HINKLE LAW FIRM LLC
hinklaw.com 316.267.2000

JANUARY 24, 2023

EAT BETTER, WORK BETTER, AND PROTECT DATA BETTER: NEW YEAR RESOLUTIONS FOR THE TAX PROFESSIONAL AND USEFUL TIPS

January brings a fresh start for many businesses as they gear up for the New Year. It is when tax professionals meet with clients and request financial records to prepare tax returns for the prior calendar year. It is also a busy time for accountants, HR staff, and payroll departments responsible for preparing W-2s for employees and 1099s for independent contractors.

When you stop to think about the type of information contained in a tax return, W-2 or 1099, or included in your financial records, it is obvious that these documents are comprised of mainly personally identifiable information ("PII") and other very sensitive data. If this type of information falls into the wrong hands, the results could be detrimental to your employees' or clients' privacy and financial security (not to mention potentially exposing you to significant liability). Consequently, it is imperative for all tax professionals to implement good privacy practices and security controls to protect PII and financial information from unauthorized access or use.

Data security is a necessity regardless of the size of your client base or business. More than that, protecting taxpayer data is the law. The Federal Trade Commission ("FTC") has authority to set data safeguard regulations for various entities, including professional tax return preparers. The failure to comply with FTC regulations could result in an FTC investigation, unwanted audits, and fines, as well as a damaging smear on your business's reputation.

According to the FTC Safeguards Rule, tax return preparers must create and enact written information security plans ("WISPs") to protect their clients' data. In doing so, tax professionals and other financial advisors should assess and mitigate risks to taxpayer data in all areas of operation, including (i) employee management and training; (ii) information systems; and (iii) detecting and managing system failures within your network. Additionally, the Internal Revenue Service ("IRS") has issued guidance to tax professionals on protecting their client's data by

Wichita Office
1617 N. Waterfront Parkway
Suite 400
Wichita, KS 67206
316.267.2000

Kansas City Office
Lenexa City Center – Penn I
8711 Penrose Lane
Suite 400
Lenexa, KS 66219
913.345.9205

implementing strong security protocols. https://www.irs.gov/tax-professionals/tax-security-2-point-0-the-taxes-security-together-checklist.

Every employee, both professional and administrative staff, should be educated about security threats and safeguards when it comes to employee or client data. Businesses should also implement good privacy practices in daily operations. To help you out, we have prepared some helpful tips on ways to implement good privacy practices. We hope they are useful to you.

For more information about compliance with the FTC Safeguards Rule or IRS's requirements on tax professionals, or for assistance with preparing a written information security plan or other privacy policy or plan, please contact Krystle Dalke, CIPM and CIPP-US, at (316) 631-3181 or via email at kdalke@hinklaw.com. We can also help you perform risk assessments, train employees, and mitigate risks of unauthorized access to sensitive data or confidential information within your business operations. The sooner you start engaging in good privacy practices, the more trustworthy and prepared your business will be.

Useful Privacy Practice Tips for Tax Professionals

- Know your data: Identify the types of data you have, where it is stored, and who has access to it.

- Perform a risk assessment to identify risks of data loss and unwanted access to confidential data and mitigate against those risks, starting from highly confidential data to publicly available data and factoring in business need, brand reputation, and legal compliance.

- Implement security controls designed to limit access to data and protect against data loss and theft, including:
    - Categorize data based on sensitivity and limit account access based upon legitimate business needs;
    - Opt for two-factor authentication;
    - Use offsite backup software and services;
    - Use drive encryption;
    - Segregate sensitive data from other data; and
    - Create and secure Virtual Private Networks.

- Establish protective barriers against unwanted intruders by:
    - Activating anti-virus software;
    - Use of a firewall; and
    - Creating a patch management schedule that is timely and proactive.

- Develop a data security plan.
    - Federal law requires all professional tax preparers (as well as several other types of businesses and industries) to create and maintain a written information security plan for client data.
    - Make sure your plan is legally compliant with governing laws, but also tailor it to be achievable by your staff—Don't set up your employees for failure by implementing rules that you know will not, or cannot, be obeyed.
    - Focus on key areas that mitigate harmful risks to sensitive data and protect your business's proprietary information.

- Educate and train your employees and contractors to identify suspicious activity and use good privacy practices.
    - Learn how to identify and react to suspicious activity on your network;
    - Spot phishing emails or other solicitations;
    - Recognize signs of unauthorized access or data theft;
    - Set-up and use secure email accounts or online file-sharing accounts with encryption to protect information transferred to, or requested from, your employees, contractors, and customers;

HINKLE LAW FIRM LLC

  - Use strong passwords and encryption to protect data at rest or in transit; and
  - Avoid needless downloads and saving confidential information on unsecure drives.

- Create a data loss recovery plan and business continuity plan and make sure these plans are readily available to your staff.
  - A data loss recovery plan (also known as a disaster recovery plan) establishes instructions for your staff to follow to identify, eradicate, recover from, and mitigate against unwanted data loss or theft.
  - A business continuity plan establishes steps or guidelines to keep a business operational in the event of a cyber attack or other data loss or theft.