OrangeHRM

ORANGEHRM DATA SECURITY

YOUR DATA IS SAFE WITH US!

Keeping your coworkers' information safe and secure is the name of the game. With OrangeHRM you won't need to worry about implementing security measures anymore. We have it all taken care of. Please read our documentation below to see all of the details you need.

CLOUD SERVICE PROVIDER - RACKSPACE

The Rackspace secure multi-cloud and hybrid solutions help us meet changing technology expectations, adopt emerging technologies and respond to tightening compliance and security mandates. Their solutions provide compliant IT as a Service, on the latest technologies, across applications, data, security, and infrastructure tailored to our needs.

Rackspace delivers unparalleled support helping us solve operational challenges faster and smarter. Rackspace guarantees;

- 100% Network Uptime Guarantee
- Unrivaled portfolio across apps, data, security, and infrastructure
- Industry-leading SLAs and customer satisfaction scores
- 24x7x365 support from certified experts
- Independent security audits and certifications (e.g., ISO, SOC, PCI, FISMA)

Visit **www.rackspace.com/** for more information.

RACKSPACE SECURITY CONTROLS

PHYSICAL SECURITY

- Datacenter access is limited to only authorized personnel.
- Badges and biometric scanning for controlled data center access.
- Security camera monitoring at all data center locations.
- Access and video surveillance log retention.
- 24x7x365 onsite staff provides additional protection against unauthorized entry.
- Unmarked facilities to help maintain a low profile.
- Physical security audited by independent firms annually.

NETWORK INFRASTUCTURE

- High-performance bandwidth provided by multiple network providers.
- Elimination of single points of failure throughout the shared network infrastructure.
- Cables properly trunked and secured.
- Proactive network management methodology monitors network route efficiency.
- Real-time topology and configuration improvements to adjust for anomalies.
- Network uptime backed by Service Level Agreements.
- Network management performed by only authorized personnel.

ENVIRONMENTAL CONTROL

- Dual power paths into facilities.
- Uninterruptible power supplies (minimum N+1).
- Diesel generators (minimum N+1).
- Service agreements with fuel suppliers in place.
- HVAC (minimum N+1).
- VESDA / Fire Suppression.
- Flood detection.
- Continuous facility monitoring.

HUMAN RESOURCES

- Background screening performed on employees with access to customer accounts.
- Employees are required to sign Non-Disclosure and Confidentiality Agreements.
- Employees undergo mandatory security awareness training upon employment and annually thereafter.

Rackspace maintains various certifications to assist you in verifying the security policies and processes Rackspace has in place for the environment of your hosted infrastructure. Rackspace has been assessed and holds validation for the following compliance frameworks.

- ✓ ISO 27001
- ✓ SSAE 16 and ISAE 3402 (previously SAS 70 Type II)
- ✓ PCI DSS

RACKSPACE COMPLIANCE

ISO 27001

Rackspace ISO 27001 certified Information Security Management System (ISMS) is an iterative management system that helps ensure the security policies and processes are effective in mitigating identified risks. Specifically, the ISMS at Rackspace certifies the management of information security in the operations of their data center facilities.

SSAE 16 AND ISAE 3402

The global Rackspace Type II to SOC 1 report can be used to satisfy requirements under both the SSAE 16 and ISAE 3402 standards. This report contains a description of the controls in place and the auditors' informed opinion of how effective the controls were during the audit period. Rackspace audit period is from 1st October to 31st September of every year.

PCI DSS

A qualified security assessor (QSA) validates Rackspace as being a PCI DSS Level 1 service provider. The QSA validation of our compliance to the PCI DSS covers:

- Physical security for Rackspace data centers located in:
  - ✓ United Kingdom
  - ✓ Germany
  - ✓ United States
- Network infrastructure (routers and switches).
- Rackspace employee access to network devices.

RACKSPACE SECURITY ASSESSMENTS

ORGANIZATION SECURITY

- Security management responsibilities assigned to Global Security Services.
- Chief Security Officer oversight of Security Operations and Governance, Risk, and Compliance activities.
- Direct involvement with Incident Management, Change Management, and Business Continuity.

OPERATIONS SECURITY

- ISO 27001/2 based policies reviewed at least annually.
- Documented infrastructure Change Management procedures.
- Secure document and media destruction.
- Incident management function.
- A Business Continuity plan focused on the availability of infrastructure.
- Independent reviews performed by third parties.
- Continuous monitoring and improvements of security programs.

ORANGEHRM COMPLIANCE

ISO 27001:2013 CERTIFIED SERVICES

ISO 27001:2013 Certification establishes the requirements for implementing, maintaining, and continually improving an information security management system (ISMS) within the organization environment along with requirements for assessing and treating information security risks.

Our certified client services include:

- Technical Operations (Tech Ops)
- Product & Training Services
- Customer Success Management
- Support Services

GDPR COMPLIANCE

GDPR, also known as the General Data Protection Regulation requires all organizations dealing with personal data of EU citizens to be compliant with this privacy and security law which was passed by the European Parliament on May 25, 2018.

As required by GDPR regulations we ensure the personal data of EU residents are protected through a range of security protocols and features such as the ability to purge employee information, consent to retain candidate and employee information, audit trails and changelogs, and strict data handling protocols.

Please follow the link to learn more about how OrangeHRM complies with GDPR -

https://www.orangehrm.com/resources/news/gdpr-readiness/

ICO REGISTERED VENDOR

According to the U.K. Data Protection Act of 1998, all organizations controlling the data of UK citizens are required to register with the Information Commissioner's Office (ICO) which implements the GDPR of the European Union in the U.K.

ORANGEHRM SECURITY CONTROLS

MANAGED DATA BACKUP

- Daily onsite disk-based database backups
- 4-week rolling backup retention - (Extended on request)
- Full backup of the file system is taken weekly and differentials are taken daily
- Encrypted backup drives

DATABASE ACCESS CONTROL

- Monitored role-based access for maintenance and security checks
- Strict governance - Read our privacy policy for more details
  https://www.orangehrm.com/assets/Documents/OrangeHRM-Service-Privacy-Policy.pdf

APPLICATION SECURITY

- HTTPS Protocol (TLS 1.2/1.3)
- Password Security
  - ✓ Security assertion markup language 2.0 (SAML 2.0)
  - ✓ Enable expiration
  - ✓ Enforced strong password
  - ✓ CAPTCHA and access block for failed attempts
  - ✓ Secondary password
  - ✓ Regular OWASP assessments
- Configurable role-based access levels

- For more information contact our Data Protection Officer (DPO) at **dpo@orangehrm.com**

Thank you!

www.orangehrm.com

Version 2.0