Security Terms, 2014-03-03

Thank you for choosing uiProject!

Terms Overview

This document specifically lists responsibilities and properties of security and privacy for uiProject (the "Service") for both uiSystems, Inc. ("uiSystems" or "uiS") and You, the Customer, as applicable.

Secure Storage

The backbone to uiProject is served through MACCIUS™ Server Hosting facility in CA, USA. The Server Hosting company provides a physically locked down data center and ensures 24x7x365 high bandwidth, redundant, connectivity to internet, redundant power source as well as a controlled environment for the server with regards to temperature and humidity and 24x7 support personnel.

Only the personnel hired by or accompanied by the Server Hosting company have physical access to the servers running uiProject. The facility is protected by alarm system, video surveillance and professional security staff. The facility has smoke detectors and fire protection as well as alarm systems for humidity, temperature and flooding. The data center is ensured against theft, damage and accidents.

Only uiSystems have login accounts to the server itself. The server is dedicated to uiSystems, hence uiSystems have full control over all applications and services running on it.

All non-essential ports on the servers are closed down to minimize risk for intrusion. The operating system is protected against virus attacks and other malign code.

uiSystems agrees to immediately notify Customer in the event that uiSystems (or its 3rd party hosting provider) reasonably suspects that Customers data has been, or may have been, lost or subject to unauthorized internal or external access.

Secure Transfers

All data exchange between the uiProject web client and the uiProject backbone on the servers are communicated over secure a channel using 256-bit SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections, if the client software used supports it.
You acknowledge that if you wish to protect your transmission of data or files to the Service, it is Your responsibility to use a secure encrypted connection to communicate with the Services.

Your Data is Backed Up

The data on all our servers are backed up daily to protect against data loss and ensure no or very limited downtime in case of malfunction of storage arrays. The backups are not intended for retrieval of lost, overwritten or corrupted data.

Privacy

We guard Your privacy to the best of our ability and work hard to protect Your information from unauthorized access.

uiSystems' employees are prohibited from viewing the content of files You store on our servers including file metadata (e.g., file names and locations). Like most online services, we have a small number of employees who must be able to access user data when legally required to do so or when working on specific customer's support cases. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.

uiSystems may include Customer's name in a list of uiSystems customers on the uiSystems website and PR material.

How to Add Your Own Layer of Encryption

Customers who wish to manage their own encryption keys can apply encryption before uploading files to uiProject. Please note that if You encrypt files before uploading them, some features may not be available. Doing so will also make it impossible for us to recover Your data if You lose Your encryption key.

Compliance with Laws and Law Enforcement

In compliance with United States law, uiSystems cooperates with United States law enforcement when it receives valid legal process, which may require uiSystems to provide the data of Your uiProject accounts and projects.