

Cybersecurity & Client Data Protection

How we safeguard your information

A Layered Approach to Protecting Your Data

We maintain a defense-in-depth cybersecurity program designed to protect client nonpublic personal information (NPI) across its full lifecycle. This includes safeguards for data, systems, identities, and access points.

How We Protect Your Information

Data Encryption

- At Rest: Client data stored in databases, file systems, and cloud platforms is encrypted to prevent unauthorized access.
- In Transit: Data shared across networks and systems is encrypted using secure protocols to prevent interception or tampering.

Access Controls and Identity Protection

- Centralized identity management limits access to authorized users only.
- Single sign-on (SSO) reduces credential exposure.
- Multi-factor authentication (MFA) adds an additional layer of verification beyond passwords.

Continuous Monitoring and Response

- Endpoint detection and response (EDR) tools monitor systems, identities, and cloud environments for suspicious activity.
- Rapid investigation and response protocols help contain and resolve threats early.

Operational Safeguards

- Access to NPI is limited to employees who require it for servicing, compliance, or operational functions.
- Physical, electronic, and procedural safeguards are in place to prevent unauthorized access.

Regulatory Alignment

Our privacy and security practices are designed to align with:

- SOC 2 Trust Services Criteria
- SEC and FINRA requirements
- Applicable state privacy laws

Cyber Insurance

Our firm maintains cyber liability insurance coverage to help protect our clients and support response efforts in the event of a cybersecurity incident.

Shared Responsibility

Cybersecurity is an ongoing effort. While we maintain robust controls, we also encourage you to take simple steps to protect your own information, such as using strong passwords, enabling MFA, and remaining cautious of phishing attempts.

You should also be wary of unsolicited emails or texts that appear to come from Wealth Enhancement.

- We will never contact you to ask for your password, user name, or personal information.
- If you receive an unsolicited call, hang up. Instead, contact your advisor directly using a known, verified number from a previous statement, not a number provided in a suspicious text or email.
- Don't ever transfer funds or give your permission for funds to be transferred on your behalf without verifying the transaction by contacting a known advisor.
- Use the Wealth Enhancement Client Portal to send secure messages or transfer files. Never send financial information by email.

OUR COMMITMENT

Protecting your information is foundational to how we operate. Our systems, processes, and teams are structured to reduce risk, safeguard sensitive data, and support the long-term security of your finances.

For more information, visit wealthenhancement.com/security.

This document is provided for general informational purposes and does not provide legal, technical, or cybersecurity advice. While we maintain active safeguards, we cannot guarantee that cybersecurity incidents will never occur. Our cybersecurity controls, processes, and tools may change over time and without notice in response to evolving threats, regulatory requirements, and business needs.