

Security Procedures/Cybersecurity Notice

Processes that keep your investments safe

AQUAS Financial ("AQUAS") maintains certain personally identifiable information regarding Customers in its electronic databases to facilitate the processing of transactions on behalf of its Customers to comply with rules, regulations, and laws. The personally identifiable information stored on AQUAS' network is protected from unauthorized access, treated as confidential, and handled according to the terms of the AQUAS Financial Privacy Policy.

Our Systems

- We utilize advanced firewalls to keep unauthorized parties from gaining access to your personal information, as well as anomaly detection and intrusion detection technology to alert us to unusual behavior in your account.
- Firewalls keep our public web servers separate from the servers that contain your account and personal data, so they can't be accessed directly from the Internet.
- Our secure website uses either 128-bit or 256-bit encryption (depending on your browser setting) on the transmission of all data transmitted between our website and your computer.
- System backups reside in either secure facilities at AQUAS or in secure storage provided by a third party specializing in secure information management.
- Personally identifying information is generally not stored on laptop computers or other portable devices. All data stored on laptop hard drives is encrypted.
- All end point computers use antivirus software that is regularly updated.
- Operating System security patches are applied to all systems on a regular basis.
- AQUAS has adopted written policies and procedures reasonably designed to protect personally identifiable information.

Our Policies

- We will never send you an email requesting your account number, UserID, PIN, Password, or other similar information.
- We require clients to create unique UserIDs and alphanumeric passwords to log on to the secure website.
- We allow you to log in using your password and a one-time-use security code sent to you by email or text message, based on your delivery preference.
- We ask you to select four security questions to answer, to be presented to you when it seems an extra check of your identity is warranted, creating an extra layer of security for your account.
- Internally, access to client information is limited by a well-established computer security approach called "least privilege access" and "need to know," is firewall-controlled, and locks people out of internal systems after a minimal number of unsuccessful login attempts.
- Our employees are thoroughly trained in our policies and how to uphold them.

- If we detect suspicious activity in your account, we'll block access until you call us. We do this to validate that the account activity was intended by you, and to protect you in case it was not.
- Our [privacy policy](#) reflects the standards we adhere to.