Capitect Security

At Capitect, data security and privacy are our top priority. We and our trusted partners meet and exceed industry standards to keep our customers' data secure, encrypted, and private.

Security

Capitect employs industry-standard capabilities to protect data, including data encryption in transit (secure HTTP with transport layer security), data encryption at rest, secure development practices (OWASP Top 10 Web Application Security Risks), and request authentication.

Encryption

Capitect utilizes bank-level encryption for all personally identifiable information beyond the typical username/password, including but not limited to names, emails, phone numbers, addresses, account names, etc. In addition, Capitect automatically encrypts data when it is stored to disk.

Account Login Information

Capitect does not store account login information, such as username and password. We partner with trusted 3rd party data aggregators to pull account data (read-only access) so that we can provide our customers a better experience viewing their financial data. We do not have write-access to your account or the ability to execute transactions within your account.

Restricted External Access

Privacy is core to our business. As Capitect employees, we only have a limited, encrypted view of your data and can only gain access to decrypted account details (firm/client details) with your permission.

Redundancy Policy

Capitect performs daily data backups on secured, access controlled, and redundant storage. In the event of outage, backups are automatically deployed to bring the application back online.

Password Protection

Capitect employs password protection on all its accounts. Users are required to authenticate themselves with an email and password prior to accessing their financial reports and documents on the site. Users are also required to verify the email they use to log in. Users are automatically logged off after 30 minutes of inactivity.

Trusted Partners

- Heroku
- Amazon Web Services
- Yodlee

To learn more about Heroku Security:
https://www.heroku.com/policy/security

To learn more about Amazon Web Services Security:
https://aws.amazon.com/security/

To learn more about Yodlee Security:
http://www.yodlee.com/yodlee-security/