Wildnote

Data Security Specifications

Infrastructure Overview

- Wildnote, a digital platform for collecting, managing, and reporting data, is a cloud-based service running on Heroku, which sits atop the Amazon Web Services (AWS) infrastructure.
- Wildnote adheres to the policies of the Amazon Web Services standard agreement. For more information, see https://www.heroku.com/policy/security and https://aws.amazon.com/security.
- All traffic to Wildnote web app and native app API is sent over 256-bit secure SSL encryption.
- Wildnote is a Ruby on Rails web application.
- Wildnote mobile apps for iOS and Android are completely native, built using Swift and Java respectively.
- All server requests are handled by a Puma web server.
- All persistent data is stored on a PostgreSQL database server.

Data Security

- All user accounts in WIldnote require 8-character minimum passwords for authentication to the system.
- Authentication uses standard challenge/response, with SHA1 password hashes stored in the PostgreSQL database.
- Photo, video and documents uploaded to Wildnote are handled by Cloudinary (https://cloudinary.com/) and stored on the AWS framework.
- All uploaded files are stored on S3, a distributed, high-availability storage engine that grows along with your Wildnote content.
- All content stored on S3 is accessible only to your user account through the web and native apps.
- The database and all uploaded content are stored redundantly across datacenter locations to mitigate data loss and increase availability and uptime.
- All data is private and is not shared between accounts on the system based multi-tenancy standards.
- A user cannot access your account unless invited by an administrator of the account. Users are assigned permissions and can only access data via assigned roles on a per-project basis.
- All users retain ownership of all data.
- Authentication to the API is accomplished via unique tokens associated with each account which can be reset at any time.