RMS® Privacy Policy for Cloud Solutions

November 2016

Table of Contents

Guiding Principles 3

- Client Data 3
- System Data 3
- Physical and Environmental Security 4
- Strong Network Security 4
- Data Encryption 4
- System Hardening 4
- Integrated Business Continuity 5
- Physically Secure Hardened Data Centers 5
- Stringent Change Management and Restricted Access 5
- Comprehensive Monitoring, Logging, and Auditing 5
- ISO 27001: The Global Standard for Security and Data Privacy 6
- Governmental Regulations and Directives 6
- European Union Data Protection Directive (Directive 95/46/EC) 6
- Cross Border Data Flow Segregation 6

Summary 7

Privacy Policy Changes and Updates 7

Guiding Principles

RMS aims to provide the most secure, the most private, and the safest way in the industry to manage your data throughout its life cycle. We recognize that this requires robust security as well as data-protection technologies and protocols to safeguard your data. It also requires that RMS lead the industry and adopt a privacy policy that provides transparency; that gives you the confidence that your data will not be used or accessed by RMS or any third party in ways that might compromise the integrity of the data or the trust you have placed in RMS; and that meets or exceeds the legal requirements of the countries in which you do business.

The RMS Privacy Policy is guided by three simple principles:

1. RMS protects your data using enterprise-class security measures built on a security framework that implements best practices from ISO 27001, CSA STAR and the National Institute of Standards and Technology (NIST) standards.
2. You are in control of the data that you have entrusted to RMS; we will not compromise the trust you have placed in us. RMS has no access to your confidential data without your express consent, other than the exceptions mentioned below. When we do receive your consent, we will use your data only as you have permitted us to do so.
3. Ensuring your privacy as an RMS user is of utmost importance to us. Metadata generated when you use RMS is tightly regulated to ensure that it is only utilized for legitimate purposes, such as for operating and supporting RMS services that enhance your user experience and for security.

Client Data

You own and control any data you upload, transfer, and generate with RMS cloud solutions. We call this data "Client Data." Client Data includes your exposures, contract data, modeling assumptions, and the settings and model results you generate.

RMS implements and maintains strict organizational, procedural, and security controls to ensure we will not access your Client Data unless we receive your express consent. Once consent is granted, we will only use that Client Data for the specific purpose you permitted. The only exceptions to the restrictions on our access to and use of your Client Data, other than exceptions authorized by your express consent, will be if RMS must interdict a virus or malicious code embedded within your Client Data; take emergency measures to address system-wide threats; perform normal database operations as required by the database administrators on the RMS support team to ensure all service-level agreements are met; or comply with the requirements of law, such as a court order.

We may, from time to time, offer services pertaining to your Client Data that you may choose to engage us to perform. However, we will not perform any services involving your Client Data unless you opt-in for those services by signing a written agreement with RMS. Finally, we will never sell, publish, or distribute your Client Data to any third party.

System Data

When a user logs in to a instance of RMS cloud solution, the system captures metadata about how the user accesses and uses the system and stores that metadata in auditable log files. We call this data "System Data." System Data may include date/time stamps, clickstream data, information about what actions were requested by the user, and what user-requested jobs were performed.

RMS uses System Data to maintain the security of our systems, to operate them, and to provide you with support. For example, RMS will use System Data to enhance the user experience; optimize resource planning and system performance; determine usage fees (if applicable); report on utilization; respond to audit requests; determine compliance with performance commitments; monitor and identify any security breaches; and respond to technical support questions.

RMS may share System Data with certain third parties after the data has been aggregated and anonymized; no client will be identifiable when System Data is shared. The aggregated and anonymized System Data may be used by such third parties to enhance the RMS user experience, to better understand how you are using certain features and capabilities of the data or applications running on RMS, and for marketing purposes.

Any RMS business partners who provide third-party models, applications, or data that you may choose to license for use or who provide products or offerings that support the operation and maintenance of our systems will be required to comply with the terms of this Privacy Policy.

Physical and Environmental Security

Maintaining the privacy of your data and your clients' data is paramount to your business operations. RMS understands your data privacy concerns: You must ensure the privacy of your data to uphold the trust of your clients and business partners and you need to comply with legal directives and regulations. RMS addresses these concerns and requirements by integrating multiple layers of security — physical security, electronic security, and operational security — to ensure the privacy and protection of your data. Each layer of security is integral to the RMS infrastructure, cloud provider partner, and its operation.

The RMS commitment to security and data privacy is backed by experienced security personnel under the direction of the Sr. Director, Information Security & Compliance and an executive-level governance council. Security measures are aligned with the RMS Privacy Policy. Our security controls and risk-management framework are based on multiple standards and globally recognized best practices that include an information security management system based on ISO 27001 and a risk-management framework based on the National Institute of Standards and Technology (NIST).

To ensure protection from unauthorized access; to thwart malware and other malicious activity; and to maintain the integrity of and high-availability access to your data, models, analyses, analytics, and applications, RMS implements the following security and data-privacy measures.

Strong Network Security

RMS network security combines advanced and hardened firewalls, intrusion detection and prevention systems, and ongoing log monitoring and analysis for threat prevention. To ensure that RMS network security defends against evolving threats, frequent vulnerability scanning is performed, supplemented by independent, third-party threat, vulnerability, and penetration assessments.

Data Encryption

RMS uses best practices to encrypt all data in transit to and from RMS data centers and its cloud providers. In addition, data transferred between end users and RMS is also encrypted.

System Hardening

To minimize security risks, RMS employs the practice of system hardening and minimization (also referred to as "operating system hardening"). This means that operating systems are reduced to the minimum necessary capabilities: All nonessential software, services, protocols, modules, programs, utilities, accounts, and usernames are removed. Only essential network ports are opened, and they are protected by the network security measures. Antivirus and anti-malware scanning is also used to safeguard the foundational software from unwanted malicious software and security vulnerabilities.

Integrated Business Continuity

Ensuring data integrity and data availability is an integral aspect of how RMS keeps your data secure. Frequent backups and an RMS data center or cloud provider dedicated to maintaining your business continuity and disaster recovery (DR) are among the measures RMS has implemented so that your data is available when you need it.

The RMS infrastructure includes a data center dedicated to business continuity and DR. The data center is geographically separate from the primary production data centers it supports and constantly receives critical data so that any RMS production data center can recover from a failure and resume production operation. Your data may be mirrored to the DR data center using encrypted transfers from any RMS production data center should you choose this option. Should a production data center experience a significant and extended outage, the DR data center is designed to include failover capability as a stand-in that provides business continuity. RMS regularly validates its DR data center and corresponding processes.

The RMS cloud provider has data centers in various locations around the world dedicated to business continuity and DR. These data centers are geographically separate from the primary production data centers they support and constantly receive critical data so that any RMS cloud provider production data center can recover from a failure and resume production operation. Your data may be mirrored to the DR data center using encrypted transfers from our cloud provider should you choose this option. Should a cloud provider data center experience a significant and extended outage, the cloud provider's DR data center is designed to include failover capability as a stand-in that provides business continuity.

Physically Secure Hardened Data Centers

The RMS infrastructure is housed in a cloud provider or multiple, strategically located, geographically separate, Tier III standards compliant data-center buildings that are designed to mitigate risks from natural and human-made disasters. RMS partners with a globally recognized cloud providers that has various locations around the world and has a SSAE16 SOC2 report that provides an opinion on the physical and environmental security of their global data centers.

All data-center buildings are constructed and operated to restrict access only to authorized personnel. Multiple physical security measures restrict entry and access to the RMS infrastructure equipment to specifically authorized people. All RMS infrastructure equipment resides in private, locked cages within each data center. A limited number of authorized personnel with clearance vetted by third-party background checks and stringent security training can physically access RMS equipment.

Only the RMS cloud operations team has the access privileges and authority to perform scheduled maintenance and upgrades. All cloud and RMS data-center access and system administrative activities are logged, monitored, and audited to be consistent with industry best practices.

Stringent Change Management and Restricted Access

High-level security is achieved from the inside out and holistically through a combination of technology and best practice–based policies and processes. RMS follows the change-management processes prescribed by the Information Technology Infrastructure Library (ITIL). RMS also follows the ITIL processes for incident management, release management, and problem resolution.

Comprehensive Monitoring, Logging, and Auditing

RMS manages and monitors security and the integrity of all data stored and processed. With the aid of security information and tools, the security operations team can identify and proactively remedy potential security concerns through frequent review and analysis of RMS activity logs. The security operations team investigates threats and anomalous activity so that any such activity and suspicious access vectors can be blocked.

Dedicated platform, infrastructure and cloud provider support teams also provide monitoring and operational support to ensure your environment runs optimally. Database administrators who are part of these support teams have access to Client Data, but this access is solely to ensure all service-level and operational-level agreements are met for your systems. All access to systems is logged and is always auditable.

When your designated end users log in to RMS, specific information related to that end-user session is captured and logged onto auditable log files. The logged information includes how each end user accessed and used the features, capabilities, and functions of RMS, such as which end user logged in and what actions were requested and performed on their behalf. This information is only used to maintain security and to efficiently and effectively operate and administer RMS systems.

Clients may request logs of their specific activity and environment to review and audit by contacting our information security officer at:

Risk Management Solutions, Inc.

Attn: Senior Director of Information Security and Compliance

ISO 27001: The Global Standard for Security and Data Privacy

The RMS cloud operations team is dedicated to ensuring the ongoing operation and security of the RMS cloud solutions by following information security controls prescribed by the ISO 27001 globally recognized information security management standard and best practices. By adhering to this information security management framework, RMS ensures effective security for confidential and private data by identifying and mitigating information security risks and by adapting RMS information security controls to accommodate evolving best practices. RMS also partners with a top tier cloud partner that is ISO 27001 and 27018 certified and has SSAE16 SOC1, SOC2 & SOC3 reports performed on an annual basis.

Governmental Regulations and Directives

RMS will comply with all applicable governmental regulations.

European Union Data Protection Directive (Directive 95/46/EC)

RMS has taken explicit steps to ensure that you can comply with governmental directives and regulations, including the European Union Data Protection Directive. To allow you to comply with the requirements of this directive, you are in control of your data; RMS will only process your data as you explicitly agree, using specific contract language. Production data center locations have been strategically chosen within the European Economic Area and in Canada to enable you to comply with the European Union Data Protection Directive.

Cross Border Data Flow Segregation

RMS cloud solutions utilize data centers and cloud providers strategically located around the world. Your designated end users can access RMS cloud solutions and the data you store within them from any location, provided that your end users have valid access credentials.

Summary

RMS has a commitment to maintaining your data privacy and integrity that is reinforced by highly experienced personnel following best practices overseen by a compliance director and reviewed by an executive-level governance council. RMS includes a suite of security and data-protection measures to ensure data privacy, data integrity, data availability, and high availability of services. Because RMS has implemented a multi-layered approach, application security, data privacy, and data-security requirements are part of the design, implementation, and quality assurance of our solutions. RMS has taken the necessary steps to put the people, policies, and technologies in place to provide the most secure and reliable platform for the insurance industry to quantify and manage risk.

Privacy Policy Changes and Updates

Internet and Web-based services evolve rapidly. Therefore, RMS reserves the right to update this Privacy Policy at any time. If RMS does change this policy, then a new, superseding version will be posted on rms.com. We advise you to review our posted RMS Privacy Policy from time to time.

Contact Information

If you have any concerns or questions relating to this RMS Privacy Policy, contact us at **support@rms.com.**

Risk Management Solutions, Inc.
7575 Gateway Boulevard.
Newark, CA 94560 USA
http://www.rms.com