Roksnet Acceptable Use Policy (AUP)

Document code: AUP
Version: 1.1
Published: 4 November 2026
Effective date: 5 November 2026
Publisher: Roksnet Solutions OÜ

This Acceptable Use Policy ("AUP") sets out the rules for acceptable use of the Roksnet Self-Service Platform and the Roksnet Services offered through it. The AUP applies to all Customers and Members. For Members, the AUP forms part of the Agreement with Roksnet Solutions OÜ ("Roksnet"). For Customers (before conclusion of the Agreement, as defined in RGT §2.2), the AUP applies as the platform's terms of use during the application process and becomes part of the Agreement upon successful Identification.

This AUP applies in parallel with the Roksnet General Terms and Conditions (RGT) and the applicable Annexes. In case of conflict, the RGT and the relevant Annex prevail. Capitalised terms have the meanings set out in the Roksnet Terminology and Definitions (RTD), unless expressly stated otherwise.

1. Scope

This AUP applies to:

- the Roksnet Self-Service Platform (https://app.roksnet.com);
- all Roksnet Services activated through the Self-Service Platform;
- all communication and support channels operated by Roksnet.

Use of the public Roksnet website is governed by the Roksnet Site Terms (RST).

2. General principles

Customers and Members must use the Self-Service Platform and Roksnet Services:

- lawfully and in good faith;
- in accordance with the RGT, the applicable Annexes, and this AUP;
- consistently with the technical and operational instructions published by Roksnet.

3. Prohibited use

It is prohibited to:

- use the Self-Service Platform or any Service for unlawful, fraudulent, or harmful purposes;
- attempt to gain unauthorised access to Roksnet systems, accounts, data, or infrastructure;
- bypass or tamper with authentication, authorisation, or other security controls;
- introduce malware, harmful code, or any technology intended to damage or disrupt Roksnet systems or the systems of other Members;
- conduct denial-of-service activity, abusive scanning, or unauthorised automation against Roksnet Services;
- scrape, harvest, or aggregate data published in the Member Directory or any other Service for purposes other than lawful data exchange or the business inquiry and discovery purpose of the Member Directory;
- provide false, misleading, incomplete, or fraudulent information during registration, Identification, or use of the Self-Service Platform;
- impersonate any person, organisation, or system;

- use the Self-Service Platform, Member Directory data, or any communication channel for unsolicited messaging, spamming, or marketing without lawful basis;
- use Roksnet Services in violation of the rights of third parties, including intellectual property, privacy, and confidentiality rights;
- submit through Support channels data beyond what is strictly necessary for the support request;
- submit personal data of individual employees or other natural persons through the Public Profile section of the Self-Service Platform. The Public Profile is intended exclusively for organisational contact details of the legal entity (such as a general organisation email and phone). Personal contact details of individuals must not be entered in these fields.

4. Security obligations

The security obligations of Customers and Members are set out in full in RGT §8, including obligations covering credentials, end-user devices, network infrastructure, access management, monitoring, incident notification, Security Servers, and Trust Services key material. Service-specific security rules are set out in the applicable Annexes (Annex B for the Member Directory Service; Trust Services documentation for AUTH and SIGN certificates). This AUP does not restate those obligations; they apply in full to all use of the Self-Service Platform and Roksnet Services.

5. Reporting violations

Suspected violations of this AUP, suspected misuse of the Self-Service Platform, or security incidents should be reported to:

support@roksnet.com

6. Enforcement

Roksnet may, in case of violation of this AUP:

- issue a warning or request remediation;
- reject or cancel a Customer's application before conclusion of the Agreement;
- suspend access to the Self-Service Platform or to a specific Service;
- terminate the Framework Membership or the Membership in accordance with the RGT and the applicable Annex;
- take legal action where appropriate.

Where immediate suspension is necessary to address an active security incident or a serious violation, Roksnet may suspend access without prior notice and inform the Member as soon as reasonably possible thereafter.

7. Changes to this AUP

Roksnet may amend this AUP in accordance with the amendment procedure set out in the RGT. Material adverse changes will be communicated to Members at least 30 days before they take effect. Other changes take effect upon publication.

Contact
Roksnet Solutions OÜ
Email: support@roksnet.com