OnceHub Support

Security best practices

Last Modified on Nov 7, 2024

At OnceHub, the privacy and security of your data matters to us. We employ the latest technologies and have built controls in our platform to ensure that your data is protected. Our security measures are re-enforced when you follow security best practices.

Passwords

If you sign in to OnceHub with an email and password combination, we recommend constructing a strong password. A strong password should:

- Contain 8 or more characters.
- Include a combination of lower case letters and numbers.
- Be changed every 3 - 6 months. Learn more about how to change your password
- Not be used on other systems or accounts.
- Not contain personal information, such as date of birth or name of someone close to you.

A default password policy is set on all OnceHub accounts. The default policy requires that all passwords are at least six characters long and include both letters and numbers.

Custom password policies

Stricter password requirements can be enforced with a custom password policy.

- Password length and complexity can be adjusted.
- Passwords can be set to automatically expire ensuring that they are updated periodically.

Custom password policies are a great way to ensure that password best practices are followed by all Users in your organization. Learn more about Custom password policies

Account lockout

Account lockout provides an additional layer of security for your OnceHub account. It protects against brute force login attempts and automatically suspends account access when multiple failed login attempts have been identified. Learn more about Account lockout policies

Short sessions

Enabling Short sessions protects your OnceHub account from unauthorized access. With Short sessions enabled, an automatic timeout is triggered after a period of inactivity. Learn more about session policies

Least Access principle

When managing multi-user accounts, the Least Access principle ensures that Users see only the data necessary for

them to fulfill their role. OnceHub provides various permission levels and User roles to allow for clear and simple management of this.

When using OnceHub, you should ensure that your Users can only access the Booking pages, settings, and meetings that are relevant to them. Where possible, restrict access to Booking pages and use granular-level permissions to prevent editing on Booking page settings that do not require changes. Learn more about Booking page access

Note:

For accounts using a G Suite ID to log in, we authenticate you using the latest OAuth 2.0 technologies. Once you are successfully authenticated by Google, we receive a secure token from them which enables access to your OnceHub account. With Google authentication, securing access to your G Suite account is equivalent to securing your OnceHub account. We recommend enabling 2-step authentication on your G Suite account, as well as following the password policy guidelines recommended by Google.