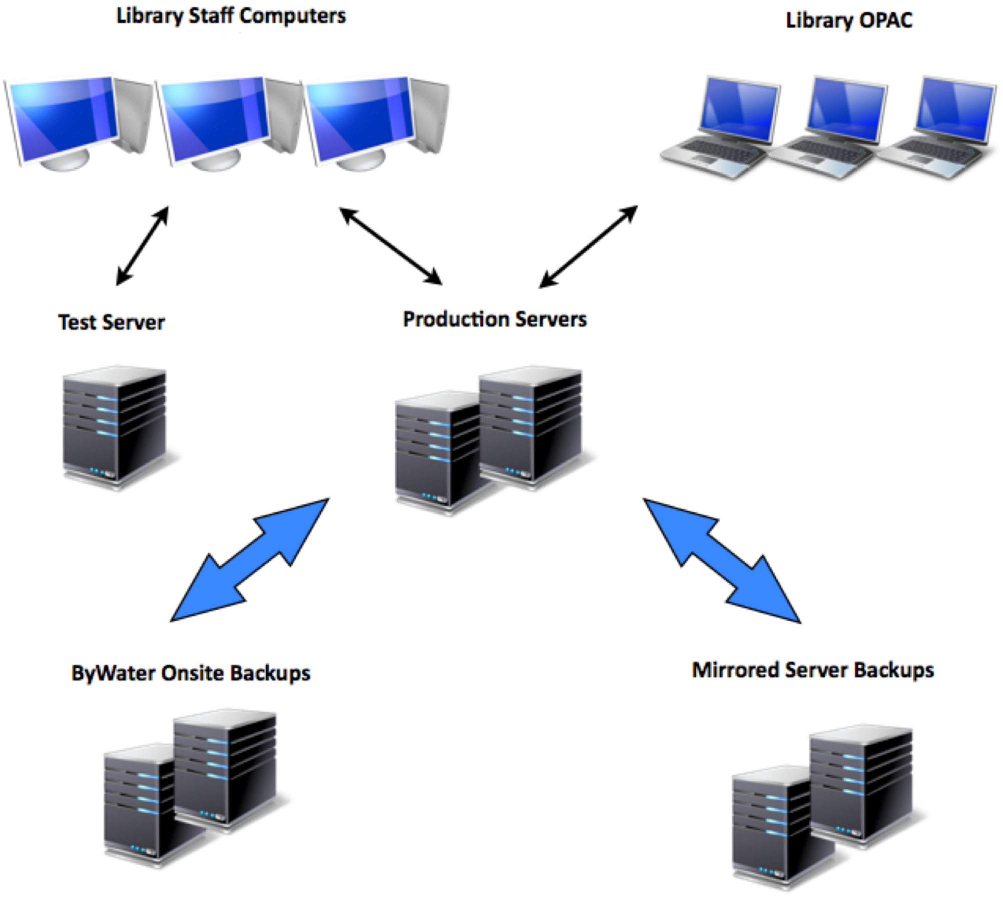
ByWater SOLUTIONS

Server and Backup Plan

ByWater Solutions plans and prepares for the worst by taking the following precautions and installing the following safeguards to protect your data. We perform a daily backup of all Koha data stored on the cloud. This information is saved both on-site and off-site, and is comprised of the all of the system data, and all other configuration information found on the main server.

In addition to the daily backups listed above, we maintain a copy of your code-base on our servers. In the event that the entire cloud server fails, we can have your system replicated on a new server, and up and running within a matter of hours. ByWater Solutions maintains archival backups as follows: daily backups for the last three days, weekly backups for one month, bi-monthly backups for up to one year.



ByWater servers are cloud-based Virtual Machines. Access to the Koha application by library staff and patrons is entirely web-based, so no additional local security devices or controls are required.

Security Overview

ByWater Solutions takes security very seriously on behalf of our partners. The following outlines some additional information about the security measures we employ.

Direct access (i.e. command line) to the Koha server is by SSH (so all traffic to and from the server is encrypted). SSH access is limited to only connections coming from ByWater gateway servers, and is limited to ByWater staff only. All ByWater staff have accounts on the server, and must login as themselves (i.e. no access using a shared account). Remote access by the root account is not allowed. Access to the ByWater gateway servers requires staff to use secure private keys. When passwords need to be generated by the Systems Administrator, they are generally a minimum of 12-14 characters in length, and include letters, numbers and special characters, resulting in a very strong password that is immune to dictionary attacks. Our cloud provider, RackSpace, does NOT have SSH access to our servers, and cannot view MySQL databases or backups.

If desired by the partner, web traffic to either (or both) the catalog and staff clients can be encrypted using SSL (i.e. HTTPS). However, the partner is responsible for procuring the SSL certificates at their expense; ByWater does not re-sell SSL certificates.

ByWater employs iptables firewall rules on every server. Access to all ports is disabled by default, and only those ports needed are opened.

All patron data and transactions are stored in Koha's MySQL database. Unless the partner specifically requests otherwise, the MySQL database server only listens for connections coming from the localhost, so attempts to directly login to MySQL remotely are not possible. When a partner does request ODBC access to their MySQL database (e.g. for reports not provided by Koha), those accounts are read-only and are limited to specific IP addresses. In addition, the Koha Community guidelines for programmers specify that all code must abide by set standards to prevent SQL injection attacks (see http://wiki.koha-community.org/wiki/Coding_Guidelines#SQL10:_Placeholders).

Within the Koha ILS itself, patrons can only view their own data, and only after logging in to the catalog using username/password. (If desired, this functionality can be turned off.) Library staff with the proper credentials can see all patron records in the Staff Interface. Care should be taken in assigning permissions to staff accounts, and in the choice of passwords for those accounts.

The following page contains all of the security features employed by our hosting provider, Rackspace:

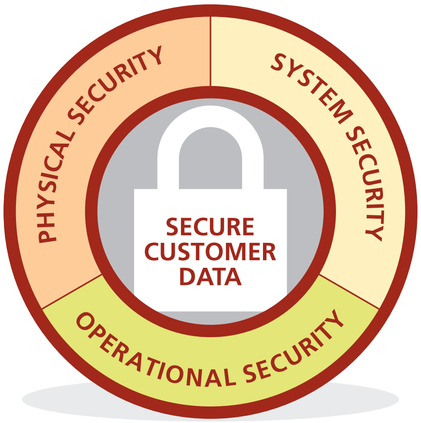
RACKSPACE® SECURITY

Triple-strength Security Backed by Fanatical Support®

Rackspace Hosting 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, our promise of Fanatical Support stands behind our security solutions. We will do whatever it takes to ensure that all our customers are satisfied.



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 PrevenTier™ 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 via the MyRackspace® customer portal
- 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

experience ***fanatical support***®

Toll Free: **1.800.961.2888** | International: **1.210.312.4700** | www.**rackspace**.com

| MODIFIED DATE: **05202009**

RACKSPACE® HOSTING | 9725 DATAPOINT DRIVE | SAN ANTONIO, TX 78229 U.S.A.

rackspace®
HOSTING