Security Data Sheet

SyncHR

SyncHR is committed to the security of your data. This document details our security architecture and procedures to protect client information.

Certifications

SyncHR is in the process of obtaining SSAE Certification. We have engaged a leading international firm (BDO) to perform an SOC audit of our environment.

- SOC 1 Type I report (as of Feb. 2019)
- SOC 1 Type II report (in process)

Additionally, our hosting provider, Rackspace, is SSAE Certified.

- Rackspace SOC 1 Bridge Letter
- Rackspace SOC 2 Bridge Letter

Network Security

- All access is centrally controlled via Identity Provider and access is role-based, limited to privileged personnel, and it requires two forms of authentication.
- Physical security is provided by our managed hosting vendor, Rackspace.
- Network hardware and operating systems are kept current as CVEs are discovered.
- Rackspace provides secure and available network, internally and externally, managed and maintained by highly-trained, privileged staff.
- Rackspace provides enterprise-grade expertise and supporting infrastructure for the SyncHR production application stack.
- Rackspace managed network provides secure network segment used for monitoring and management access.
- Firewalls provide network perimeter security via firewall policies. Traffic is segregated and firewalled into logical zones.

Product Security

Comprehensive system servers log key security indicators including (but not limited to):

- Successful and unsuccessful logins
- Privileged account usage
- Policy changes
- Account creation and Audit Trails

Data Encryption

- Backups are transmitted across an encrypted transport mechanism to remote data centers.
- All web traffic is served using Secure Sockets Layer (SSL / HTTPS).
- Passwords are encrypted with one-way encryption. Unencrypted passwords are never sent via email.

High Availability

- We maintain a local database replica to which we automatically fail over should there be any problem with the primary database.
- All application servers are redundant and load balanced within the primary data center.

Disaster Recovery Process

SyncHR maintains servers needed for Disaster Recovery in a different geographic region from our Production servers.

- In the event of an outage in our primary data center, we manually switch DNS to failover Disaster Recovery servers.
- We are constantly streaming database changes to database replicas to ensure current data on DR servers.
- We continuously synchronize documents between production and DR environment.
- We keep current software installed and running, ready to support a production load in the DR environment.
- We monitor all applications needed for runtime.

Total estimated downtime based on drills is 2 - 4 hours.

Privacy & Security Assessment

SyncHR is currently pursuing SOC-1 and SOC-2 certification. We perform periodic assessments of our security, and test our processes regularly. We have contracted with three firms to assist us with our security preparedness and testing:

- **NCC Group** is our partner for Penetration Testing. More information about them can be found at: https://www.nccgroup.trust/us/.
- **NCA Security Services** is our partner for Network security and IT procedures. More information about NCA can be found at: http://www.ncanet.com/solutions/security.html.
- **BDO** is a well-respected SOC auditor that certifies compliance with SOC-1 and SOC-2 standards.

Audit-Enabled Solution Design

SyncHR has been designed and developed in a way that provides advanced audit capability. No data is removed from SyncHR. Even "deleted" data is done in a way that marks the data as deleted but retains the data for audit purposes. Additionally, all changes are linked to a user, with access to when the change was made, and from what IP address.