarding both the financial records and relationships of both our customers and our visitors to our web site.

### **Collection, Use and Retention of Customer Information**

In order to identify and communicate with you through our web site Gulf Coast Bank may collect, use, and retain information about you. This information is collected and used to provide you with products and services that you initiate: to help us respond to specific questions that you ask: and to provide you with information that may be of interest to you. We may also use this information to help us comply with laws and regulations that apply to us. As a general rule we do not automatically collect and retain personally identifiable information from visitors to our web site, such as the user's name, address, telephone number, email address, social security number, bank account number or credit card number.

We may collect and retain certain information of a general type such as:

- The name of the domain used to access the internet.
- The Link (Internet Address), search terms or keywords used to gain access to our site
- The type of web browser used to explore our site and country from which your computer is connected to the internet based on the Internet Protocol (IP) address.
- The date and time.
- The inferred age group, inferred gender, and inferred purchase interest based on the user's activity across the web. (i.e. ages 30-35, female, interested in buying a new car)
- The number of unique visits a page on Gulf Coast Bank's website receives per month.
- Visitors may also choose to give us information (i.e.: when applying for an account).

### **Online Behavioral Advertising**

Online behavioral advertising (also known as interest-based advertising) is the practice of collecting information from a computer or device in regards to the user's browser activity to help better target advertisements. With online behavioral advertising, we hope to better understand our current website users and to engage and provide users with products or

services that may be of interest to them through targeted ads. If you wish to learn more about online behavioral advertising, you can visit <http://www.aboutads.info/consumers/>

Gulf Coast Bank & Trust has implemented online behavioral advertising which uses one or more of the below features.

- **Remarketing** will be used to reach people who previously visited our website and match the right people with the right message. To successfully target the needs and wants of our current website users; as well as inform current users of products and or services we will utilize a 3<sup>rd</sup> party to collect audience data. Third party vendors, including Google, may show advertisements across the internet as you browse. Remarketing lists built from our current website user's website activity reported by Google will not be shared with other 3<sup>rd</sup> parties.
- **Demographics & Interest Reporting** will be used to identify current website users' inferred age group, inferred gender, and inferred purchase interests. Gulf Coast Bank & Trust will use this information to inform the user of certain products or services that may interest them. For instance, we may have a specific service that is on high demand for a specific age group. This reporting will help us better target our ad spending by allowing us to directly target those who are interested in the product or service. Additionally, we can use the inferred age, inferred gender, and inferred purchase interest to help build remarketing lists. This data reported by Google will not be shared with other 3<sup>rd</sup> parties.

Gulf Coast Bank & Trust will not run online behavioral advertising campaigns to collect personally identifiable information, such as your name, email address, billing information, or other data which identifies you. The bank will not share, use, or associate personally identifiable information with remarketing lists, cookies, data feeds, or other anonymous identifiers.

### **Use of Cookies to Collect Information**

Cookies enable us to learn which advertisements bring users to our website and allow your web experience to be personalized. Cookies are small text files that a website server places on a computer.

The cookies will not collect or store any personally identifiable information, such as the user's name, address, telephone number, email address, social security number, bank account number or credit card number.

Gulf Coast Bank and third-party vendors, including Google, use first-party cookies and third-party cookies together to report how Gulf Coast Bank's ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to Gulf Coast Bank's website. First-party cookies are associated with the domain of the site a user visits or is currently viewing. Third-party cookies are associated with a domain that is separate from the site a user visits enabling us to collect non-personal identifiable information in regards to the user's activities across the web, such as the inferred age group (20-24), inferred gender (female), and inferred purchase interests (shoes).

Users can set their browsers to alert them each time a cookie is offered and **set up browsers to accept or reject certain cookies at all times**. If you wish to learn more about cookies, you can visit <http://www.aboutads.info/consumers/>

### **Opting Out**

If you wish to directly opt out of all online behavioral advertising, you will need to opt out of from **each browser** (i.e. Microsoft Explorer, Google Chrome, & Mozilla Firefox) **on each of the computers and devices that you use**. Please note if you opt out of online behavioral advertising, you may still receive advertisements from us but they will no longer be customized based on your web-browsing activities on third-party websites.

You can view a complete list of companies currently customizing ads for your browser and conveniently [opt out of online behavioral advertising](#). You will be able to opt out of all companies that participate in the Digital Advertising Alliance (DDA) Self-Regulatory Program for Online Behavioral Advertising.

You can [modify your Google Ads Settings](#) & opt-out of interest based advertising.

Please note Gulf Coast Bank may utilize third-party websites for online behavioral advertising. These advertisements will supply an advertising icon that when clicked provides a way for you to opt out of data collection and use by the third parties listed for the purposes of online behavioral advertising.

### **Maintenance of Accurate Information**

Gulf Coast Bank is committed to keeping our customers' account information accurate, current and complete. Procedures have been established to help assure that this information is correct in a manner that is commercially reasonable. Instructions for contacting the bank if a discrepancy is found are included on the account statements. We will research and resolve discrepancies as quickly as possible.

### **Employee Access to Information**

This privacy policy statement is provided to our employees during training. Employees are instructed never to divulge financial information or records of a customer to anyone outside the bank. Employee access to personally identifiable information is limited by their need to know to properly transact bank business. Employees are trained to recognize the importance of customer confidentiality and that the bank may take disciplinary measures to enforce those privacy responsibilities.

### **Protection of Information via Established Security Procedures**

Security standards and procedures to prevent unauthorized access to confidential information are in place. Updates to technology are implemented and tests conducted to improve the integrity of our systems in protecting information

### **Restrictions on the Disclosure of Account Information**

Specific information about customer accounts or reports or other personally identifiable data is not revealed to unaffiliated third parties for their independent use except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide due diligence, unless:

- The information is provided to help complete a customer initiated transaction,
- The customer authorizes it,
- Disclosure is required by/or allowed by law (e.g., subpoena, investigation of fraudulent activity, etc.)
- The customer has been informed about the possibility of disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline ("opt out").

### **Maintaining Customer Privacy in Business Relations with Third Parties**

When it is necessary to contract with outside third parties to perform specific services or support bank products the vendors selected are expected to adhere to the same privacy standards and applicable laws and regulations as the Bank. They must be additionally responsible for maintaining customer confidentiality.

### **Disclosure of Privacy Principles to Customers**

This policy contains guidelines that have been prepared so that our customers and visitors to our web site understand our commitment to personal privacy.

### **Consent and changes to our Privacy Policy**

By using our Site, you consent to the collection and use of the information by us and to the terms of this Privacy Policy.

Gulf Coast Bank & Trust Co. reserves the right to update or change this policy at any time. We will post changes to our policy so that you are aware of the changes to our policy and the information collected. By using our Site after such changes to our policy, you agree to be legally bound and consent to the policy changes.

Revised 12/2016

### **Security Statement for ONLINE BANKING**

At Gulf Coast Bank & Trust Company, we understand the importance of the responsibility that you have entrusted to us. Gulf Coast Bank is proud of the sophisticated level of data security and privacy supplied to its Online Banking accountholders. ITI and Unisys (nationally recognized vendors) have helped our data processing service bureau implement Internet security plans by selecting best-of-breed vendors for multiple functions.

Data security is provided on multiple levels: by company policy, firewall, intrusion detection software, network monitoring, and application-level security.

### **Company Policy**

Our data processing service bureau is prohibited from accumulating and distributing or selling our aggregated account holders' information to third parties. In order to identify and communicate with you through our web site Gulf Coast Bank may collect, use, and retain information about you. This information is collected and used to provide you with products and services that you initiate; to help us respond to specific questions that you ask; and to provide you with information that may be of interest to you. We may also use this information to help us comply with laws and regulations that apply to us. As a general rule we do not automatically collect and retain from our website visitors personally identifiable information, , such as the user's name, address, telephone number, email address, social security number, bank account number or credit card number. We may collect and retain certain information of a general type such as: a) The name of the domain used to access the internet; b) The Link (Internet Address), search terms or keywords used to gain access to our site; c) The type of web browser used to explore our site and country from which your computer is connect to the internet based on the Internet Protocol (IP) address; d) The date and time of access; e) The inferred age group, inferred gender, and inferred purchase interest based on the user's activity across the web; f) The number of unique visits a page on Gulf Coast Bank's website receives per month; g) Other information visitors may also choose to give us (i.e.: when applying for an account).

### **Firewall**

A firewall serves as a security gate between the Internet and our data processing service bureau's network - including our mainframe data. By intercepting Internet data "packets" first, the firewall ensures that only packets permitted by our "rule set" may be passed beyond the public Internet to our secure web commerce server, and ultimately to the Online Banking application. Our service bureau uses an integrated firewall system. This firewall system has been certified by the International Computer Security Association (ICSA).

**Intrusion Detection**

Intrusion detection software, running on its own server, unobtrusively analyzes data packets to detect patterns of hostile activity, misuse, or malicious Java and ActiveX applets. The intrusion detection system detects intrusion attempts in real time and responds to suspicious activity.

**Network Monitoring**

The firewall and intrusion detection system is monitored 7 days a week, 24 hours a day. The online banking application and its encrypted data are not available to monitoring personnel.

**Application Level Security**

Unique user codes and passwords identify authorized accountholders. The combined effect of software security and network security allow customers to access only mainframe or other networked host areas permitted through the Online Banking application.

Gulf Coast Bank & Trust Co. reserves the right to update or change this policy at any time.

Revised 12/2016