Your Data is Secure

The security and protection of your data is of the utmost importance to AssetLock®…

AssetLock® employs industry-leading technologies and policies to protect the confidentiality and privacy of each user's financial and personal data, and vigilantly updates its systems to stay at the forefront of security, privacy, and continuity protection. To assure this security, AssetLock® utilizes a number of different technologies including network security, application security, and encryption.

AssetLock® has partnered with ByAllAccounts to bring you AssetLock® Personal. ByAllAccounts, a subsidiary of Morningstar, has provided data aggregation services for more than 13 years and works with over 15,000 institutions to aggregate over $1.6 trillion in account data daily. The following security measures apply to both ByAllAccounts as well as AssetLock® Personal:

DIGITAL CERTIFICATES

Custodial integrator cabinet files and the service website are authenticated by digital certificates from a trusted commercial vendor. These digital signatures confirm the authenticity and the identity of the service with which data is exchanged.

SECURE CONNECTION – HTTPS

Connections to the service require HTTPS (HTTP over an encrypted SSL connection). Sessions on unencrypted connections are not allowed. AssetLock® also requires the use of "strong" encryption (128-bit ByAllAccounts; 256-bit AssetLock®), which ensures that the service uses the strongest measures possible to protect client data and communication.

SESSION MANAGEMENT

All service activities take place within an authenticated session, meaning that the user must log in before being allowed to do anything. Sessions are closed automatically after a period of inactivity.

DATA ENCRYPTION

All sensitive data is transmitted and stored encrypted, even when communication is between components of the service itself. Values that need to be decrypted for use are encrypted using a strong two-way encryption algorithm. Values that do not need to be decrypted are encrypted using a strong one-way encryption algorithm and cannot be decrypted. Decryption keys are maintained in a password-protected key store. The key store is not accessible from the machine(s) on which the database resides, nor is the key store present on any database back-up (where the data remains encrypted).

FINANCIAL DATA ACCESS ROLES

A hierarchy of roles and permissions defines who can access what financial data from within the service. These roles and permissions may be used not only to control who may edit information, but also to control who may see any of a client's personal information (account numbers, etc.)

AUDIT LOGS & NOTIFICATIONS

Use of any system administrative function (such as resetting a user's password) is recorded in a log file. These functions also send an email to the affected user.

INVESTOR ACCOUNT ACCESS

When an advisor and client are working together, this service allows registration of accounts at remote financial services for which information is to be gathered without the advisor ever seeing or knowing the credentials (username/login ID and password/PIN). The client is directed to a secure web form where this information is supplied, encrypted and stored directly in our database. No one other than the client sees these credentials during this process.

PASSWORD RETRIEVAL

Neither ByAllAccounts nor AssetLock® delivers or displays any password or PIN. It is not possible for a client, an advisor, an advisor's firm, or technical support personnel to "look up" a client's password—even at the client's request—for access to AssetLock®, ByAllAccounts, or any particular financial service from which information is retrieved.

If you have any questions about the security of your account, please contact your financial advisor.