Securing your account according to the GDPR

Last Modified on Nov 7, 2024

Data protection by design and default require controllers to ensure the security of their OnceHub accounts. By default, OnceHub requires Users to use a secure password with at least six characters, including numbers and letters. In addition to our default settings, OnceHub also allows Users to set custom security policies such as stricter password policies, account lockout and short sessions. These additional security policies ensure that you are protecting your account to the highest degree possible.

To update security settings, you must be an Administrator. However, you do not need an assigned product license. Learn more

Configure security settings for your OnceHub account

1. In your OnceHub Administrator account, in the top navigation menu, click the gear icon → **Security** → **Password policies**.

2. Define your password policy. You can set a minimum length, complexity, expiration period, and whether Users can reuse their previous passwords. When finished, press **Save**.

3. Click on the Account lockout policies section (see Figure 2). Click to enable Account lockout. This protects against brute force login attempts and automatically suspends account access when multiple failed login attempts have been identified. Select the number of times a User can unsuccessfully try to login within a specific time frame. When finished, press **Save**.

4. Click on the Session policies section (See Figure 3). Click to enable Short sessions. This setting will automatically sign out Users after a specific period of inactivity. Define the period of time until Users are signed out. When finished, press **Save**.

You're all set! You have now set up custom security policies to protect your OnceHub account. Learn more about security at OnceHub

To learn more about OnceHubs compliance with the GDPR, read our ebook: A practical guide to using OnceHub in a GDPR compliant manner