

Data Security Policy

Last Updated: January 1, 2026

ATIV, LLC is committed to protecting the confidentiality and security of client data. This Data Security Statement describes our general approach to safeguarding information.

Security Measures

We maintain commercially reasonable safeguards designed to protect information from unauthorized access, disclosure, alteration, or destruction, including:

- Secure client portals for document exchange
- Access controls and authentication measures
- Limited internal access based on role and necessity
- Use of reputable third-party platforms with security standards

Client Responsibilities

Clients play a critical role in data security. Clients are responsible for:

- Maintaining confidentiality of login credentials
- Using secure networks and devices
- Promptly notifying us of suspected unauthorized access
- Transmitting documents through approved secure channels

We are not responsible for security incidents resulting from client negligence or unauthorized credential sharing.

Third-Party Platforms

Our services rely on third-party software providers (e.g., accounting platforms, payment processors, portals). While we select reputable vendors, we are not responsible for outages, breaches, or security failures attributable to third parties.

No Absolute Guarantee

Despite reasonable safeguards, no system is completely secure. We do not guarantee that information will be immune from unauthorized access, loss, or misuse.

Incident Response

If we become aware of a data security incident affecting client information, we will take reasonable steps to assess the issue and comply with applicable notification obligations.

Updates

This Data Security Statement may be updated periodically. Changes will be posted on our website.

Contact Information

Questions regarding this Data Security Policy may be directed to:

ATIV, LLC

2017 Bald Eagle Way, Eagle Mountain Utah 84005

ambert@ativfinancials.com

(801) 232-6340