St. John Financial Group, Inc.

Nonpublic Personal Information Privacy Policy

This policy is established to comply with the Gramm-Leach-Bliley Act of 1999, and the regulatory mandates related to the same. It applies to all employees of St. John Financial Group, Inc. Some employees employed by St. John Financial Group, Inc. may meet with the public under the "Doing Business As" (DBA) names of St. John Insurance, St. John Financial Services, and St. John Insurance and Financial Services. Regardless of the DBA name used with the public, this policy applies in full force for any and all entities. When the name, "St. John Financial Group, Inc." is used below it includes all entities listed above and any future entities that may used as DBA names with the public.

The parties subject to this privacy policy share certain nonpublic personal information about the customers of St. John Financial Group, Inc. This information sharing is necessary to effect, administer, or enforce transactions that customers have requested or authorized in connection with servicing or processing a financial product or service.

Nonpublic Personal Information is information about customers that is:

a. Personally identifiable financial information, such as information a customer provides to a financial institution to obtain a financial product or service from the institution, and information about a customer resulting from any transaction involving a financial product or service between the institution and the customer, or information the institution otherwise obtains about a consumer in connection with providing a financial product or service to the customer.
b. Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
c. Nonpublic information includes information that is maintained in paper, electronic or any other form that is maintained by or on the behalf of St. John Financial Group, Inc.
d. Customer information systems includes any electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.
e. Nonpublic personal information includes both nonpublic personal financial information and nonpublic health information.

I. Confidentiality of Information

All customer nonpublic personal information of St. John Financial Group, Inc. is deemed to be Confidential Information and St. John Financial Group, Inc. agrees to maintain necessary safeguards to ensure the integrity and confidentiality of said information.

II. Non-Disclosure of Nonpublic Personal Information

St. John Financial Group, Inc. and its employees will not disclose to any person or party other than the company doing business with each customer any customer information which is nonpublic personal information; however, employees may disclose the customer information as authorized by federal or state law.

In the event of a disclosure authorized by law, a report of said disclosure is to be given to St. John Financial Group, Inc. before said disclosure is to be made. The report is to contain the type of information to be disclosed, who it will be disclosed to, and, if ascertainable, how the information is to be utilized.

III. Unauthorized Disclosure

In the event of any discovered unauthorized disclosure of any customer information, the employee shall immediately notify St. John Financial Group, Inc. of the disclosure.

IV. Nonpublic Personal Information Security Program

St. John Financial Group, Inc. has implemented a Security Program to protect and secure all nonpublic personal information of its customers.

a. Outdated information no longer required by applicable rules and regulations will be shredded.
b. Files not in use will be secured in filing cabinets. File cabinets will be locked when not in use and at the close of each business day.
c. Clients must authorize in writing, disclosure of information to third parties such as spouses, relatives, friends, businesses, etc.
d. Any time the office is closed, the last person leaving will lock the exterior door and set the alarm.
e. All computers containing customer information will have the encrypted hard drives, passwords to access user accounts and passwords to access databases. No database password shall be set on "remember me." Encryption and password standards will meet the highest minimum standards set by regulatory authorities, current broker-dealer or other vendors of products.
f. Current and future standards of the Oklahoma Insurance Department as outlined in Title 365, Chapter 35 shall be incorporated into this policy.
g. Standards of the state and federal regulatory authorities and the current broker-dealer shall be incorporated into this policy.
h. Visitors claiming to be regulators, inspectors, utility personnel, etc. will be identified using their ID badges. If necessary to verify identity, phone calls will be made to the home office of such visitors.
i. Client identification will be verified by appropriate means, including DOB, SSN, driver's license, caller ID, etc.
j. All employees are expected to keep up with changes to this policy and implement said policy to the best of their abilities.
k. Security risks will be reviewed on an annual basis or as needed to react to new information concerning potential threats or to make appropriate changes to this policy.