

Rackspace Managed Hosting™ Security

Triple-Strength Security Backed by Fanatical Support™

Rackspace Security is a powerful, fully integrated portfolio of services, managed devices and best practices — all designed to ensure the highest levels of security for customer data.

Our portfolio covers all three critical security areas: physical security; operational security; and system security. Physical security includes locking down and logging all physical access to servers at our data center. Operational security involves creating business processes that follow security best practices to limit access to confidential information and maintain tight security over time. System security involves locking down customer systems from the inside, starting with hardened operating systems and up-to-date patching. Rackspace offers a full range of options to take system security to the next level.

As with all Rackspace offerings, Rackspace Security solutions are backed by Fanatical Support™ — our absolute commitment to doing whatever it takes to ensure that all our customers are 100% satisfied, 100% of the time.



Rackspace Security supports all three areas of data security, ensuring maximum protection for customer data.

Rackspace Security at a Glance

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

System Security

- System installation using hardened, patched OS
- System patching configured by Rackspace to provide ongoing protection from exploits
- Dedicated firewall and VPN services to help block unauthorized system access
- Data protection with Rackspace managed backup solutions
- Optional, dedicated intrusion detection devices to provide an additional layer of protection against unauthorized system access
- Distributed Denial of Service (DDoS) mitigation services based on our proprietary Rackspace PreventTier™ system
- Risk assessment and security consultation by Rackspace professional services teams

Operational Security – the Rackspace Infrastructure

- ISO17799-based policies and procedures, regularly reviewed as part of our SAS70 Type II audit process
- All employees trained on documented information security and privacy procedures
- Access to confidential information restricted to authorized personnel only, according to 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 continuity plans in place for Rackspace headquarters and support services

Operational Security – Customer's Application Environment

- Best practices used in the random generation of initial passwords
- All passwords encrypted during transmission and while in storage at Rackspace
- Secure media handling and destruction procedures for all customer data
- Support-ticket history available for review at My.Rackspace.com
- Help available from Rackspace in configuring system logging to create a system audit trail
- Rackspace Security Services can provide guidance in developing security processes for compliance programs

MODIFIED DATE: 11-09-2008

Managed Hosting Backed by **FANATICAL SUPPORT™**

United States: www.rackspace.com | 800.961.2888

Europe: www.rackspace.co.uk | +44 20 8734 2600

