PRIVACY POLICY

Addison Capital (AC) views protecting its customers' private information as a top priority and, pursuant to the requirements of the Gramm-Leach-Bliley Act (GLBA), AC has instituted the following policies and procedures to ensure that customer information is kept private and secure.

This policy serves as formal documentation of the Company's ongoing commitment to the privacy of its customers. All employees will be expected to read, understand, and abide by this policy and to follow all related procedures to uphold the standards of privacy and security set forth by AC. This Policy, and the related procedures contained herein, is designed to comply with applicable privacy laws, including the GLBA, and to protect nonpublic personal information of AC's customers. In the event of new privacy-related laws or regulations affecting the information practices of AC, this Privacy Policy will be revised as necessary and any changes will be disseminated and explained to all personnel.

Scope of Policy

This Privacy Policy covers the practices of the Company and applies to all nonpublic personally identifiable information of our current and former clients. If a client decides to close its account(s) with AC, or becomes an inactive client, AC will continue to adhere to its privacy policy and practices with respect to that client.

Information Collected

AC limits the use, collection, and retention of client or potential client information to what we believe is necessary or useful to conduct our business and offer quality services to our clients or potential clients. AC collects nonpublic personal information about clients from various sources. These sources and examples of information include:

- Account and service applications such as client surveys, agreements, etc. which typically request name, address, telephone number, social security number, date of birth, employment status, annual income, and net worth.
- Information about transactions and account custodian(s) such as account numbers, balances, types of transactions and investment history.
- Conversations between clients and AC's representatives.

Protecting Customer Information

In Regulation S-P, the SEC published guidelines pursuant to section 501(b) of the GLBA that address the steps a financial institution should take in order to protect information. The overall security standards that must be upheld are:

- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of customer records.
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Employee Responsibilities

- Each employee has a duty to protect the nonpublic personal information of customers collected by AC.
- No employee is authorized to disclose or use the nonpublic information of customers on behalf of AC.
- Each employee has a duty to ensure that nonpublic personal information of AC's customers is shared only with employees and others in a way that is consistent with the Company's Privacy Notice and the procedures contained in this Policy.
- Each employee has a duty to ensure that access to nonpublic personal information of AC's customers is limited as provided in the Privacy Notice and this Policy.
- No employee is authorized to sell, on behalf of AC or otherwise, nonpublic information of AC's customers.
- Employees with questions concerning the collection and sharing of, or access to, nonpublic personal information of AC's customers must look to AC's CCO for guidance.
- Violations of these policies and procedures will be addressed in a manner consistent with other AC's disciplinary guidelines, up to and including termination of employment.

Disclosure of Information to Nonaffiliated Third Parties

AC has a "Do Not Share" policy. We do not disclose nonpublic personal information to nonaffiliated third parties, except under one of the GLBA privacy exceptions as described below. Since AC currently operates under a "do not share" policy, it does not need to provide the right for its clients to opt out of sharing with nonaffiliated third parties, as long as such entities are exempted as described below. If AC's information sharing practices change in the future, we will implement opt out policies and procedures, and we will make appropriate disclosures to our clients.

Types of Permitted Disclosures – The Exceptions

In certain circumstances, Regulation S-P permits AC to share nonpublic personal information about its clients with nonaffiliated third parties without providing an opportunity for those individuals to opt out. These circumstances include sharing information with a nonaffiliated (1) as necessary to effect, administer, or enforce a transaction that a client requests or authorizes; (2) in connection with processing or servicing a financial product or a service a client authorizes; and (3) in connection with maintaining or servicing a client account with AC.

Service Providers

From time to time, AC may have relationships with nonaffiliated third parties (such as attorneys, auditors, accountants, brokers, custodians, and other consultants), who, in the ordinary course of providing their services to us, may require access to information containing nonpublic information. These third-party service providers are necessary for AC to provide our investment advisory services. AC requires assurances from those service providers that they will maintain the confidentiality of nonpublic information they obtain from or through us. In addition, AC selects and retains service providers that we believe are capable of maintaining appropriate safeguards for nonpublic information.

Sharing as Permitted or Required by Law

AC may disclose information to nonaffiliated third parties as required or allowed by law. This may include, for example, disclosures in connection with a subpoena or similar legal process, a fraud investigation, an audit, or examination, or the sale of an account to another financial institution.

AC has taken the appropriate steps to ensure that it is sharing customer data only within the above noted Exceptions. AC has achieved this by understanding how AC shares data with its customers, their agents, service providers, parties related to transactions in the ordinary course of business, or joint marketers.

Safeguarding of Client Records and Information

AC has implemented internal controls and procedures designed to maintain accurate records concerning customers' personal information. AC's customers have the right to contact us if they believe that records contain inaccurate, incomplete, or stale information about them. AC will respond in a timely manner to requests to correct information. To protect this information, AC maintains appropriate security measures for its computer and information systems, including the use of passwords and firewalls.

AC will use shredding machines, locks and other appropriate physical security measures to safeguard client information stored in paper format. Employees are required to secure client information in locked cabinets when the office is closed.

AC maintains physical, electronic, and procedural safeguards to protect the integrity and confidentiality of customer information. Internally, AC limits access to customers' nonpublic personal information to those employees who need to know such information in order to provide products and services to customers. All employees are trained to understand and comply with these information principles.

Privacy Notice

AC has developed a Privacy Notice, as required under Regulation S-P, to be delivered to customers initially and on an annual basis. The notice discloses AC's information collection and sharing practices and other required information, and has been formatted and drafted to be clear and conspicuous. A notice will be revised as necessary any time information practices change. A copy of AC's Privacy Notice is attached.

Privacy Notice Delivery

If two or more individuals jointly obtain a financial product or service, AC may satisfy the initial, annual and revised notice requirements by providing one notice to those individuals jointly. The firm will make every attempt to deliver the notice electronically to customers and maintain evidence of delivery. Prior to the electronic delivery, clients should consent to such delivery, and the Firm must provide a hard-copy, if requested, within 30-days of such request. In situations where the Privacy Notice is delivered via hard copy, the firm will maintain evidence of delivery by a method of the firm's choosing, whether it be certified mail receipt, client attestation, etc. The firm will maintain evidence of delivery in the firm's books and records.

Initial – As regulations require, all new customers receive an initial Privacy Notice at the time when the relationship is established.
Annual – The GLBA regulations require that disclosure of the Privacy Policy be made on an annual basis. AC delivers its annual Privacy Notice to all existing clients no later than April 29th of each year.

Revised – Regulation S-P requires that a company amend its Privacy Policy and distribute a revised disclosure to customers if there is a change in the Company's collection, sharing or security practices.

Regulation S-P: Privacy, Safeguards, and Disposal Policy

Addison Capital (the "Firm") has adopted this Regulation S-P Policy (the "Policy") to ensure compliance with Regulation S-P (17 C.F.R. Part 248) under the Investment Advisers Act of 1940, as amended by SEC Release No. 34-100155 (May 16, 2024).
This Policy establishes written procedures to protect nonpublic personal information ("NPI") of clients and consumers, ensure secure disposal of customer information, oversee service providers, and implement an incident-response and customer-notification framework consistent with the 2024 Reg S-P amendments.
This Policy applies to all employees, officers, and supervised persons of the Firm, and to all third-party service providers or affiliates that access or maintain customer information on behalf of the Firm.

Definitions and Applicability

- Customer Information – Any record containing nonpublic personal information about a client or former client, or a client of another financial institution, regardless of form (paper, electronic, or other).
- Sensitive Customer Information – Any element of data (alone or in combination) that could create a *reasonably likely risk of substantial harm or inconvenience* if accessed or used without authorization.
- Service Provider – Any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information in performing services for the Firm.
- Incident – Any unauthorized access to or use of customer information, or reasonable likelihood thereof.

Safeguards and Procedural Requirements

1. Information Security Program

The Firm maintains a Written Information Security Program (WISP) consistent with the Safeguards Rule.

2. Incident-Response Program

The Firm's incident-response plan is designed to detect, respond to, and recover from any unauthorized access or use of customer information.

3. Customer Notification Procedure

If the Firm determines that sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, it will notify each affected individual as soon as practicable, and in any case no later than 30 calendar days after awareness of the incident.

Notification Content: Description of the incident, categories of data affected, protective steps for the individual, and Firm contact information. If individuals cannot be identified, the Firm shall notify all whose information resided in the affected system.
Exception: Notification may be delayed if the U.S. Attorney General determines that immediate notice would pose a substantial risk to national security or public safety.
4. Service-Provider Oversight and Notification

- The Firm shall conduct due diligence on service providers that access or maintain customer information and ensure contracts require them to:
    - Implement and maintain safeguards consistent with this Policy; and
    - Notify the Firm within 72 hours after becoming aware of any security incident involving customer information.

5. Disposal of Customer Information
The Firm shall take reasonable measures to protect against unauthorized access to, or use of, customer information in connection with its disposal.
6. Recordkeeping
The Firm shall maintain all documentation demonstrating compliance—including incident logs, testing results, notifications, and vendor oversight—for five years, with two years readily accessible.

Testing and Reviews
The CCO will ensure at least annual testing of the Firm's safeguards and incident-response plan. Testing outcomes are documented, reviewed by senior management, and incorporated into remediation plans.