tamigo

Service Level Agreement (SLA)

01 System availability

System availability is measured in terms of uptime over one month. Uptime is measured by an independent third-party monitoring solution (Host Tracker) and is defined as "time during which the web services are available and respond to valid requests, excluding Permitted Downtime".

The guaranteed monthly uptime is 99.5%.

This uptime guarantee covers the following solution components:

- Main web application (app.tamigo.com)
- tamigo Touch (touch.tamigo.com)
- tamigo signin
- tamigo API

a Exceptions:

Permitted Downtime, caused by any of the following, is not included when measuring uptime:

1. General internet issues, including congestion or general DNS services not directly relating to tamigo or services provided by tamigo.

2. Force majeure events as described in the terms of agreement.

3. Actions or inactions of the Customer (unless undertaken at the express direction of tamigo) or third parties beyond the control of tamigo.
   Note: Subcontractors of tamigo are not considered a third party and tamigo takes full responsibility for subcontractors.

4. A result of Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of tamigo.

5. Scheduled infrastructure maintenance.

b Compensation:

Compensation is available to customers with a Professional, Premium or Enterprise package.
If the observed uptime is lower than the guaranteed one for a certain month, the Customer may request to be compensated with service credits which may be only used to pay for future invoices.
The service credits are calculated based on the table below:

Monthly uptime percentage	Monthly credit (% of monthly fee for the product)
Less than 99.5% but greater than or equal to 99%	10%
Less than 99% but greater than or equal to 95%	25%
Less than 95%	50%

To receive service credits, the Customer must submit a support request containing the claim within 15 days following the end of the calendar month in which the downtime occurred.

c Reporting:

tamigo automatically provides uptime information on its status page, but monthly overview of uptime for each application can be requested by the Customer.

02 Support availability

Support can be accessed by named individuals as agreed between tamigo and the Customer.

Support can be accessed in the following ways, unless agreed otherwise:

- Phone support, from 09:00 to 16:00 (CET/CEST), Monday to Friday.
- Email support, from 09:00 to 16:00 (CET/CEST), Monday to Friday.

03 Incident management

An operational incident is any unplanned interruption to, or reduction in the quality of, the tamigo service. Incidents are logged, classified by severity, and managed in accordance with tamigo's Incident Management procedures.

– Critical incident

Description: Complete service component outage – tamigo is inaccessible.
Response target: Immediate response, 24/7.
Resolution target: Continuous efforts until service is restored.

– Major incident

Description: Core functionality (i.e., exporting) is unavailable and without workaround.
Response target: Immediate response during business hours.
Resolution target: By default, 2 business days, but no more than 2 full weeks.

– Medium severity

Description: Degraded functionality impacting use of tamigo.
Response target: Within 24 hours during business hours.
Resolution target: Scheduled with the customer, typically the next development cycle

04 Backup & contingency plans

All data is backed up in three levels, making sure that substantial data loss is not possible.

1. For essential data, single entities are logged directly in the database in order to be able to restore accidentally deleted data or for revision tracking.

2. The complete servers, including OS, are backed up nightly, providing an extremely fast and dependable method of restoring normal operations in case of catastrophic partial failure.

3. In case of a catastrophic failure, i.e. flooding in the data centre or other factors causing severe hardware malfunction, rendering the main hosting centre inoperable, tamigo has remote nightly backups. These can be used to restore normal operations. tamigo has a secondary data centre, which can be used in case the primary data centre is not operational within reasonable time to meet our RTO of 12 hours.

Upon catastrophic failure, the upper maximum limit for data loss (RPO) is 24 hours. This is extremely unlikely. Procedures for catastrophic failure are simulated and tested annually.

tamigo

go get in touch

+45 70 27 93 30
support@tamigo.com

tamigo
Kristianiagade 8
2100 Copenhagen
Denmark

www.tamigo.com
VAT DK28277679