(This content is rented from CPA Site Solutions)

Client Portal Security Measures

"Our Client Portal is the Most Secure Client Portal available on the market."

Your data is protected in extremely secure environments. Most Client Portal vendors provide 5 or 6 layers of security. Woltman Group, PC, uses CPA Solutions as their portal. If you would like to read more details please click on the PDF below.

(PDF)

1. SAS 70/SSAE 16 Certified Datacenter

Not all datacenters are alike. You don't want your client's data hosted on a low cost "cheap" datacenter. The best datacenters are both SSAE 16 and SAS 70 Type II certified. That means a specially trained CPA Firm performed an in-depth audit attesting to the fact that the datacenter has sufficient processes, controls, and safeguards to keep your data safe from theft, corruption or mishandling.

Unlike the Type I Certification which only measures a certain point in time. The Type II Certification measures and evaluates security over time.

The Sarbanes-Oxley Act requires all publicly traded companies to use SSAE 16/SAS 70 Type II Certified datacenters. So you can protect yourself the same way publicly traded companies protect themselves, because all of CPA Site Solutions' Servers are located in high quality SSAE 16/SAS 70 Type II Certified Datacenters.

The servers are housed in a secure, 24/7, around-the-clock, guarded facility with closed-circuit motion sensitive video surveillance. Physical access to the servers is strictly limited to only authorized datacenter personnel. And all personnel are further restricted by Dual Factor Biometric Authentication Barriers.

2. Encrypted File Storage

Almost all Client Portal providers encrypt the data as it's transferred to the server. But what they fail to do is encrypt the data when it's on the server. Since the data spends almost all it's time on the server, we feel it's necessary to store the data in an encrypted format.

If this were easy to do, everyone would be doing it. Storing data in an encrypted format requires a lot of programming from extremely high level security experts. All the encryption and decryption places a heavy load on the server's processors so significantly fewer accounts can be

placed on each server.
It's expensive, but worth it when you consider that encryption is considered the most effective method of securing personal and corporate information according to corporate and government security regulators. In fact, many data protection laws specifically list encryption as a "safe harbor" exception to notification rules, and some laws explicitly require the use of encryption.

3. High Level Filename Obfuscation

As an additional level of security all of the filenames stored on the server are completely unrecognizable. Instead of meaningful filenames they are listed as a totally random set of characters and numbers.
On the very unlikely event a hacker finds their way into our servers, they would find it impossible to make any sense of the files. And remember, they can't read the content of the files because all files are encrypted.

4. Forced SSL Transfer

Hackers have many ways to intercept data that is transferred insecurely over the web. And now it's even easier with the wider use of laptops and wireless routers.
The best way to protect your data is to transfer the data over a Secure Socket Layer (SSL). SSL encrypts the data so the data is absolutely useless to anyone who goes through the effort of capturing it.
You are always protected because the Client Portal automatically recognizes if a user is trying to transfer information insecurely. The Portal then forces the transfer to occur under an encrypted Secure Socket Layer.

5. SQL Injection Protection

SQL Injection is a method hackers use to break into databases. Once in a database, a hacker can easily wreak havoc. Millions of websites are hacked with SQL injection every year. Even the United Nations website was recently hacked using SQL injection and cost hundreds of thousands of dollars to repair.
CPA Site Solutions' Client Portal renders SQL Injection attacks completely useless because it utilizes the "Best Practice" of parameterized data calls.

6. Brute Force Login Protection

Brute force attacks occur when a hacker writes a program that runs through millions of common username and password combinations to gain access to a secure system.
You are protected from Brute Force attacks because after 3 incorrect login attempts the Client Portal uses CAPTCHA technology which requires a human to read an image that appears. This stops computer programs from guessing correct user and password combinations.

7. Strong Password Policies

Weak "easily cracked" passwords are unsafe. The client portal never allows weak passwords and allows firm administrators to require users to create passwords that meet certain levels of strength.

8. State-of-the-Art Firewall

CPA Site Solutions uses a state-of-the-art CheckPoint UTM-1 Edge Firewall that is configured with the least number of ports open and advanced IP restrictions.

9. Real Time Virus Scanner

The server is continually scanned for viruses and the virus database is updated every hour.

10. Encrypted "Cross Server" Backups

Another common hack is to attack and gain access to backups. Backup media often is held and transferred in "less secure" environments. Hackers know this and often find ways to gain access to backup data. This is impossible with CPA Site Solutions' Client Portal because the backup files are encrypted and stored in extremely secure facilities. Even if a hacker got their hands on our backups they would not be able to access any information because of the high-level file encryption.

11. FireSlayer - Denial of Service Attack Protection

The servers are additionally protected from denial of service attacks. A denial of service attack is made when a virus infects thousands of computers on the Internet. Then all those infected computers make repeated requests to a single server. The targeted server often can't handle the load and crashes. The FireSlayer system detects this kind of activity and automatically blocks the abusive traffic on-the-fly.

12. TippingPoint - Intrusion Prevention System

Hackers attempt to gain access to servers in many different ways. That's why we use the award-winning TippingPoint Intrusion Prevention System. This system fully inspects every packet of data coming to the servers, then instantly determines whether it's legitimate or malicious. This instantaneous form of protection is the most effective means of preventing attacks from ever reaching their targets.

13. Detailed Audit Trails and Reporting

All accounting firms must comply with the Gramm-Leach-Bliley Act and are specifically accountable for the safe and verifiable delivery of sensitive information. Firms must additionally make sure the intended recipient is the only recipient.

The Client Portal provides records of every transaction and allows you to...

- Reduce the time and cost of complying with privacy regulations
- Prove that information has not been leaked
- Eliminate the customer service costs associated with disclosure of a data breach
- Eliminate the legal liability associated with data breach disclosure

14. Operating System Hardening and Patch Management

There is a lot more to managing secure servers than you may realize. Server Operating Systems are not secure when they come out of the box. It takes highly skilled software technicians to hone and harden the System Software to minimize exposure to current and future threats.

Our servers are continually updated with the newest OS patches, hot fixes and updates to reduce the threat of security attacks and system downtime.

These advanced security measures are fully compliant with Sarbanes-Oxley and Gramm-Leach-Bliley.