

Security Statement

Expensewatch.com is safe and secure

At ExpenseWatch.com, we ensure that our data is never compromised. We know that security is crucial to you. That's why we devote significant resources to continually develop our security infrastructure. The result: unsurpassed security and privacy for our customers' information.

With ExpenseWatch.com, you enjoy protection and peace of mind. Among other security measures we offer.

- Experienced, professional engineers and security specialists dedicated to around-the-clock data and systems protection
- Ongoing evaluation of emerging security developments and threats
- Complete redundancy throughout the entire ExpenseWatch.com online infrastructure
- Total commitment to a secure, scalable, private, collocated system (online hosted system arrangement, ExpenseWatch.com manages all aspects of its operations)

Security Details

The ExpenseWatch.com security infrastructure includes proven, up-to-date firewall protection, intrusion detection systems, SSL encryptions, and other security technologies.

Application Security

Our robust application security model prevents one ExpenseWatch.com customer from accessing another's data. This security model is reapplied with every request and enforced for the entire duration of a user session.

Data Encryption

ExpenseWatch.com leverages the strongest encryption products to protect customer data and communications, including 128-bit VeriSign SSL Certification and 1024-bit RSA public keys. The lock icon in the browser indicates that data is fully shielded from access while in transit.

Internal Systems Security

Inside of the perimeter firewalls, the systems are safeguarded by network address translation, port redirection, IP masquerading, non-routable IP addressing schemes, and more. The specific details of these features are proprietary.

Physical Security

Our production equipment is collocated in Philadelphia, Penn., and Scottsdale, Ariz., facilities that provide 24 hour physical security, palm print and picture identification systems, redundant electrical generators, redundant data center air conditioners, and other backup equipment designed to keep servers continually up and running.

Operating System Security

ExpenseWatch.com enforces tight operating system level security by using a minimal number of access points to all production servers. We protect all operating system accounts with strong passwords, and production servers do not share a master password database. All operating systems are maintained at each vendor's recommended patch levels for security and are handled by disabling and/or removing any unnecessary users, protocol, and processes.

Database Security

Whenever possible, database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a number of points, and production databases do not share a master password database.

Perimeter Defense

The network perimeter is protected by multiple firewalls and monitored by intrusion detection systems, all sourced from industry-leading security vendors. In addition, ExpenseWatch.com monitors and analyzes firewall logs to proactively identify security threats.

User Authentication

Users access ExpenseWatch.com only with a valid username and password combination, which is encrypted via SSL while in transmission. An encrypted session ID cookie is used to uniquely identify each user. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Server Management Security

All data entered into the ExpenseWatch.com application by a customer is owned by that customer. ExpenseWatch.com employees do not have direct access to the ExpenseWatch.com production equipment, except where necessary for system management, maintenance, monitoring, and backup. ExpenseWatch.com does not use any managed service providers. The ExpenseWatch.com systems engineering team provides all system management, maintenance, monitoring, and backup.

Reliability and Backup

All networking components, Web servers, and application servers are configured in a redundant configuration. All customer data is stored on a primary database server that is clustered with a backup database server for redundancy. All customer data is stored on disk storage that is mirrored across different storage cabinets and controllers. All customer data, up to the last committed transaction, is automatically backed up on a nightly basis.

About ExpenseWatch.com

If you run a business, you have expenses. ExpenseWatch.com empowers you to control them. Expense Reports, Purchasing and AP Invoice Management modules can be subscribed to individually or as part of a fully-integrated operation expense control suite. Annual subscriptions include implementation, training and support. ExpenseWatch.com: Expense automation, visibility and control.

Contact Us

ExpenseWatch.com

1100 East Hector Street Suite 223
Conshohocken, PA 19428

T 866-399-2824

F 610-397-0539

Updated 2/2009