GRABCAD

SECURITY AT GRABCAD

SECURITY AT GRABCAD

The GrabCAD platform

The GrabCAD platform contains user submitted engineering information across three applications: Workbench, Print, and Community. All information submitted to GrabCAD Workbench and GrabCAD Print is kept strictly confidential. This paper will outline the industry-leading measures that GrabCAD has taken to ensure that our users' intellectual property is secure.

How it works

GrabCAD hosts two different and separate types of information: private and public. Intuitively, only the GrabCAD Community hosts information that is typically shared publicly.

GrabCAD Workbench and GrabCAD Print host private information. In these applications, users can upload models for private collaboration. These models are never shared with the Community. When a user uploads a model into Workbench or Print, no one can see it until the member invites specific people, typically by entering their email address.

The invited user receives an email and must log in to GrabCAD with their name and password to see the model. This ensures that GrabCAD Workbench and GrabCAD Print models are only seen at the invitation of the submitter.

By comparison, the content in the GrabCAD Community is public – this includes 3D models or renderings that members load for sharing, answers that they post in response to public questions, and member profile information like name and education. This information is meant to be shared and is clearly identified as such.

Information like a user's email address password and usage patterns are always private, regardless of where they are in the GrabCAD platform.

Secure Communication

All models and comments loaded into GrabCAD Workbench and GrabCAD Print use secure https URLs and are encrypted using industry standard 256 bit AES encryption.

Data Center Security

GrabCAD stores all data using Amazon Web Services (AWS). With AWS the data is stored redundantly across multiple devices across multiple environmentally controlled facilities. AWS infrastructure and controls are subject to annual SAS-70 Type II audits and AWS information security management processes and controls have achieved ISO 27001 and PCI DSS Level 1 certification. GrabCAD is located in Cambridge, MA and all of our AWS data centers are located in the United States.

Network and Application Security

GrabCAD ensures that our network and application are secure by constant maintenance and regular penetration testing by third parties. Maintenance procedures include ensuring that all network software is up to date, while penetration tests include testing application for common and application-specific vulnerabilities that could be exploited. All traffic related to your account data and private materials stored in GrabCAD Workbench and GrabCAD Print is sent over the network in encrypted form, using TLS 1.0 industry standard protocol with AES-128 or AES-256 encryption, depending on your browser.

Internal Controls

GrabCAD grants access to stored data internally using the "principle of least privilege"

through appropriate roles and only on a “need to know” basis, and manages its systems in line with security industry best practices including the ISO 27000 series and NIST Security Publications. GrabCAD’s engineers do have the authority to transfer your data – as is required to assist you at your request – or to handle some of our infrastructure management tasks such as load-balancing. Such transfers do occur exclusively within the GrabCAD data environment.

Cancelling Your Account

In the event that a GrabCAD account is canceled, the account’s data will be deleted as part of the cancellation process. If you wish to migrate or download the models, you can arrange for this service prior to cancellation. Deleted files are unrecoverable – by design – to ensure that your data is not compromised.

Find Out More

If you’re interested in learning more about the measures we take to protect your intellectual property, please contact us at any time.