



# ePledge Security Overview

*by ePledge provider: Upic Solutions*

Security is our top priority. We have the latest, state of the art security systems to prevent your data from being compromised. We continually invest in developing our world class security infrastructure because we value providing exceptional security and privacy for our customer's data.

The purpose of the security overview document is to provide detailed information on key aspects of ePledge security to help respond to client inquiries regarding the overall security of the application.

## **Encryption Technologies**

Access to the ePledge application is provided over the standard Transport Layer Security (TLS) Protocol. In addition, all email communications will also use the TLS protocol to encrypt communications if the customer system also supports the protocol. [SSL/TLS, SHA2 with 256 bit encryption (High Assurance); RSA with 2048 bit exchange]

## **Server Security**

Our production servers are located in Cincinnati, Ohio hosted by CyrusOne, in a SSAE 16 Tier 3 data center. The data center provides 24x7x365 physical security, video surveillance cameras, and fully redundant systems that span all aspects of hosting (internet connectivity, air conditioning, power, fire prevention systems, etc.) Our hosted environment is designed to keep our servers running without interruption in the most secure environment possible today.

## **Network Monitoring**

We employ a layered network security system that incorporates multiple security vendors and analysis techniques to thwart and detect unauthorized system access. Our multi-stage network monitor system utilizes multiple vendors and monitoring algorithms to ensure system events are detected even in the event of a single monitoring system failure. The following are some of the tests and monitors we administer:

- Daily network vulnerability scan (Independent Security Vendor 1)
- Daily PCI network vulnerability scan (Independent Security Vendor 2, PCI-ASV)
- Quarterly internal vulnerability scan
- Annual penetration testing (Independent Security Vendor 3, PCI-ASV)
- Annual internal vulnerability scan (Independent Security Vendor 3, PCI-ASV)
- Weekly internal patch scanning for security updates
- Real-time performance and up-time monitoring

## **User Authentication Policies**

Upic offers several options for user authentication, we will work with you to determine which policies and procedures are best suited for your security profile.