1847Financial | HTK

What to consider when selecting or using a third-party vendor

FOR FINANCIAL PROFESSIONALS

Here are some best practices from Penn Mutual Information Security to consider when selecting or using a third-party or vendor services or solution for your business:

- **Always be diligent by researching the reputation of a prospective vendor, service or application before signing a contract or signing up for a service or application.**
    - You should verify the business is legitimate.
        - To verify a U.S. company is legally registered, you can view the "Secretary of State Website" in the state's official website where the business is operating.
    - Leverage public resources such as the **Better Business Bureau** and ask for client references so you can find out more information.
    - Ask or verify if the company has offshore resources that support your solution (this isn't an issue directly, but depending upon what function they provide, this may provide an elevated risk), in general, your clients may or may not like their personal data shared and/or stored outside the U.S.
    - Popular information security verifications (attestations) would include a SOC2 Type 2 Report, ISO 27001 certification, or SIG report. A company who has these and/or other certifications does NOT guarantee their program is mature and/or their ability to protect your data. However, generally a company with these types of certifications will have a more mature information security program than those without it.
        - It's a good rule of thumb that the more volume and/or personal data that a company/software requires you to provide, the more mature you should expect their information security program and practices to be.

- **Always make sure you have read and understand the Terms of Service or contract.**
    - Users are expected to read, understand and conform to the license requirements of any software products they use or install.
    - Look for details about who is responsible for liability, penalties and costs if a security or data loss event occurs.
    - Be sure to look at the privacy policy (often there will be a link at the bottom of a website to security or privacy and contain important information there) to determine what a company will do with your information and who owns it after you sign up or accept the Terms of Service.

- **Ensure any software you purchase is receiving, and will continue to receive patches (or updates).** This is an important way that companies provide fixes to bugs and/or vulnerabilities that exist in software. If they remain unpatched, bad people can take advantage of the vulnerabilities and cause harm or disruption to your system.

- **Be wary of "free" software, as in most cases you are then the product (meaning your personal data and/or usage is often sold and/or marketed to other companies for your usage of their product for free).** In most cases, using a pay-for-use product vs. a free tier product will provide some or all of the following benefits:
    - Privacy policy improvements (typically they're less likely to sell your private information if you pay to use or you may have the choice to opt-out.)
    - Ongoing patches/updates
    - Support (such as a helpline and/or email support)
    - Upgraded security controls
    - Upgraded functionality