Data Security Measures

At Evolved Finance, protecting your data is our top priority. After consulting with leading data security experts, we've implemented robust processes and procedures to ensure that all sensitive information in our care remains secure.

We continuously update our systems and practices to stay ahead of the latest advancements in technology and data security standards.

Our approach to safeguarding sensitive data focuses on three key areas: Human Resources, Hardware & Software, and Client Interactions. Each of these categories plays a critical role in maintaining the highest level of security for your information.

Human Resources

Educating our employees is the first line of defense to ensure that any sensitive data we have access to is not shared inadvertently. We understand that human interaction with any type of malware is the biggest threat we face. As such, every employee that works at Evolved Finance is required to read and understand all relevant sections of IRS publication 4557 when they are hired.

Anyone who works at Evolved Finance that has access to confidential and/or sensitive information is a United States based employee, and has undergone an independent and detailed background check to verify:

1. Their Social Security number
2. Their identity
3. Their education experience matches their resume
4. Their employment history matches their resume
5. They are not sex offenders
6. They are not on the domestic watch list
7. They are not in any nationwide criminal databases for any offense
8. They have not been the defendant of any federal criminal court cases
9. They have not been the defendant of any county criminal court cases

Some of the items we check for may seem insignificant or even irrelevant. However, in our eyes checking for all of these items helps to ensure that we are hiring a trustworthy human in all areas of life.

Furthermore, in an effort to reduce exposure to sensitive information - any document, spreadsheet, and/or password we have access to is shared ONLY with the necessary team members.

Hardware & Software

When it comes to data security, hardware and software play a critical role in our overall strategy to keep sensitive data safe. By leveraging hardware and software, we can create a barrier between cyber criminals and sensitive information. Below is a list of our internal protocols that help us ensure sensitive data is kept safe:

1. All of our computers are encrypted, which protects information from being read on our computers if they are ever lost or stolen.
2. All of our computers use a Firewall, which blocks unwanted connections regardless of network settings.
3. All of our computers are registered with Apple's #1 preferred Mobile Device Management software, Jamf. Jamf gives us control to remotely wipe and manage every device that carries, stores, and/or has access to sensitive information.
4. Anti-virus software is installed proactively before any computer is used to prevent bad software from causing damage or compromising a computer.
5. Anti-malware is installed as well, which prevents unauthorized software from stealing information that is on a computer.
6. We use LastPass to manage, store, and share passwords internally. Additionally, we've enabled a setting to prevent foreign IP addresses from accessing LastPass.
7. We host all sensitive data and documents using Google's encrypted business class software, which is actively monitored and optimized using the latest security technology available.
8. We use strong passwords of ten or more characters that are auto generated via LastPass. The passwords include special and alphanumeric characters and we do not use the same password for any two accounts.
9. We require multi-factor authentication whenever possible, including requiring the use of YubiKey to authenticate LastPass and Google.
10. All of our computers are password protected and are programmed to auto-sleep after 10 minutes of inactivity.
11. Before any computer is decommissioned, we wipe the hard drive clean of all data.

Client Interactions

As we work with you on a monthly basis, please keep in mind a few important details about how we operate:

1. We will **never** ask you to share a username and/or password via email and we ask that, in return, you refrain from doing so as well.
2. We ask that any sensitive information you share with us be provided using your secure account information spreadsheet or, if you're a tax client, TaxDome.
3. We frequently require 2-step verification codes from our clients. Most of the time we will ask for this code via text from our main phone number, which is (424) 241-3350. However, when we know a code will come via email to a client, we will ask for those codes via email from an @evolvedfinance email address. **We will never contact you from any other phone number or alternative domain.**
4. Please save our company phone number to your phone so you know it is us - **(424) 241-3350.**
5. If you are ever unsure about a request from us, please do not hesitate to call us to verify first.

For any questions related to the above security measures, please reach out to info@evolvedfinance.com.