PROCORE | odrive

Security Overview

Using odrive with Procore is safe and secure. Our service is hosted on Google Cloud and Amazon Web Services, and we use proven standards and protocols. Email us at sales@odrive.com or learn more at: https://docs.odrive.com/docs/security-faqs

Does odrive store my files?

No, odrive never stores your files. All of your files remain in the Procore service.

How is authorization to Procore handled?

The OAuth 2.0 standard is used for authorizing odrive to access your Procore data. When odrive asks you sign in to your Procore account, you sign in directly to Procore's service, so odrive never sees your password. Procore assigns odrive an access token which odrive retains.

How does odrive interact with Procore?

Linking and authorizing Procore allows odrive to send requests to Procore on your behalf. The odrive sync app can then make encrypted HTTPS requests directly to the Procore API, providing storage management and sync capabilities.

What does odrive store?

After authorization is granted, the access token given to us by Procore is stored encrypted (AES in CBC mode) in the odrive service layer so users with installs across multiple systems won't need to re-authorize each system separately.

Procore's access tokens expire every two hours, requiring odrive to get a new access token from Procore periodically. The encrypted access tokens are deleted if you unlink your Procore account. You can also revoke authorization for odrive from the Procore Web application at any time, rendering the tokens useless. In either case, odrive loses the ability to access your Procore files.

What file permissions are enforced?

Documents tool permissions are fully enforced when using odrive. This includes your access level to the Company and Project level Documents tool (None, Read Only, Standard, Admin) and also at a file and folder level when setting the "Make Private" checkbox.