Church360° is a cloud-based application software suite from Concordia Technology Solutions (CTS) that is used by churches of all sizes to manage their membership data, website, and financial information. This software suite includes Church360° Members, Church360° Unite, and Church360° Ledger.

Security Summary

- Church360° can be accessed on any device that has access to the internet, but it is secured with separate usernames and passwords that are unique to each user.
- CTS performs nightly backups of the Church360° production databases and retains these backups for one month.
- The physical servers that house Church360° are provided by third-party hosting companies who apply the best practices in online security to protect our customers' data.
- These third-party servers sit behind the state-of-the-art firewall protection that is used in both the banking and ecommerce industries.
- Church360° always runs on the most up-to-date versions of Ruby on Rails®, which keeps the application secure when vulnerabilities are discovered in other applications.
- CTS utilizes a third-party service to audit the Church360° code for security vulnerabilities.
- To protect the integrity of the system, CTS does not provide complete server architecture or security procedures as this information may be used to compromise the integrity of the system.

For more information, contact Concordia Technology Solutions
softwaresales@cts.cph.org • 1.800.325.2399

Data Centers

Church360° databases are operated by Heroku, a company that specializes in deploying and operating applications. Heroku's physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. AWS's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

Penetration Testing and Vulnerability Assessments

Third party security testing of the Heroku application is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.

Physical Security

Heroku utilizes ISO 27001 and FISMA certified data centers managed by AWS. These data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by AWS employees is logged and audited routinely.

Environmental Safeguards

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

Management

Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Network Security

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.
Host-based firewalls restrict customer applications from establishing local host connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

DDoS Mitigation

The infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. Heroku works closely with their providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not

addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

System Security

System Configuration

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

System Authentication

Operating system access is limited to Heroku staff and requires username and key authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

Vulnerability Management

The vulnerability management process is designed to remediate risks without customer interaction or impact. Heroku is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third party mailing lists and services. Each vulnerability is reviewed to determine if it is applicable to Heroku's environment, ranked based on risk, and assigned to the appropriate team for resolution.
New systems are deployed with the latest updates, security fixes, and Heroku configurations and existing systems are decommissioned as customers are migrated to the new instances. This process allows Heroku to keep the environment up-to-date. Since Church360° runs in an isolated environment, it is unaffected by these core system updates.
To further mitigate risk, each component type is assigned to a unique network security group. These security groups are designed to only allow access to the ports and protocols required for the specific component type.

Data Security

Church360° database is stored in a separate access-controlled database. This database requires a unique username and password that is only valid for that specific database and is unique to the Church360° application. This connection to postgres databases requires SSL encryption to ensure a high level of security and privacy.

Backups

CTS performs nightly backups of the Church360° production databases. These backup are

retained for a time period of one month. In the event of data being lost due to user error or problems with the code, these backups are used to restore the database to the state it was in at the time of the backup.

Disaster Recovery

Continuous Protection is employed by the third-party platform to keep Church360° data safe in the case of a natural disaster. Every change to the data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state.

Platform

Our third-party platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. This platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. Our third-party provider reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

Access to Customer Data

All customer data is access controlled. The CTS staff does not access or interact with customer data or applications as part of normal operations. There may be cases where CTS is requested to interact with customer data or applications at the request of the customer for support purposes.

Employee Screening and Policies

As a condition of employment all CTS employees undergo pre-employment background checks and agree to company policies including security and acceptable use policies.