Last Updated: 12th March 2021

SureCloud – API Acceptable Usage Policy

This Acceptable Usage Policy (AUP) outlines appropriate usage of the SureCloud API service and any data retrieved by this service by SureCloud Users ("Users"). By using this service, Users agree to comply with all terms of this AUP.

As used in these Terms, "API" means programmatic web APIs and associated tools and documentation that SureCloud makes available to SureCloud customers and partners under these Terms.

We may amend, modify or substitute this AUP at any time. Any updates will become automatically effective for all Users. We recommend that Users visit the SureCloud Swagger API documentation portal regularly to check for any updates or amendments to this AUP.

This AUP governs the use of the SureCloud API service. This does not supersede any existing agreements already in place between SureCloud and the User.

1. Access to the API

Access to the API will be granted only to Users who have an active SureCloud subscription. On termination of the contract with SureCloud, the Users API access will also be terminated.

Users can request access to the API and associated documentation through SureCloud Technical Support or their Customer Success Manager. Users will be given access to a unique API secret key which in turn can be used to generate a API token required to authenticate to the APIs.

The API token enables us to associate User API activity with the User's SureCloud user account. All activities that occur using these Access Credentials are the User's responsibility.

2. Responsibility of the User

Responsibility

a) Users agree to use SureCloud's API Service in a manner that is legal, appropriate and in conformity with industry standards.
b) Users may not share API secret key or API token with any third party except as permitted by SureCloud for the use of the User's Service.
c) Users may not use the SureCloud API to distribute any virus, spyware, adware, malware, or other harmful or malicious component.
d) Users may not use the SureCloud API for any purpose which might overburden, impair or disrupt SureCloud Services or related services, servers or networks.
e) Users may not systematically crawl SureCloud API or Service.
f) Users must add appropriate information to API request headers which identifies the calling application. This information will be used to track usage and inform User of any odd usage patterns. Specifically include these fields:
    i. Application-Name (e.g. "App Name")
    ii. Application-Version (e.g. "1.2.5")
    iii. Application-OrgName (e.g. "SureCloud Org")
    You can find your SureCloud organisation name by logging into the SureCloud console and viewing the name that appears on the top toolbar (top right).

If Users breach any of the terms within this policy, SureCloud may immediately remove access to the API Service. SureCloud may also terminate or suspend access to User account.