TotalRewards Software

Security Datasheet

Total rewards management that lets you sleep at night

- Full disk and database encryption using separate encryption keys for each organization ensuring that even in the highly unlikely event of a compromise of our file system your data at rest is still protected.
- Data is replicated and backed up regularly to ensure that no data is lost in the event of catastrophic events.
- Strict firewall configuration preventing database and storage server access from the public.
- Network packet inspection, filtering and transformation at the Link, Network, Protocol, and Application layers.
- Datacenter servers are certified against ISO 27001 and AICPA: AT 801 (formerly SSAE-16) with SOC 1, SOC 2, and SOC 3 reporting.
- Data in motion is encrypted using AES 128-bit SSL certificates implementing only TLS 1.2. Supported browser may even take advantage of ECDH-ECDSA cipher suites to make data in motion compliant with NSA Suite B Cryptography requirements.
- Password hashing implementing PBKDF2-SHA512; exceeding NSA Suite B Cryptography requirements.
- Infrastructure management requires IP whitelisting and two factor authentication from our IT staff to ensure that only approved individuals can access infrastructure.
- Working documents are stored on encrypted storage devices with policy driven access controls to ensure that only your implementation manager has access to sensitive data before uploading to our platform.
- Our physical facilities are secured by multiple controlled entry points.

Your total rewards information is safer in our world. We value security, performance, availability, and resilience above all else. Our organizational culture is built on those key values, which reflects in how our sales, implementation, support, and technical teams interact with you.

Security Specifications

Goal	Method	Reference
Protect data in motion while accessing Software-as-a-Service via a web browser	• AES 128-bit encrypted SSL Certificates • TLS 1.2 only • ECDH-ECDSA handshaking cipher suite when support by the client browser; meets NSA Suite B Cryptography	http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf
Protect data at rest on the file system level	• Data is encrypted at rest using the AES-128-CBC algorithm • All servers in our datacenters follow this requirement	
Protect data at rest in the database	• Data is encrypted at rest in our database using the AES-256-CBC algorithm • Meets NSA Suite B Cryptography	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
Ensure ISO and AICPA compliance of server infrastructure	• Certified against ISO 27001 • Certified against AICPA: AT 801 (formerly SSAE-16) • SOC 3 reporting available upon request • SOC 1 & SOC 2 reporting available with NDA	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm http://www.aicpa.org/research/standards/auditattest/downloadabledocuments/at-00801.pdf
Ensure passwords of users are protected	• Password hashing using PBDKF2-SHA512 • Exceeds NSA Suite B Cryptography requirements	http://tools.ietf.org/html/rfc2898 http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
Control and monitor network access of system resources	• Packet inspection, filtering and transformation at the link, network, transport, and application layers	