Biomeme

Biomeme App Security Statement (v1.1)

The Biomeme Cloud ecosystem has been designed for security and data integrity. Databases are securely stored with industry-standard AES-256 encryption. All Cloud connections require HTTPS connections. The Cloud ecosystem is deployed within a virtual private cloud with minimal access to the external cloud system further isolating and protecting the system.

Biomeme mobile applications leverage iOS and Android application sandboxing to protect data. It is recommended to further protect the data by adding a secure passcode to the phone along with encrypting the phone's storage. Mobile applications use the same secure HTTPS connections as all of Biomeme's web applications to ensure all data is protected in transit.

Biomeme Cloud users must always be authenticated using stringent password requirements.

- Forced SSL connections
- Network limited access to the database
- Fully authenticated API
- Original data is always stored and cannot be overwritten

REFERENCES

AES-256 encryption: *https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.Encryption.html*

Client-side SSL certificates: *https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html*

Lambda security overview: *https://d1.awsstatic.com/whitepapers/Overview-AWS-Lambda-Security.pdf*