Security Overview

Understanding the need to address security concerns, Procore has created a multi-tiered approach to ensuring data security and application stability, both integral to maintaining the safekeeping of your virtual capital. Procore employs solutions to three main areas of concern: the privacy and security of your cyber data, software failures, and hardware failures due to unplanned phenomena.

1 Data is private and secure.

Procore has a multi-pronged approach to privacy and cyber security both provided via Procore's standard operating security policies and those offered within the application, giving privacy control to the company itself.

Procore employs the "gold standard" of advanced security.

Procore has implemented top-level security measures to ensure data is unbreachable with Secure Sockets Layers (SSL) encryption technology to safely deliver your data is via transit through the Internet. Procore also practices advanced encryption standards, using 256-bit encryption technology.

Information and passwords are double protected.

When users register with the Procore application, they are guaranteed the highest level of user password encryption using hash + salt cryptography making reverse engineering for hackers a difficult task. With this procedure in place, Procore, or any software developer for that matter, cannot access a user's password.

Users have control over privacy and permissions within the application.

Procore also puts privacy and security into the hands of the company administrators within the application, providing granular level control through "triple permissions" flexibility. Company administrators can determine a user's access from the individual user level, individual document level, and the individual project level which means that projects, documents, and communication won't be shared with those who aren't approved.

Nothing goes untracked within the application. Nothing.

Procore actively logs every user action globally and locally—right down to the individual Tool level. Every action per document or schedule change is logged as well as all user logins. So, in the unlikely event a user attempts a malicious activity within the application, the company administrator can easily trace the action back to the perpetrator.

2 With Procore, preparedness is paramount to security and stability.

Protecting a company's virtual information and ensuring application stability of the software is imperative to providing a seamless and confident user experience.

Procore uses redundancy.

Procore's entire information architecture, both software and hardware, is designed to operate within a system of redundancy. Customer data and assets are maintained in a remotely hosted application database. Using "master and replica" architecture, the data is simultaneously written to two separate databases, on two different physical devices, in two different geographical locations. All data is then copied nightly to a third, off-site file storage disk array.

Secure online code repositories.

Procore's application code (minus customer data) is kept in a secure online code repository hosted by an external commercial provider. This means fewer headaches for internal code developers and more product stability for companies using Procore.

3 In the rare case of a disaster, Procore and its users are covered.

Procore has prudently determined various solutions to ensure that whatever potential unplanned phenomena, hardware, data, user security, and application stability are protected.

Procore uses state-of-the-art, secure facilities.

Procore's servers are located in a secure cagespace at Rackspace facilities that utilize the latest internal security technology such as biometric scanning and keycard protocols. The facilities are under 24 hour interior and exterior surveillance monitoring and only authorized data center employees who have undergone multiple background security checks can enter.

Component failure won't interrupt service.

Procore ensures the hardware units are not only safe, but "hot swappable," meaning they can easily be replaced or supplemented. Rackspace, the server host center, utilizes N+1 redundant HVAC UPS (Uninterruptable Power Supply) systems ensuring if there is a component failure, there is an immediate back up, reducing the chance of service interruption for Procore customers.

The continuous evolution of security procedures is always on the mind of Procore leaders who understand that compromises in data, security, and privacy are foundational business concerns. Procore has initiated above standard procedures at all levels to maintain application security and stability. Moving forward, those procedures will continue to grow and extend in order to ensure peace of mind for all users.

If you would like more information on the aforementioned security policies, procedures, or standards, please feel free to contact us at: sales@procore.com