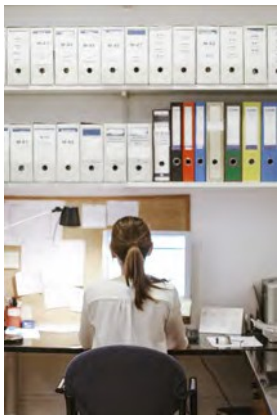

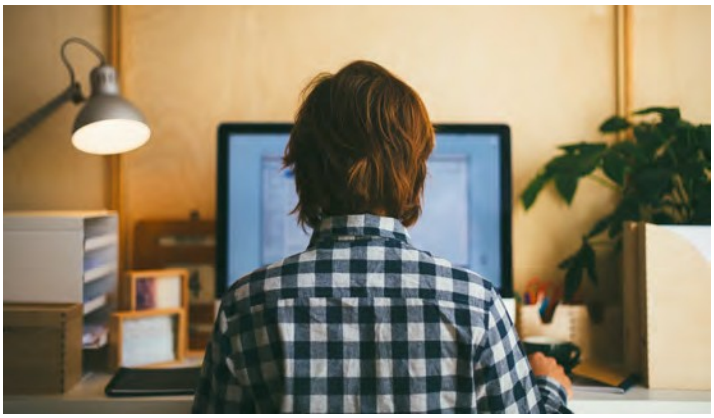

yourmembership.com

Technology + Security Overview

Company Information

Date: 09/16/2014

Our Technology

One of the first questions we often get is, "How can you make your software so affordable?" It's all in the technology – and a great in-house team of systems engineers, software developers, product support specialists and designers who strive to provide the most robust membership management software with the best customer service in the industry.

Data Center Presence

YourMembership.com's primary data center presence is at DataSite Orlando. DataSite is Tier III designed and SSAE 16 Type II Certified, providing the most robust IT infrastructure facility available. We also have multiple secondary datacenter locations as backups in the event of a disaster at the primary.

- 130,000 Square Foot Purpose-Built Data Center Fortress
- Diverse High Voltage Substations on Separate Power Grids
- 3 Jet Turbine Generators
- 8.4 Megawatt Generator Plant
- Dual Concrete Encased Fiber Duct Banks
- Multiple Diverse UPS & Battery Rooms
- 2,750 Ton Centrifugal Chiller Plant
- 3N Redundant Water Supply
- 40,000 Gallons of Reserve Fuel Stored Underground
- Three Above Ground 440 Gallon Day Tanks
- 7/24/365 On-Site Security Guards
- Vehicle Blockades, Bulletproof Walls, Biometric + Keycard Access
- Extensive Video Surveillance Systems
- Redundant Fiber Providers Running BGP
- Cisco Routing, Firewalls and Intrusion Detection Systems
- 7x24 Service-aware Application Monitoring

Application Architecture + Redundancies

YourMembership.com's applications are not only hosted within a hardened facility with many redundancies, but also the network itself is supported by system redundancies of its own.

Multiple fiber providers connect the application to the Internet. These routes are monitored 24x7x365 by systems that alert YourMembership.com engineers should an aberration be detected.

Cisco routing and firewalling optimizes and defends the network against malicious requests and alerts engineers of anomalies.

Web application firewalls also inspect requests for anomalies and look for attempted attack vectors to protect the web application from malicious activity.

To provide maximum uptime and ensure our platform is as scalable as possible, the YM systems engineering team has designed the infrastructure to be almost entirely virtual. This means we can perform maintenance, respond to hardware failures, scale our hardware up and out, and dynamically allocate resources all without affecting customers. This also allows the engineering teams to perform point in time snapshots of the servers before changes are made so we can quickly roll those changes back if there are any problems.

The physical servers have redundant disk subsystems, networking and power. The servers run in clusters to handle spikes in usage and provide fault tolerance should an individual node encounter a localized complete system failure.

Clusters of web servers are load balanced so HTTP/S requests are processed using the most optimal nodes at any given time.

Database servers operate as highly-available "AlwaysOn HADRON" clusters which not only allow for the distribution of read-only traffic to secondary replicas but also allow any other replica to step in as a primary replica should a physical node encounter a localized system failure.

DNS is hosted in our data center as well as in the cloud. Our systems hosted by cloud providers use anycast addressing which routes DNS requests to the closest geographic location.

System Security

Member data is secure and inaccessible to non-members. All members must maintain a username and password for community access. Initial member registration approval can occur one of two ways. First, members can register and be manually approved via an administrative approval process. Second, non-member importation can include private member known data that will be required as part of the registration and auto-approval process.

Administrative backend accounts require a username and password and can only be managed by an administrator with account creation rights. Administrator passwords are expired and must be changed at regular intervals. Administrators with the right to create accounts may create as many accounts as needed, each with different administrative accessibility (i.e. member profile management, donation management, store order management, mass emailing capability, etc.).

Passwords are not stored as clear text in the database. New and changed passwords are “hashed” using the industry-standard 160-bit SHA1 (or 128-bit MD5 upon customer request) encryption algorithm. Only hashed versions of passwords are stored. They cannot be decrypted, thus anyone who would compromise them must resort to an attempt of "brute force".

Agile Development

YourMembership.com follows best practices for agile software development, making us an efficient (and secure) environment. The emphasis is on collaborative communication and dedication to producing high-quality code while retaining the flexibility to adapt.

- Our software is built upon Microsoft technologies including the Microsoft ASP.Net Framework and Microsoft SQL Server
- Our software is architected and maintained in-house by our cross-functional development team employing agile principals and the Scrum methodology
- Each developer works in a dedicated environment with their own copy of application and database source code
- Application and database source code is version controlled by Microsoft Team Foundation Server (TFS)
- Prior to release, developer updates are first delivered to a shared testing environment which is isolated from the production environment
- Release code must pass developer unit tests, automated test plans and manual testing by
- QA Engineers before being deployed into the production environment