Swivl Security Overview

(2014-10-28)

Infrastructure

- Swivl Cloud runs on Amazon EC2 Compute Cloud for the core application. Swivl Cloud uses Amazon S3 for storing your video. Amazon states that they have highly secure data centers which utilize state-of-the art electronic surveillance and multi-factor access control systems, that its data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. You can learn about Amazon's security at the AWS Security Center.
- AWS has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). AWS undergoes annual SOC 1 audits and have been successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems.
- Access to Swivl Cloud data portal management is limited to several key employees and is protected by a two-factor authentication mechanism for access, requiring authorized team members to first log in using their email address and password, then enter a six-digit access code that refreshes every 30 seconds from a linked mobile device.
- All private data exchanged with Swivl Cloud is always transmitted over SSL.
- For API connectivity between Swivl Capture app and Swivl Cloud, we use OAuth authentication occurring over SSL protocol.

User Video Access

- Other Cloud users can't see your projects unless you deliberately share public links to projects or share projects via email or group.
- If a video is shared with a specific user via email, if someone else gets this email, they will be unable to access the video unless they have login credentials of that user.
- Public projects are only viewable by people who have a link to the project(s).
- Videos that are deleted by the user are retained for 30 days for recovery purposes due to accidental deletion (per user request) and then removed permanently from the Swivl Cloud storage servers.
- Swivl Cloud user listings are not available or visible to individual users and thus all student data is hiden
- Only Swivl Cloud Institutional Account administrators have additional visibility to their member data, but it is specifically configured by each administrator and has to be explicitly accepted by each Institutional Account member.

Company Policies

- Swivl employees are prohibited from viewing the content of files you store in your account. Employees may access file metadata (e.g., file names and locations) when they have a legitimate reason, like providing technical support. Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so).
- A very select number of employees (senior engineering leadership) have the ability to access video data only when legally required or requested by customer for technical support.