Centerbase

Security & Data Redundancy

The Protection and Security of your Firm's Information is a Core Competency at Centerbase:

At Centerbase, we understand your responsibility to your clients to keep their personal information safe, secure, and confidential. With over 16 years of incident-free experience hosting clients in our secure Cloud infrastructure, we create a safe environment for both you and your client's information.

Centerbase understands that while many law firms are excited about the prospect of moving to the Cloud, they also feel anxious about losing direct control and physical access to their data. Concerns over where those servers are located and who has access to them naturally arise, and we are excited to answer them.

This document outlines the measures and processes we utilize to provide a safe and secure Cloud-based solution for your data.

A Summary of Centerbase's Security Practices:

Physical Security	Data Privacy	Data Redundancy
Centerbase owns and operates private servers in SSAE 16, SOC1&2, HIPPA Compliant ITAR, EUUS Privacy, GLBA, PCI Colo, and PCI Demarc certified datacenters. Our datacenters are in nondescript locations protected by secured perimeters and 24- hour security. Datacenter access requires photo ID, keycode, badge and biometric screening. Individuals must be on a screened and preapproved list.	Centerbase encrypts all client backups with industry standard 256-bit AES encryption before writing the data to our servers. We use industry standard SHA256 4096 bit RSA encryption for all data transmission and 256-bit AES encryption when storing at rest backup data. With our 256-bit AES backup encryption. Brute force attacks would require over 1 trillion years to break through these measures.	Centerbase owns and operates private servers in SSAE 16, SOC1&2, HIPPA Compliant ITAR, EUUS Privacy, GLBA, PCI Colo, and PCI Demarc certified datacenters. All Centerbase databases are continuously backed up. 20-minute restore points are available for 2 days, and daily backups are kept for 28 days. Centerbase maintains a mirrored disaster recovery location, which is fully capable of taking over in the unlikely event of catastrophe at our main datacenter locations.

Centerbase's Cloud Computing Platform:

The Centerbase cloud is built on industry standard and trusted platforms that power much of the internet today. Our server hardware and firewalls are enterprise class systems from Dell Computer. We run 24/7 high availability VMWARE clusters that allow us to keep your services up and running continuously. We constantly replicate our main site to our off-site disaster recovery location to allow for a quick transition in the unlikely event of a catastrophe in our main location. Our servers have resided in our current main facility for over 14 years without need for a single failover. We have maintained a 99.999% uptime over the last 14 years, an average of < 5 minutes of down-time per year.

Physical access to our facilities is incredibly secure, requiring pass cards, ID cards, biometric eye scans, and pre-screeningautorization to enter the building. Within the facility, an authorized 3rd party is required to physically unlock the cages where your information is located.

Owning our own infrastructure allows Centerbase some unique and valuable advantages over companies that host your services in 3rd party providers. Our team intimately knows the systems that make up our infrastructure. Hosting your data on 3rd party providers raises questions such as: How old are the servers? How many hours they have logged? Are upgrades and investments made regularly to ensure my data is protected by the up-to-date security measures? We manage our own internet border security, firewalls and security policies and have over 16 years of incident-free experience. We design our systems to actively refuse connections from high risk countries known for hacking activity. We also continuously monitor our systems for vulnerability and malicious activity in order to constantly stand vigilant against cyberattacks and DOS incidents.

Our datacenters hold every conceivable certification for safety and security best practices. Our main datacenter:

- Boasts over 68,000 square feet of environmentally controlled, secure data center space.
- Has a true 2N power and multi-homed connectivity from leading carriers.
- Offers 24 x 7 x 365 onsite personnel, biometric access, physical ID check and more than 100 internal and external video cameras (with 90-day video storage).
- Maintains six (6) backup diesel generators on standby with on-site fuel capacity of over 50,000 gallons, which are tested bi-weekly and routinely run at full load.
- Has superior connectivity through 15 on-net providers with access to 65 additional providers through layer 2 connectivity.

Centerbase's Cloud Computing Platform:

Centerbase has been in the SaaS online hosting business for over 16 years. We practically grew up with the boom of Software as a Service, and moving clients from in-house, server-based systems into the cloud.

This allows us invaluable experience helping law firms confidently take advantage of the benefits of moving to the cloud. We constantly improve and develop our proprietary platform to take advantages of the cloud. With Centerbase, you are choosing a partner that has the experience to provide expert council, advice, and service.

Encryption:

Protecting your data, both in transit and at rest in our database, is critical to your piece of mind. Centerbase employs industry standard SHA256 4096 bit RSA encryption from your browser to our datacenter. This is the same secure transport used by banks, healthcare providers, and nearly all other secure internet services.In addition, we encrypt all backups of your data using 256-bit AES algorithms. Data Transmitted to our disaster recovery location facility is always encrypted during transport using AES-256 bit encryption over the wire. These measures help ensures that your data is safe at Centerbase.

Application Security, Audit and Change Logs:

Centerbase contains a user-definable change tracking, audit log and deletion log system. From an easy to use dashboard, you can quickly review all the activity by user that is happening in the system. You can easily see what is changed. This log contains the name of the user, the item being changed, and the old and new values.

Application Security, Audit and Change Logs: 3. In addition, you can see what items have been deleted from the system, and by whom. The system also provides a monitoring tool, so you can see who is logged in, and even log out users if needed remotely. Our advanced application level security settings allow you to set permissions to any data in the system on a user or group policy basis. It's easy to allow or restrict access to financial data, billing rates, sensitive documents, and cases to only those individuals that need access.

Our webserver also logs and monitors every connection and communication that is made with your system. We store the IP address, what is being accessed, and the date and time of all interactions. This detailed level of logging allows you and us to understand exactly who is using and accessing your system at any time.

Uptime and Performance Monitoring

We keep a close eye on the performance and response time of your system. Offsite monitoring software constantly monitors our infrastructure for issues before they become failures. All client sites are part of a high availability group, so even a server hardware failure would mean only a few minutes of downtime while another server immediately picked up the workload for you site without loss of data. We also monitor each client's website for response time to make sure you experience great performance. Our network operations center contains large displays to immediately indicate warning and issues visually to our team, who also monitor these operations on their individual workstations. Finally, our operations staff is notified via text and email when issues arise, and are on call and available 24 x 7 x 365 to make sure your systems are up, running, and available to you. We understand there are no excuses if you have deadlines and court dates. Things need to work. All the time. No exception.

Conclusion:

We hope that this document has helped you understand more about our capabilities and commitment to protecting your information. We believe our cloud hosting and cybersecurity knowledge built over 16 years of incident-free experience in the cloud makes us a leader in Cloud-based practice management, billing and accounting software. If you have any further questions about our procedures and practices, please do not hesitate to reach out to our team, we are happy to help!