Helpdesk

- Security and GDPR best practices
- Processing of request on the Helpdesk

Security and GDPR best practices

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:

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.

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.

Processing of request on the Helpdesk

Getting started

The article contains essential information and procedures regarding requests and tasks raised by the Helpdesk team.

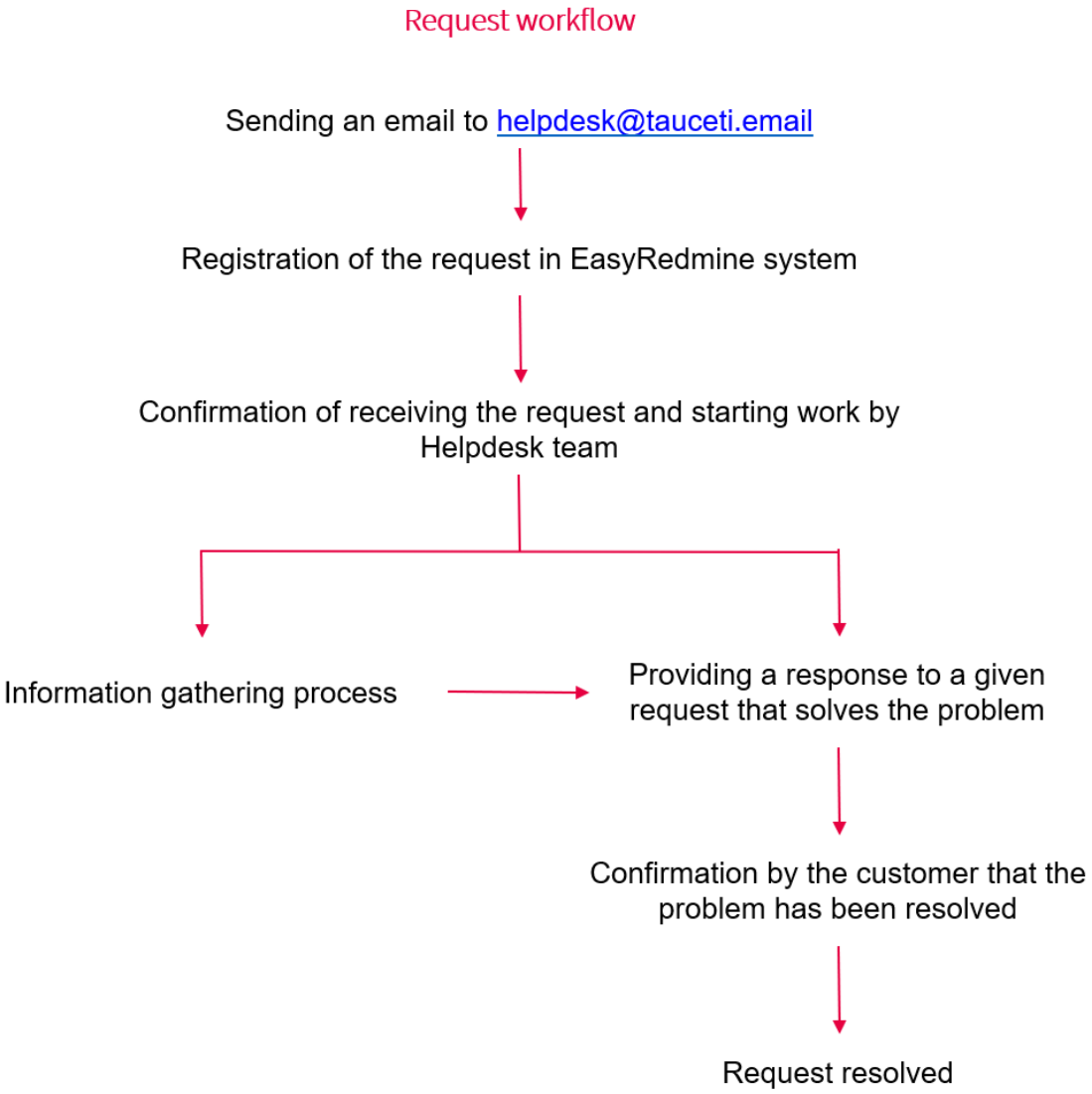
Table of contents:

General information

Helpdesk request Workflow

- EasyRedmine is a bug tracking system that we use to handle customers' requests.

- To send any kind of request, just send an email to helpdesk@tauceti.email.
- After a while, the system registers the ticket and we confirm its acceptance.
- Our answers are sent directly from the Bugtracker level and then they reach the sender by the e-mail message.
- The e-mail sent to helpdesk@tauceti.email may contain everything that the standard mail message contains.
- If you want to reply to a message received by us - simply reply to the email you have received.



Request types (Helpdesk vs DEV)

In general, requests are divided into two types:

Helpdesk requests

- All requests described later in this article

Dev requests

- DEV requests are non-standard requests that require the involvement of the development team in order to execute a given request (e.g. a request that cannot be executed by the HD team using the administration panel).
- All DEV-type requests should be processed on Asana.

Helpdesk working hours

Helpdesk provides technical support to the client and is available in the following periods:

Monday-Friday 1)	
Helpdesk working hours	09:00-17:00 hrs CET
Emergency Operator Support 2)	17:00-24:00 hrs CET

1) excluding Polish public holidays
2) only Blocking Anomalies can be reported in Emergency Operator Support time.

Saturday-Sunday 3)	
Helpdesk working hours	none

Emergency Operator Support 4)	09:00-17:00 hrs CET

3) excluding Polish public holidays
4) only Blocking Anomalies can be reported in Emergency Operator Support time.

Emergency Operator should be contacted by e-mail: helpdesk@ tauceti.email or by phone +48660599425 (Robert Wrębiak), +48660599416 (Maciej Bochyński).

Helpdesk reaction time

Helpdesk reaction time

Priority	Event	Response Time	Report Delivery Time
PRIO1	Blocking Anomaly	2 hours	8 hours
PRIO2	Major Anomaly	1 working day	2 working days
PRIO3	Anomaly	2 working days	5 working days

Emergency operator reaction time

Priority	Event	Response Time	Report Delivery Time
PRIO1	Blocking Anomaly	Monday-Friday: 4 hours Saturday-Sunday: 6 hours	8 hours
PRIO2	Major Anomaly	Not supported	Not supported
PRIO3	Anomaly	Not supported	Not supported

Definitions

Response Time – specifies the maximum time period before the Helpdesk (or Emergency Operator) confirms receipt of the issue notification and assigns priority to this issue.

Report Delivery Time – specifies the maximum time period between Response Time and the moment of delivery of the progress report on the issue to the CUSTOMER. The progress report will include: the status of the issue, verified priority level, estimated time of the solution or proposal for temporary solution if available.

Request categorisation

Requests in the context of importance are categorised into:

- **PRIO1**
- **PRIO2**
- **PRIO3**
- **Non-issue**

PRIO1 - this corresponds to SLA category 1 requests, i.e. failure of critical services.

PRIO2 - this corresponds to SLA category 2 requests, i.e. partial failure of critical services or non-critical services.

PRIO3 - all incidents/problems that are not PRIO1/2.

Non-issue - request of nature (examples):

- request for support in explaining how the mechanism works - "how to"
- An idea or a suggestion

> **Remember**
>
> It is possible to automatically mark a sent e-mail request as PRIO1, PRIO2 or PRIO3. To do that you have to type the priority level in the e-mail title for example:
>
> **PRIO1** Slovakian website is not working
> **PRIO2** Unable to search for products on PL PROD
> **PRIO3** Product is not visible on CZ PROD
>
> By doing that it will allow us to react to the issue more swiftly. Please remember that it is

> case-sensitive, so our system won't recognize "**Prio1**", or "**PRIO 1**". It has to be "**PRIO1**".

Definition of PRIO1

The PRIO1 request is a serious problem with the highest priority. There is a separate handling procedure for this request. Types of problems that can represent the definition of “PRIO1":

- Entire unavailability of the website, where the website means a full set of pages available under a given domain (desktop/mobile), for all users
- The time of loading pages of the website excludes the use of the website, for all users
- The key process does not work for all users
- The integrity of key data has not been preserved
- The security of key data has not been preserved
- The security of personal data has not been preserved
- Unauthorized access to the system
- Unauthorized change of data

What is the key process?

Key process - division:

1. From the customer side:

- User registration
- User login
- Order execution
- Functionalities in the basket enable the execution and finalization of the order

2. From the business user's side:

- Logging in to the administration panel
- Failure of the administration panel element to act directly and immediately affect key processes for the consumer (for example support of the *on/off-site* functionality)

3. From the system side:

- The exchange of order data between the web platform and the logistics system ("YRMA Logistics") does not work in a way that affects the key processes for customers
- The exchange of payment data does not work in a way that affects and is visible to customers
- The failure of integrations that directly affect the operation of key processes for customers

---

Definition of PRIO2

PRIO2 requests are partial failures of PRIO1 type critical services, however:

- Their occurrence is not massive or continuous
- Critical processes are not interrupted

Examples of problems that can be classified as "PRIO2":

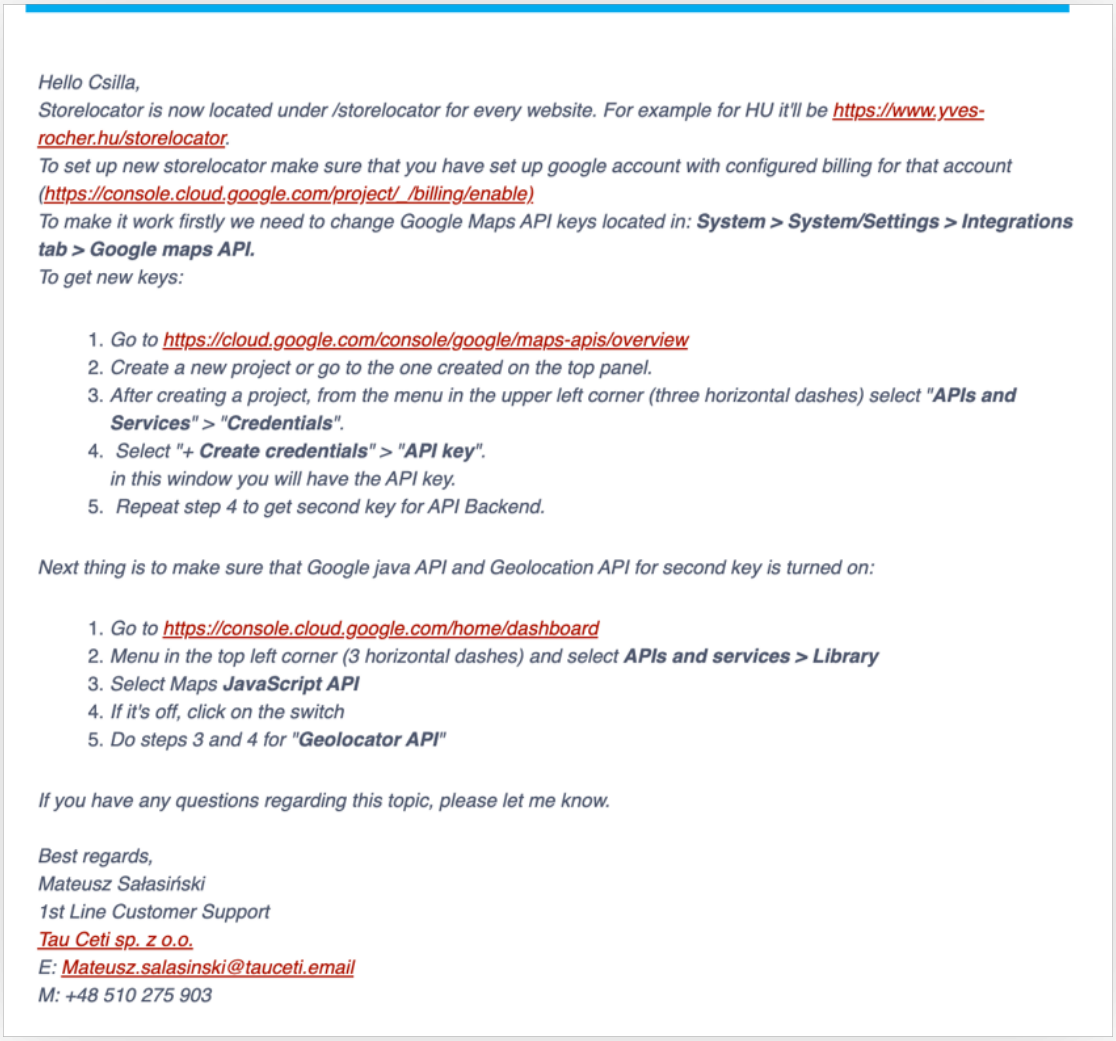
- The order confirmation email is not sent to the customer, but the order itself can be placed correctly by customers
- Partial unavailability of the website
- Product search engine on the website does not work properly
- Password reminder functionality does not work

Raising requests - best practices

1. Giving the appropriate title to the request. The title of the e-mail will be identical to the title of the registered request in our bug tracking system. The appropriate title will significantly improve the detection of the source of the problem.

2. One email sent to helpdesk@tauceti.email causes one separate ticket to be registered in our system. Therefore, the commonly used, best and strongly recommended by us practice is to describe one problem in one email.
    1. Applying threaded answers to our feedback to avoid generating new tickets which would be duplicated.
3. Giving as many details as possible about the request. This will make it much easier for us to detect the problem and solve it more efficiently.
    1. Giving exact reproduction steps.
    2. Adding bug illustrating attachments (screenshot, video).
    3. Providing information when a problem occurred.
    4. Determining where the problem occurs - only on the desktop version, only on the mobile version or on both.
    5. Determining whether the problem was one-off or repeatable.
    6. It is often useful to provide information about the device on which the problem occurred.
        1. device model
        2. operating system version
        3. information about the browser (and the version you are currently working on)
4. Information on whether the problem occurs in a mass/global scale or only for one user.
5. Specifying the environment in which the problem occurs.
6. In case of a PRIO request by typing in the e-mail title **PRIO1**, **PRIO2** or **PRIO3** you will change the priority of a task in our system automatically to the written PRIO level. This will allow us to handle your request swiftly.

View of a sample answer sent by us from Easy Redmine system



Hello Csilla,
Storelocator is now located under /storelocator for every website. For example for HU it'll be https://www.yves-rocher.hu/storelocator.
To set up new storelocator make sure that you have set up google account with configured billing for that account (https://console.cloud.google.com/project/_/billing/enable)
To make it work firstly we need to change Google Maps API keys located in: **System > System/Settings > Integrations tab > Google maps API.**
To get new keys:

1. Go to https://cloud.google.com/console/google/maps-apis/overview
2. Create a new project or go to the one created on the top panel.
3. After creating a project, from the menu in the upper left corner (three horizontal dashes) select "**APIs and Services**" > "**Credentials**".
4. Select "+ **Create credentials**" > "**API key**".
   in this window you will have the API key.
5. Repeat step 4 to get second key for API Backend.

Next thing is to make sure that Google java API and Geolocation API for second key is turned on:

1. Go to https://console.cloud.google.com/home/dashboard
2. Menu in the top left corner (3 horizontal dashes) and select **APIs and services > Library**
3. Select Maps **JavaScript API**
4. If it's off, click on the switch
5. Do steps 3 and 4 for "**Geolocator API**"

If you have any questions regarding this topic, please let me know.

Best regards,
Mateusz Sałasiński
1st Line Customer Support
Tau Ceti sp. z o.o.
E: Mateusz.salasinski@tauceti.email
M: +48 510 275 903

Visualization of an example helpdesk response message