



ServiceAutopilot™

DATA SECURITY

FACT SHEET

Data Security

How We Ensure Service Autopilot Doesn't Go Down, Your Data is Backed Up, and Your Credit Card Numbers are 100% Secure

Do you back up your company data daily? Do you take a copy of your data off site to a secure location daily? Do you have redundant data lines? Do you have two of every computer just in case one crashes? Do you have an exact copy of the data on every computer just in case a hard drive fails? Could someone steal your computers and your data from them? Are you certain your router, firewall, and security measures are so tight no one could hack into your office? Is all your data protected to prevent an unhappy employee from stealing or destroying your records?

We can answer YES to all the above.

These are the security concerns we worry about and manage daily. As you read about the level of sophistication behind Service Autopilot's infrastructure, ask yourself if your systems are this safe, secure, and reliable.

1. We use the highest--level SSL (Secure Socket Layer) Encryption method available to transfer your personal information across the Internet from your computer to our secure servers. This *prevents* hackers from intercepting and deciphering your personal data.
2. We utilize Thawte (owned by VeriSign) and GoDaddy for SSL data encryption. Both are two of the most recognized and trusted names in data transfer encryption.
3. Once your personal information reaches our servers, identifying information is encrypted and stored securely. Not only is your private information encrypted while being transmitted, but it's also stored in our secure system in an encrypted format. Our team is unable to access your data unless you provide access.
4. Your data is stored and backed up in multiple secure facilities (VA, TX, and CO).
5. A back up of your data is captured every hour. In addition, 100% of your data is replicated in real-time to a redundant system.
6. Our computer systems are in our physically secure and protected data centers, which make theft near impossible.
7. We store your personal information on servers located within the United States.
8. Every web server, database server, firewall, load balancer, storage device, and more has an exact replica waiting to take over if it crashes.
9. The data centers we use are accredited to PCI DSS, ISO27001, and ISAE 3402 Type II standards and maintain an average uptime of 99.9%.
10. Though we manage your data, we have no rights to it and no ownership of it. Your data is your data. We will *not* sell or trade your personal information with anyone.
11. All credit card transactions are processed using secure encryption—the same level of encryption used by banks. Credit Card information is transmitted, stored, and processed securely on a PCI-Compliant network.

We use Tokenization to securely store credit card numbers. The use of Tokenization mitigates your risk, as your client's credit card numbers are stored with your merchant instead of within your database. For example, if your system were to be hacked, the hacker could not access your client's credit card number. All he would capture is a token (a string of numbers). The token is worthless to the hacker.

If you have any questions, please contact us at Support@ServiceAutopilot.com