First Ascent Asset Management

INFORMATION SECURITY

First Ascent operates 100% in a cloud/web-based environment. There are no physical or virtual servers hosted onsite. The Advisor Portal, accessed by Advisor logins through our website, uses HTTPS, the communication protocol encrypted using Transport Layer Security.

Orion Advisor Technology

Portfolio Accounting, Investment Management, Trading, Billing, Reporting

Orion has adopted an Information Security Management System (ISMS) and is ISO/IEC 27001 certified. This certification is the highest security standard in the technology industry and verifies that they possess the required internal controls to operate, monitor and maintain an ISMS that:

- Meets both US and international guidelines
- Has been and continues to be reviewed and approved by accredited ISO auditors

Access Controls include but are not limited to:

- Multi-Factor Authentication
- Need-to-Know Access
- New Hire/User Access Forms
- Changes to Access Require Authorization
- Internal Audit Review
- Controlled Remote Access

TD Ameritrade Institutional

Primary Custodian

TD Ameritrade has a Security Risk Management department under the management of a Chief Information Security Officer (CISO) This Department has issued a formalized set of information security policies, standards and procedures which are in place enterprise-wide. All standards comply with all relevant laws and regulations and are benchmarked against ISO27001/2 and NIST standards for information security.

Access Controls include but are not limited to:

- Network Perimeter Security
- Internal Network Security
- System Auditing
- System Access Controls
- Security Operations

Anvil uses HTTPS, the communication protocol encrypted using Transport Layer Security. Heroku and Amazon host its servers.

- The database is encrypted.
- SSNs and DOB's are encrypted before sending to their servers. No one will ever know the clear text associated with that data.
- All data transactions are transmitted over an encrypted channel (HTTPS/SSL).
- Only server administrators have access to form submission data which requires 2-factor authentication.
- Anvil conducts 3rd party penetration testing and has Intrusion Detection Systems.

First Ascent's Information Security Policy

The purpose of the Information Security Policy and separate underlying procedures is to establish administrative, technical and physical safeguards appropriate to the size and complexity of the Firm. Implementation of the policy and underlying procedures shall:

- Ensure the security and confidentiality of client information;
- Protect against any anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any client;
- Ensure the proper disposal of client information;
- Exercise appropriate due diligence over external service providers, and require these vendors to provide appropriate measures designed to meet the Firm's control objectives; and
- Require compliance testing of all elements, including those services provided by external service providers.

Background

Cybersecurity is a growing concern and has become a hot button issue amongst business publications and consumer national news. Regulatory boards that monitor the financial services industry are taking note to quickly shift accountability to financial advisors. Cybersecurity is a critical aspect of success, business health, and keeping our clients' personal information safe.

Responsibility

The CCO has the responsibility for the implementation and monitoring of our safeguard procedures as it relates to both physical and cyber security.

Procedure

Key FAAM personnel, including the CCO, work with the firm's 3rd party IT consulting firm and employees to establish and follow a testing and maintenance program as it relates to security of its systems, hardware, and software, if applicable. Details of testing and maintenance are further outlined in the firm's security safeguard procedures, and include but are not limited to the following:

- Penetration Tests
- Vulnerability scans
- Patch management of hardware and systems
- Physical premises
- Social engineering
- Access rights
- Vendor management

First Ascent has also implemented additional security measures covering:

- Anti-Phishing Email Security Platform
- Managed Threat and Response
- Cybersecurity Awareness Platform and Training
- Advanced Malware Protection
- Email Full Content Scanning and Encryption
- Advanced encryption on laptops and other mobile devices
- Advanced spoofing/phishing protection