Security

Obo Risk Mitigation

Your product data is your precious intellectual property, and it may be highly confidential. That's why our top priority is the security and privacy of your data in Obo.

Cloud Security

The Obo cloud infrastructure runs on secure Amazon Web Services (AWS). Obo leverages AWS network security for our product environments (dev, QA, staging, demo, and production). We periodically install patches for major releases or monthly, whichever is more frequent.

Application Security

OWASP Zed Attack Proxy (ZAP) scans Obo production and staging environments after every release push. We use periodic log inspections to look for anomalies in application usage.

Secure Architecture

The Obo application is multi-tenant. Data is always encrypted at rest or in flight. Obo utilizes AWS instances, with Amazon RDS encrypted DB (Amazon Relational Database Service). The Obo application uses Auth0 to manage Obo authentication (MFA, SSO, etc.). SonarQube scans Obo application code on every code push.

Privacy

Customer data is accessible only by the Obo customer who owns the data. Only with express consent may an Obo employee view a customer's data, and even then only after a customer tenant admin creates an account for that Obo employee. Obo does not have a "super user" or backdoor method for viewing data stored in Obo customer tenants.

Security Responsibilities

Our Chief Technology Officer (CTO) is responsible for defining Obo security policies and operations. Our CTO oversees all security reviews, audits, scans, policy enforcement, and incident responses. All Obo employees take personal responsibility for our customers' security.

Incident Response Plans

Obo has an extensive Incident Response Plan (IRP) that defines responses for all common incidents, including security and data breach incidents, which could affect Obo operations or Obo users.

Security Policies and Training

Obo has documented policies for acceptable encryption, clean desk, email, passwords, and customer data. In addition, every employee is required to attend an annual Obo Security training session given by the CTO and monitored by Obo executive staff. All employee laptops are strictly monitored by the Obo asset management plan.

Physical Security

In addition to the physical security provided by AWS, the Obo office enforces keycard access for all employees.