425 Metro Place North #400
Dublin, OH 43017
tel: 614.451.5010 fax: 614.451.5009
www.AssociationSoftware.com

WebSuite2 System Security Information

At TCS Software, data security and data backups are our top priorities.

Our web servers are hosted at Amazon Web Services (AWS) (aws.amazon.com/what-is-aws/), a leading Internet hosting company that provides robust physical and electronic security, as well as continuous (24/7/365) system monitoring.

Our resources on AWS are protected through several layers of security. Our only public-facing resources are those which are required to be public to receive and process incoming traffic, such as the Internet Gateway and Application Load Balancer. All other resources, such as the application servers and databases, are made private with highly restricted access.

Private resources require an approved IP address, an approved account protected by multi-factor authentication (MFA), as well as encrypted keys and secret access points for certain services such as the databases. Accounts and services are granted the least privilege necessary to perform their required actions, and all other actions are not enabled.

Information traveling to and from our application passes through multiple firewalls and services that are managed both by AWS experts as well as TCS Software. These services and firewalls block a range of cyber attacks and provide several ways of blocking invalid requests and IP addresses. AWS provides extensive metrics, logging, and expert analysis for us to closely monitor all traffic to the application and the performance of our firewalls.

To ensure consistent application and database availability, we have implemented redundancy by running multiple instances of our resources across different AWS availability zones. If an availability zone becomes unavailable, our application, database, and other resources will experience minimal or no downtime because they are already available in another zone. Our resources are configured to detect such shifts and switch to available database and application instances to maintain availability.

We also have redundancy of database backups which are automatically taken once per day, encrypted, and stored with all of the protections of a private resource explained above. The integrity of these backups are tested at least twice a month to ensure the backups are consistent and reliable. Backups are also regularly downloaded in the TCS Software corporate office, compressed and encrypted, requiring two passwords to decrypt and unzip the contents. Only TCS staff has access to the database backups and the passwords needed to unlock these files. As stated above, the databases on AWS are private, each encrypted with a different key, and require an approved IP address, an approved account protected by multi-factor authentication, encrypted access keys, and a secret access point.

Along with redundancy, we have also configured automatic scaling and restarting of resources. The application instances are configured to automatically come back online if they go down and to scale up in size if necessary to keep the application running. Our redundancy and scaling configurations have been tested and implemented by AWS experts in collaboration with the staff at TCS Software.

The WebSuite2 system has also been built with these security features:

- Sensitive credit card data is never input into, processed or stored by the system. We transfer end-users to your choice of two external PCI-DSS compliant payment processing systems. We send contact details (name/address/phone) to those systems, so your members don't have to reenter the information. Those systems then report back to WebSuite2 with transaction IDs and approval/denial responses – but not account numbers or other sensitive financial data.

- ACH transaction details are received via SSL-encrypted requests to our servers. ACH information is encrypted prior to storage into the WebSuite2 database. Information is encrypted and decrypted using the SHA1 cipher with a proprietary salt key.

- System passwords are one-way encrypted before they are stored in the database. That means they can never be decrypted or read by anyone. (When logging in, the system prompts end users to enter a password. That password is then encrypted. If it matches the encrypted version stored in the database, it is accepted.)

- Every feature of the system is assigned a specific permission level based upon end user roles (administrators, staff, members and public). Thus users with system access must also have the permission to complete certain tasks.

- Access to content on your website may be restricted to members-only groups. You may further restrict access of certain content to other sub-groups, such as a board only section, as needed.

- All website communication utilizes the https/SSL protocol on our domain of associationdatabase.com. If your organization utilizes custom vanity URL(s) you are required to purchase (and periodically renew) an SSL certificate registered to your domain name. With that certificate we are able to route all requests that reference your domain name through https/SSL.

People at your organization with staff or administrative privileges in WebSuite2 should be reminded to choose passwords that are not easily guessed - and those passwords should be updated regularly to prevent unauthorized direct access to your data. Future updates to the software may tighten password requirements and incorporate additional security measures.

Sensitive financial or personal information should not be stored within a Contact record. Nonetheless, from time-to-time our clients need the ability to store certain privileged or proprietary information. WebSuite2 now offers encrypted user-defined Contact attribute fields. Access to these encrypted attributes may be restricted to specific individuals within your organization (i.e. staff members who have access to the Contacts module internally). Please contact us if you'd like assistance with utilizing this feature.

If you have any questions about security please contact Tim Rorris at tim@TCSsoftware.com or call our office at (614) 451-5010.

Updated 08/14/2024.