January 24, 2023

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;
  - 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.

Krystle M.S. Dalke
Attorney – CIPM, CIPP/US
kdalke@hinklaw.com
316-631-3181