OnceHub Support

Introduction to Security

Last Modified on Jun 5, 2023

This article describes security processes and features in our application. To learn about all our security processes, visit the OnceHub Trust Center.

OnceHub is a vendor you can trust. Customer trust is earned via the transparency we provide through four guiding principles: Security, Availability, Privacy and Compliance (the OnceHub pillars of trust). By exposing the processes and measures we take to protect your data, we hold ourselves accountable to the highest level. At OnceHub, trust is an ongoing effort to continually evolve, learn and improve in the ever changing security landscape.

We understand that even with the best intentions, security vulnerabilities can exist. We take a multi-tiered approach to reduce the likelihood of a breach, and minimize our exposure to the risks. Through tight controls, good training and secure development we provide the assurance you need to entrust us with your data.

Application security features

As part of our application security we've delivered various security features to meet the requirements of our Customers.

Account security

OnceHub allows you to enforce organizational information security policies through account level security features. You can enforce:

- Two-factor authentication - enable two-factor authentication to add an extra layer of security to your account.
- Password policies - including password length, complexity and expiration.
- Account lockout - enable or disable account lockout and decide how many unsuccessful login attempts result in a lockout.
- Session timeout - enable or disable session timeout and set the timeout time frame.

Learn more about how your sign-in credentials are stored and protected by OnceHub

Third-party integrations security

We understand that third-party systems contain sensitive data you need to protect. Where possible, OnceHub integrations use secure authentication methods such as OAuth 2.0 and data is encrypted at rest using AES with 256 bit keys.

Learn more about how we secure data in our Trust Center

OnceHub Booking page security

The Booking page is a key junction in the data flow into OnceHub. The Booking form automatically operates in a private mode when stored customer data from a database is used to prepopulate the booking. Users are always required to sign in to download secure attachments.

Application security processes and controls

Application security is a core component of the Security Trust pillar. At OnceHub, we consider the security of your

data at every stage of the development lifecycle. From concept and design stages to implementation and testing, we make sure that our application keeps your data private and protected.

Privacy and security impact assessments

New features are reviewed by our security manager and executive management. They are assessed for their potential impact on privacy and security. We make sure that settings that potentially expose your data are kept private by default.

Secure development best practices

We work with an experienced development team that is regularly trained on security best practices. We follow OWASP guidelines to ensure we develop secure applications.

Security QA and testing

We take a multi layered approach to testing. Developers perform peer reviews, our QA team performs vulnerability scans and an external team perform periodic penetration testing on the application and infrastructure.