Contract Guardian Security

"*Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The goals of information security include protecting the confidentiality, integrity and availability of information*". Contract Guardian Support Team.

Contract Management Security Efforts

Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement that we take very seriously. Below is a discussion of what we consider some of the most aggressive contract security efforts in the contract management industry to protect your data both in the Cloud and On Premise.

Contract Management Security Activities

Key Features

- E-Verify of all new employees
- BAA – Offer to sign comprehensive Business Associate Agreement
- Multilevel application security
- Redundant Backup (See Data Center)
- Own Your Data - It is your data and can access/download at your discretion
- Physical Security Systems
  - Biometric
  - Card and PIN Access
  - Combination Lock Access for Cabinets
  - 24/7/365 Video Surveillance
- Environment Controls (HVAC, Generators, Fire Retardation)
- Antivirus - operates bi-directionally and will detect and quarantine viruses
- Web Filtering
- Intrusion Prevention
- SSAE 16 (SAS 70) - Compliant Facilities for Increased Security
- 99.95% Uptime Guarantee
- Contract Vaulting - In addition to normal backups, all of the contracts are vaulted at a secondary data center(s). Contract Guardian uses the services of UCG Technologies. UCG Technologies backs up an entire organization's business-critical data to their secure data center(s). Safe and Off-site, the Encrypted Data is Available online at all times for Immediate, user-initiated Recovery.
- Frequent vulnerability scanning : OS command injection, SQL injection, ASP.NET tracing enabled, File path traversal, XML external injection, LDAP injection, XPath injection, XML injection, ASP.NET debugging enabled, HTTP PUT enabled, Cross-site scripting (stored), HTTP header injection, Cross-site scripting (reflected), Flash cross-domain policy, Silverlight cross-domain policy, HTML5 cross-origin resource sharing, Cleartext submission of password, Referer-dependent response, User agent-dependent response, Password returned in later response, Password field submitted using GET method, Password returned in URL query string, SQL statement in request parameter, Cross-domain POST, ASP.NET ViewState without MAC enabled, Open redirection, SSL cookie without secure flag set, Cookie scoped to parent domain, Cross-domain Referer leakage, Cross-domain script include, Cookie without HttpOnly flag set, Session token in URL, Password field with autocomplete enabled, Password value set in cookie, File upload functionality, Frameable response (potential Clickjacking), Browser cross-site scripting filter disabled, TRACE method enabled, Database connection string disclosed, Source code disclosure, Directory listing, Email addresses disclosed, Private IP addresses disclosed, Social security numbers disclosed, Credit card numbers disclosed, Robots.txt file, Cacheable HTTPS response, Multiple content types specified, HTML does not specify charset, HTML uses unrecognized charset, Content type incorrectly stated, Content type is not specified, SSL certificate

Role-Based Access and Security

Ensure security and flexibility through robust role-based access controls.

Unlimited Roles

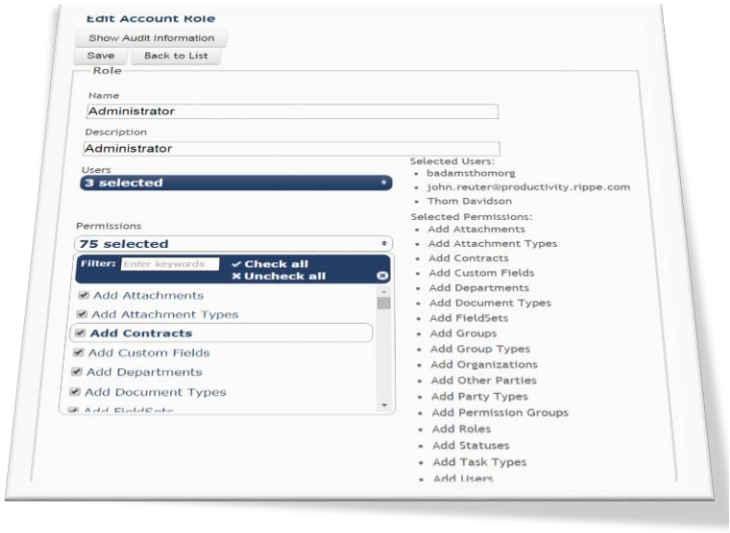
Contract Guardian allows the creation of ***unlimited contract management roles, departments, groups and even organizations.***

A role can be given a series of permissions like add contract, change contract, etc. A group can have one or more roles. A user can be a member of one or more groups. Therefore, a user gains the permissions based on the groups that they are a member.

Roles can be created and managed by grouping together access privileges and administrative capabilities that meet the access needs of users in a group. Often, roles are based on job responsibilities. When a contract manager, for example, signs on as a new user, the person is assigned the appropriate role that automatically allows access to all of the designation services needed to perform the job. It is an easy, efficient way to set access privileges for users. It also provides an efficient mechanism for altering access privileges for common groups of users in the future.

The following are suggestions for your contract management role permissions and names. The contract role descriptions shown below are just examples. You can create an infinite number or roles and associated permission to match your organizations needs and naming conventions.

- Administrator
- Contract Manager
- Contract Author
- Contract Reader



User Access Audit Reporting

A complete detailing of permissions and access is available directly from the User Profile. In addition, one can perform filters from the Contracts Grid queries and generate Reports to identify the specific documents (contracts).

User System Requirements – Modern Browser and Internet Access (*Chrome is our preference*).