zipBoard

Security Overview

User data protection & security is a top priority for zipBoard. We want to make sure that while using zipBoard your & your client's data is secure & protected. We make every effort to share our security policies and practices.

zipBoard uses industry-standard physical, and technical infrastructure to preserve the security of your information. We understand the importance of securing your work and are available for further questions regarding security at support@zipboard.co

Customer Data Access

Access to customer data, logs is restricted to only authorized employees. Security training is provided to all employees and contractors. On termination of employment or contracts, all access to internal systems are revoked. Password managers / SSH access used to access admin systems & service accounts.

Audits & Third party assessment

zipBoard engages independent third party auditors to conduct regular penetration tests. Findings of these tests are reviewed by an internal team and fixed on priority at regular intervals. Scheduled tests for continual security improvements are also conducted.

Security Monitoring & Alerts

We have an internal security monitoring system in place to detect and block suspicious activity. Regular review of internal logs & CloudWatch to prevent any malicious activity for better insights.

Access through secure connection (TSL/SSL & HTTPS)

zipBoard transmits data over networks using an encrypted SSL (TLS) connection to ensure data privacy. All authentication data or sensitive data is encrypted using AES -256 encryption. We use SSL certificate issued by Comodo Inc.

Data Centers

zipBoard uses Amazon AWS as the primary data center & server. The AWS infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure AWS data centers. The servers operate at full redundancy.
Amazon Simple Storage Service (Amazon S3) provides a highly durable storage infrastructure designed for mission critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities within a region, designed to provide a durability of 99.999999999% (11 9s). Find more details about AWS data centers **here**.

Data Deletion

On canceling an account with zipBoard, all user data is immediately deleted. Also, the related backups and log data is deleted within 30 days.

Backups & Disaster Recovery

Scheduled weekly & monthly backups (EBS & S3 snapshots) are done to ensure continued access & a fab back solutions. Well tested & fast access to backups also stored on AWS.

Conclusion

We understand the importance of data & more importantly customers data. We treat security as our top priority and work hard to win our customers trust.