Security and GDPR best practices

Screenshot_2020-04-29_at_19.1 Getting started

In this article, you can find information about best security practices when using the Tau Ceti admin panel and contacting the Tau Ceti helpdesk team.

Table of contents:

Screenshot_2020-04-29_at_19.1 TC account best practices

If you have a local account on any Yves Rocher admin panel website or a Tau Ceti Global Authorization Center you should follow the following steps to ensure that your account is secure:

Account sharing

Your account is only yours and shouldn't be shared with other employees and 3rd parties. Sharing your account information creates a high risk of a data leak, and any actions on your account show in the system log with your e-mail address. In case there is a need to create an additional account for an employee please contact the Tau Ceti helpdesk at helpdesk@tauceti.email or contact your direct supervisor.

Strong password

Your password should be strong and hard to guess. It shouldn't contain obvious information like your name, date of birth, company name, etc.

A strong password should contain:

- Lowercase letters (i.e. a, b, c)
- Uppercase letters (i.e. A, B, C)
- A number (i. e. 1, 5, 9)
- A special character (i.e. !, %, #)
- A length of a minimum of 8 characters

Your password should additionally be different than the rest of your passwords.

Examples of weak passwords:

Password123, YvesRocherTomas321, Michael20051989

Examples of strong passwords:

^vJ5a7RF6x!A@wB,chEwbAccAp!ZZa531

Tau Ceti system will not allow you to set your password without the requirements described above.

Enabling Google Authenticator

As on the TC admin panel and GAC platforms 2-factor authenticator is required and enabled by default currently you use the SMS messages to log in to your account. We highly recommend enabling the Google Authenticator, which uses the phone app to generate secure codes, which allow you to log in without receiving SMSes. It is a more secure authenticator method as well as more reliable, as it is possible to log in even when there is an outage in the SMS provider.

You can find information on how to enable and configure the Google Authenticator in the Google Authenticator article.

Screenshot_2020-04-29_at_19.1 Data sharing

Various data and data types are shared between co-workers as well as between companies. There might be a request sent to the Tau Ceti helpdesk, which requires sending data containing customer data.

Sharing sensitive data should proceed with caution and attention, as sensitive data should be received and seen only by the receiving party without the risk of a third party being able to see the information.

In order to ensure that the data is sent securely please follow the following requirements:

- If the information is available in the admin panel, please provide the link or necessary, non-personal information like order number instead of providing sensitive information like customer name, surname, and address. This will allow us to still find and check the customer without the risk of sharing their personal information.
- If the information is in an external file like a .xlsx Excel file do not share it directly.
  - Pack the necessary files into a .rar, .zip or .7z with a password using an application like Winrar or 7zip. Do not share this password with any third parties
  - The created password should be sent to the recipients by the SMS message.
  - After the request has been fulfilled and the attached file is no longer necessary the file should be deleted from the computer or secured.

Revision #2
Created 27 November 2024 21:05:32 by Tau Ceti
Updated 27 November 2024 21:06:27 by Tau Ceti