

Security

November 2009

At ContractExpress.com we take security seriously. We are 100% dedicated to making the system safe and ensuring that your documents, data and personal information remains secure. This document provides an overview of the security procedures and protocols we have in place.

ContractExpress.com is a Software as a Service based document assembly solution optimized for the creation of legal contracts. The ContractExpress.com solution enables individuals, corporate legal departments, law firms and other professional services organizations to streamline document and contract creation, ensure compliance, improve the quality of deliverables, ensure use of up to date content and increase employee productivity.

Data Center - Rackspace®

Physical Security

- Data center access limited to data center technicians
- Biometric scanning for controlled data center access
- Security camera monitoring at all data center locations
- 24x7 onsite staff provides additional protection against unauthorized entry
- Unmarked facilities to help maintain low profile
- Physical security audited by an independent firm

System Security

- System installation using hardened, patched OS
- Dedicated Cisco ASA firewall and VPN services to help block unauthorized system access
- Data protection with managed backup solution

Operational Security

- ISO17799-based policies and procedures, regularly reviewed as part of our SAS70 Type II audit process
- All employees trained on documented information security and privacy procedures
- Access to confidential information restricted to authorized personnel only, according to documented processes
- Systems access logged and tracked for auditing purposes
- Secure document-destruction policies for all sensitive information
- Fully documented change-management procedures
- Independently audited disaster recovery and business continuity plans in place for Rackspace headquarters and support services

Application - ContractExpress®

Application Security

- Implementation of the WS-Federation security protocol using SAML 1.1 tokens
- Message based encryption for all data and transport encryption for authentication
- All web traffic between browser and server is encrypted using SSL 128 bit
- Port hardening – inbound traffic only on port 443 to web site and port 80 to WCF web services
- SQL injection safe
- Regular 3rd party penetration testing
- Session timeout
- Password complexity enforced: must be at least 8 characters, must contain one integer and one CAPS
- Implementation of a user lockout after 5 failed attempts in 2 hour period
- Logout to close and invalidate the session. No data is held on the client
- Access Control Lists on each object such as template and document
- To prevent the hijacking of sessions, the application uses non-predictable session IDs and SSL encryption
- HTML source does not reveal important information about the code behind or architecture of the application
- Error messages are controlled and provide minimal information if displayed
- Optional dedicated data storage is available for additional piece of mind