How ***TouchPoint*** Works to Keep Your Data **Safe in the Cloud**

TouchPoint

People Focused. Ministry Maximized.

How TouchPoint Works to Keep Your Data Safe in the Cloud

With what feels like an increase in breaking news stories about hacks and stolen data, cloud security is top of mind for many of today's organizations—including churches.

While the convenience and capabilities of cloud services are a huge benefit for your church, you also want to know that your data and the data of your congregation members is safe and secure.

At TouchPoint, we know your data is important to you.

And it's incredibly important to us, too. We take our responsibility to give you secure, convenient, fast, and reliable access to your database very seriously. That's why we have a number of protections in place to keep your data secure.

In this resource, we'll explain some of the ways we're working to protect your information so you can be confident your data will be safe in the cloud.

Where Is Your Data Stored?

You know your data is in "the cloud," but what does that really mean? It means you don't need your own on-site facility with hardware for storing all your information and the software you're using. Instead, you are accessing that information remotely over the Internet from a secure data hosting environment.

But cloud or no cloud, your data still needs to be stored on a server in a physical space somewhere. In the case of TouchPoint, **we host your data on our own servers at Rackspace—a world-class, widely known data center**. Our servers are located in their Chicago data center, where only authorized employees have physical access to the servers.

Here are some of the ways Rackspace provides us (and you) with peace of mind:

Private Managed Cloud

Rackspace manages a set of dedicated servers for our account. We do not share any resources with any other Rackspace customer. We have two 16-processor servers, a firewall, and a load balancer in our managed cloud. Rackspace monitors all of our critical services and has 24/7 support.

Proactive Monitoring

Rackspace pro-actively monitors all of our hardware for potential problems. If a problem should occur, Rackspace responds quickly.

Layers of Protection

When sensitive information is being shared, you want to be sure the right protections are in place. We've thought about these things and taken action to provide additional levels of security in the places you need them most.

Here are a few key examples:

Secure Sockets Layer (SSL)

We have a wildcard SSL certificate, which secures all traffic between our web server and your browser. This means that all data is encrypted over the wire, so no hacker can "sniff" your data and see what you're sending and receiving. If you are sitting in Starbucks working on your church management system, you don't have to worry about someone stealing important information over the network.

**Important note: While this capability protects your information from being stolen over the network, it does not protect you from someone looking over your shoulder and seeing the information on your screen. The most dangerous and effective hackers do not use code or hardware to get your data—they use social hacking techniques like these.*

Credit Card Data

TouchPoint provides integration with Sage Payments, Authorize.Net and TransNational to allow you to set up online giving and other fee-based registrations. **We do not store any Credit Card or Bank Account information on our servers.** A user can save his payment information but we put it in a secure Vault service through one of these gateways. We cannot see the information. All we can do is issue transactions on this saved payment data, via the gateway.

Social Security Numbers

Social security numbers are not accessible or stored in TouchPoint. The only time we ever store Social Security Numbers is when you do a background check using our integration with Protect My Ministry. Even then we encrypt the social security number in such a way that even with physical access to the database you would not be able to retrieve the actual number.

Preventing Downtime and Data Loss

Today's data security is about more than just having the right server. It involves taking precautionary action and planning ahead to prevent problems before they occur.

Here are some ways we do that:

1. Web Farm

One of our servers is a hypervisor with three virtual web servers. That might sound like techno jargon, but what it means is we can publish new features and bug fixes at any time, even while activity is high, without disrupting service. While each server is updated with new software, the other two handle the requests. This helps ensure uptime for your system.

2. Disaster Recovery

Our plan for disaster recovery is built around the cloud. We are software developers and software support analysts, not networking, hardware or IT experts. That's why we outsource this expertise to proven, trusted companies in the cloud such as Rackspace. This is a critical component of our disaster recovery plan.

Our disaster recovery plan includes:

- Hosting everything in the cloud
- Using multiple service providers that are the best at their area of focus
- Being agile and as agnostic as possible about which service we use

For example, we use the following cloud services:

- Rackspace (for hosting of our data and web servers)
- SendGrid (for email)
- GitHub (for hosting all of our source code and documentation)
- WordPress.com (for our website and blog)

Our disaster recovery plan is as follows:

- Establish accounts at a new cloud provider
- Move all backups to this provider
- Install software on this new provider
- Point our DNS to this new provider
- Finish this whole process in under six hours

**We have tested our Disaster Recovery Plan in a real, live situation with successful results.*

Your Own Database

Every church client in TouchPoint has their own separate database. Even though all churches share the same web servers, each church's data is isolated from all the others.

Backing Up Your Database on a Regular Basis

Ask anyone who's ever forgot to save an important document and lost hours of work knows: Backing up your files is essential. It's no different with your church's database. You want to ensure, no matter what, you'll never lose all your vital information.

Here are the backup plans we use to protect your data:

Main Backup Plan

- Your database is backed up daily at 1:00 AM
- We copy your backup to a separate cloud files infrastructure
- We keep daily backups for the first month
- Then we keep weekly backups for the next 8 weeks
- After that we keep monthly backups

Weekly backups are performed every Wednesday. Monthly backups are performed on the first Wednesday of each month.

Image Backup Plan

- Your image database can be much larger than the main database but has less critical data
- Your image database is backed up daily at 1:00 AM
- We keep the most recent backup on our database server
- Each Saturday, we copy the most recent image backup to the cloud files infrastructure

Your backups are stored in a separate location from the database server. At any point in time, your data is in three different places:

1. The live database on our database server
2. The previous night's backup file on our database server
3. Multiple versions of your data, including the previous night's backup on our Cloud Files account at a different server facility (but still in the Rackspace data center)

Backups on Your Own Rackspace Account

Backups for all churches are stored in a separate location from the database server. However, if you are interested, we can write your database backups to your own Rackspace Cloud Files account. This allows you to download the previous night's backup of your data to your own computers on a daily basis. You can even schedule your backups to download automatically each day.

Choosing this option provides you two key advantages:

1. You can be confident that your data can be restored even in the event of a disaster at our data center.
2. You can write your own custom reports to analyze your own database. Obviously, this would require your own report writing tools and expertise to do this.

This does require some work and set up on your part, but it is a relatively inexpensive way to achieve an off-site storage plan for your data.

Making Cloud Security a Top Priority

In today's modern world, data security is critical. We want your church to be aware of this—and we want you to know we are taking measures to ensure protections are in place when you use TouchPoint.

To quickly recap some of the key ways we work to keep your data safe in the cloud:

- Storing your data on our servers in a world-class data center
- Putting precautions in place to prevent downtime and data loss
- Incorporating additional layers of protection to keep your information secure
- Backing up your data on a regular basis to a separate infrastructure

At TouchPoint, along with providing you the best church management and mobile engagement tools, we want you to feel confident your data is being managed in most effective way possible.

When it comes to cloud security, we know today's churches have questions. We want to provide you the answers.

If at any time you have questions about TouchPoint and how we work to keep your data safe in the cloud, please contact us directly. We'd love to talk with you.

TouchPoint
People Focused. Ministry Maximized.

15660 North Dallas Parkway, Ste 1000
Dallas, TX 75248
touchpointsoftware.com

CONTACT US