



SpringCM® Innovation

SECURITY FAQ

THE NEW STANDARD IN ENTERPRISE CONTENT MANAGEMENT

SPRINGCM SECURITY: FREQUENTLY ASKED QUESTIONS

1. HOW IS SPRINGCM OPTIMIZED FOR SECURITY?

Cloud enables SpringCM engineers to build additional security at points within our solution where typical on-premises enterprise content management (ECM) products cannot. The definition of Cloud — purpose-built Web technology — implies modularity. Because auditing and securing small modules is the cornerstone of many security architectures, our Cloud model provides customers with additional security benefits beyond the limits of most traditional applications.

Through the Cloud, the SpringCM solution is more agile and better prepared to respond to new security requirements, customer demands and changes. SpringCM is built upon industry-standard tools, protocols and frameworks — such as Microsoft .NET — that contain a wide variety of pre-existing security enhancements such as Secure Socket Layer (SSL), two-factor authentication and strong access control. We leverage, embrace and extend these existing security technologies to our customers, thereby dramatically increasing the overall security of our solution.

2. WHAT ELSE DOES SPRINGCM DO TO ADDRESS SECURITY CONCERNS?

Security is always a concern when handling confidential and proprietary documents. At SpringCM, we take your data's security very seriously by investing a large amount of resources into a proactive security framework that ensures we always maintain the highest levels of security for your data.

SPRINGCM 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 processes.



SpringCM addresses security concerns using a method known as “defense in depth.” We look at each area of our solution, organization and people to see where security controls can reduce the risk of a potential data breach. To guarantee that we meet industry-standard best practices, SpringCM has a SAS 70 Type II certification that is based upon known frameworks, such as ISO 27007 and Control Objectives for Information and Related Technology (CoBiT), two universal security frameworks.

Our effective data security framework aids SpringCM in building and maintaining specific targeted security controls within our core solution, data centers and internal processes in support of our customers security requirements. Data availability, integrity, and confidentiality are top priorities.

4. HOW IS CUSTOMER INFORMATION CONTROLLED?

We use many controls to protect our customers’ data. Specifically, SpringCM employs an advanced access control framework built into the core solution that enables secure authentication, records logs of user activity and allows administrators to control which users have access to highly sensitive documents.

Once your data resides in our SAS 70-certified data center, SpringCM has a disaster recovery plan that includes redundant and failover servers, routers and switches. Our internal security program contains comprehensive policies and procedures that ensure only those who need access to production systems are granted access and only for a limited period of time. This minimizes the chance of unauthorized individuals gaining access to confidential customer data. SpringCM’s IT staff follows a best practices system-hardening process to strengthen our core systems and network devices from potential attacks.

5. DOES SPRINGCM DISCLOSE THE DETAILS OF THE CONTROLS?

We provide detailed information about our security policies and processes to customers who sign a non-disclosure agreement (NDA).

6. CAN CUSTOMERS ADD ADDITIONAL CONTROLS LIKE ENCRYPTION OR OTHER AUTHENTICATION?

Customers cannot add additional controls to our servers, systems and equipment; however, additional services like encryption are available for a reasonable fee. Adding controls to customers’ networks and systems will further reduce risk. We recommend that all of our customers implement an IT security program to protect their data once it leaves SpringCM.

7. WHAT CONTROLS PROTECT INFORMATION DOWNLOADED FROM SPRINGCM?

We use an industry-standard authentication framework and SSL encryption to ensure that anyone downloading documents from SpringCM is properly authenticated and that the download cannot be intercepted during the transfer.

8. DOES SPRINGCM MIX CUSTOMER INFORMATION ON THE SAME SYSTEMS?

Many Cloud architectures — SpringCM included — follow the multi-tenant data model that uses a common data store with virtual partitions of the data. Enhanced security controls ensure that customers’ data never mixes.

During threat-modeling exercises, we ensure that one customer cannot access a different customer’s data through a variety of detection controls as well as aggressive permission and access control lists installed and configured on our servers located in our secure data center. SpringCM developers follow similar

guidelines when addressing areas of our solution in which customer data is accessed, presented or modified.

9. DOES SPRINGCM PROVIDE THE RESULTS OF SAS 70 OR OTHER AUDITS TO CUSTOMERS?

Yes, any customer who has signed an NDA may request audit results. We currently use a third-party vendor to perform an annual penetration test to check the strength of our solution from an external attack.

10. WILL SPRINGCM ALLOW CUSTOMERS TO CONDUCT AUDITS OF YOUR FACILITIES?

Yes we will, depending upon the customer and type of audit. However, we always limit access to areas that contain confidential customer information.

11. WHAT ARE SPRINGCM'S INTERNAL CONTROL STANDARDS?

The SpringCM security model is governed by our holistic SAS 70 certification. We have adopted ISO 27002 and CoBiT as the two leading standards frameworks. We also use the IT Infrastructure Library (ITIL) to measure our effectiveness in meeting the objectives within each framework.

12. WHAT CONTRACTUAL ACTIONS DOES SPRINGCM PROMISE ITS CUSTOMERS REGARDING THE SECURITY OF THEIR INFORMATION?

We do not publicly disclose information regarding customer contracts.

13. WHAT CONTRACTUAL REMEDIES DOES SPRINGCM OFFER CUSTOMERS IN CASE THEIR INFORMATION IS COMPROMISED?

Even though we dedicate numerous resources to keeping customer data secure, security is performed at a best-effort level. Contractually, we rarely enter into an agreement where SpringCM guarantees confidentiality or integrity of a customer's data; however, customers are welcome to request additional conditions to the SpringCM Security Board for consideration.

14. DOES SPRINGCM OFFER CUSTOMERS LEVELS OF PROTECTION FOR CONFIDENTIALITY OR AVAILABILITY?

Yes, we provide a service level agreement for the availability of customers' data. We invest heavily within our Information Technology Security programs to ensure the confidentiality and integrity of our customers' data, but we do not offer various levels of protection for different customers. All customers receive the highest level of confidentiality and data integrity protection we can offer.

15. WHAT PLANS DO YOU HAVE IN PLACE FOR DISASTER RECOVERY?

SpringCM provides various levels of disaster recovery options throughout our architecture and infrastructure components. Disaster recovery is provided seamlessly to the customer from failover data center facilities to offsite backups.

16. CAN CUSTOMERS VIEW AUDIT RECORDS?

You can review log-in and log-out times and user activity history. These records provide customers with essential data for incident response or investigations when an unauthorized individual accesses a user's account.

17. DOES SPRINGCM OUTSOURCE WORK TO OTHER FIRMS?

We do not outsource critical development and support to outside firms. External vendors perform audits.

18. HOW DOES SPRINGCM TEST ITS SOLUTION?

We perform an annual application assessment against our entire solution suite. We also use third-party security firms to educate our developers, IT staff and executives about upcoming security threats and trends.

All development includes threat modeling and risk assessments for all areas of our solution that interact with customer accounts or data.

19. HOW CAN CUSTOMERS PROTECT THEIR INFORMATION?

We have a white paper that customers can view after signing an NDA. The white paper covers the processes and technologies that can be deployed to help protect information. We can also offer consulting services under a normal statement of work.

20. WHAT HAPPENS WITH MY DATA IF I DECIDE TO LEAVE SPRINGCM?

For customers who require backups of both the original customer documents as well as the metadata associated with those documents., SpringCM can deliver a backup of your data as it is used in SpringCM to your location of choice in a variety of formats such as tape backup, optical storage or disk depending upon size of the data. This service is provided for a reasonable fee. Standard customer agreements are available.

LEADERS RELY ON SPRINGCM

ACS
Alcatel
Apptis
Avon
Base Technologies
Boeing
Cable ONE
CACI
Comcast
Cox Communications
CSC
DSA Inc
HealthNet
ManTech
Oberon
REDC
Rescare
STG
Scientific Research Corp.
Siemens



ABOUT SPRINGCM

SpringCM is the recognized market leader in enterprise-class cloud platforms for managing content and business processes. SpringCM's affordable, rapidly deployable solutions enable organizations of all kinds to address their most critical Enterprise Content Management (ECM) and Business Process Management (BPM) challenges. SpringCM's solutions are trusted by customers such as the Department of Energy, Comcast, and Siemens. SpringCM partners include salesforce.com, Microsoft, and Ricoh.com.

For more information, please email: sales@springcm.com or call 877.362.7273.

www.springcm.com

SpringCM is a trademark of SpringCM Corporation.
All other marks are the property of their respective owners.