

API Terms

Publication date: 15.06.2026

Last updated: 18.06.2026

Rules for merchant access to the API, creation of payment requests, operation statuses and webhook notifications.

These terms govern use of the WHITECAPITAL API by merchants.

Access

API access is provided only after review, approval, signing of the agreement and technical setup.

Purpose of API

The API may be used for:

- creating payment requests;
- generating payment links;
- generating QR scenarios;
- receiving operation statuses;
- receiving webhook/callback notifications;
- operation reconciliation;
- report export.

Restrictions

The API may not be used for:

- unapproved websites;
- processing payments for third parties;
- prohibited goods or services;
- operations without an order;
- fraud;
- unauthorized access;
- circumvention of restrictions.

Security

The merchant must:

- keep API keys secure;
- restrict access to the API;
- notify WHITECAPITAL of key compromise;
- not transfer access to third parties;
- comply with technical instructions.

Operation statuses

The merchant must fulfil its obligation to the buyer only after receiving a confirmed successful operation status.

Suspension

WHITECAPITAL may suspend API access in case of suspicious activity, breach of agreement, key compromise, bank request or prohibited activity.