



SpringCM's FEATURES

SpringCM develops enterprise-class content management software delivered as an on-demand service with fully integrated capture, document management, workflow and business process automation technologies.

With on-demand delivery, SpringCM can have you up-and-running in less than a day. For businesses of all sizes, SpringCM helps accelerate revenue, decrease costs and avoid penalties by automating document-centric processes.

INDUSTRY LEADERS USING SpringCM



MORE INFORMATION

www.springcm.com

Toll Free 877.362.7273

sales@springcm.com

SpringCM Security: Protecting Your Valuable Content

SpringCM provides a secure, hosted environment for your content. All aspects of our on-demand document management and workflow solution encompass six key areas of security:

Core Application

- VeriSign encryption and Secure Sockets Layer (SSL)
- Folder- and document-level access restrictions for specific users or groups
- Yearly third-party application security assessments
- Secure software development lifecycle through the use of threat modeling and risk assessment

Infrastructure

- Statement of Auditing Standards (SAS) 70 Type II Certified Tier 1-hosted data center model
- Full infrastructure redundancy — hardware “backups” — at all levels of the architecture
- Load-balanced Internet server farm
- Use of hardened operating systems that adhere to the Center for Internet Security's standards

Data Protection

- Enterprise Storage Area Network (SAN) equipment with xPB capacity
- Redundant SAN processor and switch connectivity
- RAID architecture optimized for performance, reliability and availability
- Hardware encryption and compliancy-based storage options

Disaster Recovery

- 24/7/365 online data center redundancy currently in implementation stages
- Offsite data center equipment located in a “standby” facility
- Eight- to 16-hour data recovery service level agreement
- Daily tape backups stored offsite are available for one calendar year

Security Controls

- Adhere to International Organization for Standardization 27002 guidelines
- National Institute of Standards and Technology (NIST) 800-53 controls relating to security
- Control Objectives for Information and Related Technology (CoBiT) and IT Infrastructure Library (ITIL) standards-driven security design
- Managed by Certified Information Systems Security Professionals

Security Management

- IT Service Management V3 security process
- Quarterly and annual audits
- Recurring automated source code analysis
- Audit trails throughout the application/infrastructure