itnext

next generation | it consulting.

Safeguarding Taxpayer Data

Data security can protect your business as well as your clients

Cisco Meraki · CrowdStrike · DNSFilter · OpenDNS · Datto (The Leader in Backup and Disaster Recovery) · Fortinet · Sophos (Security made simple.) · Malwarebytes · SentinelOne · TitanHQ · Palo Alto Networks

Federal Trade Commission

FTC Compliant

Under the Safeguards Rule, financial institutions must protect the consumer information they collect. Learn if your business is a "financial institution" under the Rule. If so, have you taken the necessary steps to comply?

Many companies collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.

But safe-guarding customer information isn't just the law. It also makes good business sense. When you show customers you care about the security of their personal information, you increase their confidence in your company. The Rule is available at ftc.gov.

The definition of "financial institution" includes many businesses that may not normally describe themselves that way. In fact, the Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services.

https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

National Institute of Standards and Technology

NIST - Information Security Fundamentals

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure.

Small businesses are an important part of our nation's economic and cyber infrastructure. According to the Small Business Administration, there are approximately 28.2 million small businesses in the United States. Small business is defined as an organization/business of less than five hundred employees. These businesses produce approximately 46 % of our nation's private sector output and create 63 % of all new jobs in the country [SBA FAQ].

For some small businesses, the security of their information, systems, and networks might not be their highest priority. However, an information security or cybersecurity incident can be detrimental to their business, customers, employees, business partners, and potentially their community. It is vitally important that each small business understand and manage the risk to information, systems, and networks that support their business.

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

IRS

IRS - Protecting Taxpayer Information is the law.

Data thefts at tax professionals' offices are on the rise. As the Security Summit makes progress, identity thieves need more taxpayer data to file fraudulent tax returns. And they have placed tax practitioners firmly in their sights. Data security is now a necessity for every tax professional, whether a partner in a large firm or a sole practitioner, and every Authorized IRS e-File Provider. Every employee, both professional and administrative staff, should be educated about security threats and safeguards. Everyone has a role to play in protecting taxpayer information.

Protecting taxpayer data is the law. Federal law gives the Federal Trade Commission authority to set data safeguard regulations for various entities, including professional tax return preparers. According to the FTC Safeguards Rule, tax return preparers must create and enact security plans to protect client data. Failure to do so may result in an FTC investigation. Online providers also must follow the six security and privacy standards in Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns.

Protecting taxpayer data is good business. Data security can protect your business as well as your clients. A theft may also mean a loss of reputation, a loss of clients or a loss of money. Consider engaging security professionals for assistance or check with your professional liability carrier about data theft coverage.

https://www.irs.gov/pub/irs-pdf/p4557.pdf

How can we help?

ITNEXT has the experience and knowledge to help protecting your business.

We've built a checklist of all requirements specified by the IRS, NIST and FTC in order to make it easy for our customers. We've leveraged key enterprise technologies and strategies to make it affordable to Small Medium Business. We provide enterprise level security infrastructure through our partnerships with the most recognized vendors in the industry. We know one solution does not fit all customer's needs, and that is the reason why we have come up with a checklist that can be mapped to different technologies from different providers. We, as consultants, our job is to determine the best strategy based on your needs.

Checklist

	REQUIREMENTS	PRIORITY	DONE
Endpoint Protection	Anti-Virus, Anti-Spyware, Personal Firewall	High	○
	Drive Encryption	Medium	○
	DNS Filter (Anti-Phising, Content Filtering, Threat Protection)	High	○
Network	Network Firewall (Web and Email Filters)	High	○
	Cloud Managed Switch and Secure Wireless Access	Medium	○
Stored Client Data	Automated Encrypted Backups to the Cloud (Ransomware free)	Medium	○
	Folder Based Backups (Files only, MAC and Windows)	High	○
Secure File Sharing	If you must share files with clients via email (SSN, etc), send only password-protected and encrypted documents.	High	○
	Cloud File Sharing with encrypted and password protected features, temporal URLs, Mobile Apps available.		
	The File Sharing portal can be customized with your Logo, Colors, etc and provide secure access to your clients.		
BCDR	Busines Continuity and Disaster RecoveryCloud File	High	○
	In case of data loss, like stolen computer, natural disaster, or hardware failure. This allows to restore your info.		
	Imaged Based Backups (Entire Windows system, including apps). All backups are checked for Ransomware		

itnext

next generation | it consulting.

SOCIAL NETWORKS

www.itnextus.com

Itnext 2717 Commercial Center Blvd, Ste E200, Katy, TX 77494.
Phone: 214 226 81 71 | E-mail: info@itnextus.com