TransparentCMS™

Compliance Management System

Description of Hosted Services Security

OVIYA SYSTEMS LLC

231 Market Pl, Ste.373, San Ramon, CA 94583 l www.oviyasystems.com | 1-877-GO-OVIYA

Disclaimer:

Oviya Systems Security Statement

The Oviya Systems, LLC, a California limited liability company ("Oviya Systems") information systems platform offers multiple layers of security to ensure that the integrity of customer data is not compromised. We know that security is crucial. That's why we devote significant resources toward safeguarding and protecting customer data entered into the system.

At the infrastructure level, we ensure that data is secure, safe, recoverable and isolated. At the application level, we have implemented the following multi dimensional data security protocols: business unit level, role level, user level, application function level and screen level.

1. Oviya Systems Application Security

1 Each customer operates under their own independent application instance, which implies a separate application environment with a separate database. This aids in preventing any accidental security compromise.

2 Any documents uploaded will stay under their respective application instance, hence providing document isolation from other instances.

3 Each document uploaded is scanned for viruses using industry-standard virus-checking software.

4 There is a file size limit for uploading documents.

5 Oviya Systems' TransparentCMS provides the following security levels within the application.

- **Business group level**

  Each client can have more than one business group configured in their account. Data pertaining to one business group will not be available or visible to another business group, unless the client actively provides for such access.

- **Role Level**

  The application provides security at the role level. Each role has separate permissions for their activity as well for the data that is viewed and used by users belonging to other roles.

- **Page Level**

  Page level permissions can be given to each role. Users mapped to that role will be able to view only those pages for which they have permissions. Activities like create, delete, modify and view on each page can also be defined.

- **User group Level**

  The application also provides security at the data level. Users can define permissions based on location. Users mapped to a role can only view data belonging to that region/Country.

2. Managed Hosting

Rackspace is the managed hosting provider of choice for Oviya's Systems' SaaS Solutions. Rackspace (www.rackspace.com) is one of the worlds' largest hosting provider. They not only pioneered Managed Hosting services, but also set the standard for Cloud, Managed and Email Hosting with their support, expertise and diverse solutions for customers of all sizes, kinds and needs. Rackspace has a well-earned reputation for their service and 24x7x365 support. The company has the added distinction of guaranteeing 100% uptime of their network.

3. Datacenter Security

Rackspace's data centers are engineered to the standards required to support the Zero-Downtime Network™. They are designed and maintained to be uncompromising on security or redundancy.

They have Global data centers on3 continents:

North America: *San Antonio (TX), Dallas (TX), Ashburn (VA), Herndon (VA)*

Europe: *London, UK (2), Slough, UK*

Asia: *Hong Kong*

Each data center is a single-purpose facility engineered to address security and network redundancy, enabling Rackspace to offer high availability to its customers.

Physical Security

- Data center access limited to Rackspace 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

Precision Environment

- Rackspace data centers feature redundant HVAC (Heating Ventilation Air Conditioning) units, which provide consistent temperature and humidity within the raised floor area. HVAC systems are inspected regularly and air filters are changed periodically.
- Redundant lines of communication to telecommunication providers provide Rackspace customers with failover communication paths in the event of data communications interruption.

- Data centers are equipped with sensors, including smoke detectors, fire suppression systems and floor water detectors, to detect environmental hazards.

Conditioned Power

- Should a total utility power outage ever occur, all of Rackspace's data centers' power systems are designed to run uninterrupted, with every server receiving conditioned UPS (Uninterruptible Power Supply).
- Rackspace's UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails.
- If an extended utility power outage occurs, Rackspace's routinely tested, on-site diesel generators can run indefinitely.

Core Routing Equipment

- Only fully redundant, enterprise-class routing equipment is used in Rackspace data centers.
- All routing equipment is housed in a secured core routing room and fed by its own redundant power supply.
- Fiber carriers can only enter Rackspace's data centers at disparate points to guard against service failure.

Network Technicians

- Rackspace requires that the networking and security teams working in their data centers be certified. Rackspace also requires that they be thoroughly experienced in managing and monitoring enterprise level networks.
- Rackspace's Certified Network Technicians are trained to the highest industry standards.

4. Information Security

Rackspace implements Information Security best practices to protect the confidentiality and integrity of customer and company data systems. A Security Awareness program communicates security expectations to Rackspace workforce during the initial Security training at new employee orientation. Quarterly Security Awareness bulletins also support the Security awareness program. All visitors are required to sign in via a visitor log. Building Operations, Security or Data Center Management review and approve visitor access and issue visitor badges for identification purposes before access is granted to any non-Rackspace employee. For their facilities in London, in lieu of sign off sheets, an email of visitor logs is reviewed by the Data Center Manager and emailed to Rackspace Corporate Security. Controlled building access and secure access to specific areas are ensured through the administration of proximity cards. An Incident Response Process has been instituted to respond to and document security incidents.

5. Operational Security

- ISO17799-based policies and procedures are regularly reviewed, as part of Rackspace's SAS70 Type II audit process
- All employees trained on documented information security and privacy procedures
- Access to confidential information restricted to authorized personnel only in accordance with 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

6. Network Uptime

Rackspace strives to guarantee 100% Network Uptime. Here is their statement on this:

"100% Network Uptime Isn't Wishful Thinking, It's A Guaranteed Reality

We know that every second the network is down we're losing opportunities, revenue and the confidence of the users. That's why we partnered with a hosting provider who has designed and built the Zero-Downtime Network to minimize downtime and we are so confident about its capabilities, based on their track record and customer testimonials.

7. Network Security - Firewall

All Oviya systems' SaaS offerings are protected by a dedicated Cisco Firewall to secure the network from Malicious Activity. A dedicated firewall is an important first step in securing your hosted environment and acts as a protective barrier to keep destructive forces away from the mission-critical data.

In addition to filtering traffic, Oviya Systems' servers have a more secured form of communication with the implementation of a Virtual Private Network (VPN) which encrypts all information between designated hosts and the Hosting Environment. This will be used by Oviya Systems' internal team for managing the software and the server environment.

8. Network Security

Rackspace Managed Hosting provides 24x7x365 staffed security and the monitoring of both internal devices and external threats. Their 100% Cisco Powered Network, built on hardened routers and regularly audited by Cisco, ensures maximum security protection. Their network incorporates patented Rackspace Intrusion Detection Systems.

9. SSL Encryption for Secure Data Transfer

Secure Socket Layer ("SSL") is the protocol for securing data transmissions across the Internet. An integral component of most web browsers, it secures your users' data by using public-and-private key encryption systems. It also authenticates the server's identity, reassuring the application users that they're actually who they claim to be.

Oviya Systems' servers have been deployed with SSL certificates provided by *thawte*. *thawte's* SSL123 certificates are domain validated SSL certificates that are capable of providing 256-bit encryption for securing the application users' data transactions.

10. Data Recovery and Managed Backup

Oviya systems servers' data is preserved and the integrity is maintained by Rackspace's managed backup service. It offers a flexible and reliable unmetered managed backup service during disaster recovery by reducing the risk and restoring the data as quickly and completely as possible. Here are some salient features of the Managed Backup service.

- Unmetered Managed Backup (essentially unlimited backups with a 2 week retention period).
- Full Backups every week and differential backups every day. This makes a full data recovery speedy because the required data only has to be restored from two Backup Sets.
- File and directory backups are included with the standard Managed Backup service and are provided by a File System Backup Agent. Oviya Systems has also purchased the SQL backup agent to capture Oviya Systems' selected Database information.
- Data backups are performed off Oviya Systems' server and onto tape media as opposed to a separate drive.
- Managed Backup technicians are available 24x7 to monitor backup jobs, perform data restores, configuration changes.
- Data restores are initiated immediately upon request.

11. System Monitoring by Rackwatch Platinum Service

Oviya Systems Servers are currently being monitored by Rackspace's Rackwatch Platinum services. Oviya Systems is set up to receive alerts regarding FTP, HTTP, MSSQL Server, Ping and SMTP. If the ping fails on any of these ports, Rackspace's monitoring service will notify the dedicated Rackspace team and they will restart IIS. If the problem persists, Rackspace's experienced technicians will automatically attempt to fix the problem according to their support policy. Oviya Systems will be notified of any issue via the ticketing system.

12. Virus Protection by Rackspace Managed Antivirus

With Cyber Crime posing an unyielding threat to businesses today, an anti-virus solution is one of the most critical, effective and affordable ways to avoid infections from viruses, spyware, adware and potentially unwanted applications. Oviya Systems Servers are protected by Managed Anti-Virus from Rackspace which is an advanced technology that's fully managed by Rackspace which will protect Oviya Systems servers round the clock.

Benefits of the Rackspace Managed Anti-Virus Solution

- Provides proactive, sustained protection against viruses, worms, Trojans, spyware and other malware in one solution
- Uses Behavioral Genotype Protection™
- Provides zero-day protection by proactively identifying programs that will behave maliciously before they execute.
- Behavioral Genotype Protection identifies malicious code on file servers and deletes it before it executes, or
- reaches endpoint computers on your network
- Provides 24x7x365 protection by SophosLabs,
- Sophos's global network threat analysis centers and the smallest update size (typically <5kb) in the industry
- Can be automatically updated as frequently as every five minutes or on demand
- Includes an end-user quarantine manager for deleting or disinfecting infected files
- Provides proactive and continuous protection against viruses, worms, Trojans, spyware, malware and root-kits.
- Proactively identifies programs that behave maliciously before they execute by using Behavioral Genotype Protection tm. Behavioral Genotype Protection identifies malicious code on file servers and stops it before it executes or reaches endpoint computers.
- Updates are performed automatically every 5 minutes or on demand.

13. Rackspace's Commitment to Sustainable Operations

As a company whose product and mission is to primarily manage sustainable operations of companies, Oviya Systems is careful in choosing whom to partner with.

On the managed hosting side, we are glad to find a partner in Rackspace who is committed to sustainability. With eight data centers worldwide producing thousands of tons of CO2 a year, Rackspace knows they make a huge difference to the environment by their sustainable operations. They are dedicated to energy conservation and continue to explore new and alternative ways to conduct their business.

- Rackspace designs all of its data centers with power conservation in mind and leverages energy efficient hardware and equipment.
- Rackspace's UK data center operates on renewable energy.
- Rackspace has always leveraged energy efficient hardware and equipment in the data center.

  In 2005, Rackspace adopted the Dual-Core AMD Opteron Series processors, which consume less electricity than prior processor models.

  Rackspace recently introduced the latest generations of both Intel and AMD low voltage processors, which allow customers to generate power savings when right-sizing their configuration.