Verkada

API Use Policy

This API Use Policy ("**Policy**") governs your access to and use of the Verkada Command application program interfaces ("**APIs**"). By accessing the APIs, you (1) confirm that you are a User (as defined in the End User Agreement ("**Agreement**") between Verkada Inc. ("Verkada") and your organization) authorized by your organization to use the APIs, and (2) agree to comply with this Policy. The APIs are considered a Product and this Policy forms part of the Documentation.

If you are not a User, you must separately obtain permission from Verkada to access and use the APIs. For the avoidance of doubt, this Policy does not apply to integration partners or their agents or contractors (collectively each, a "**Partner**") developing, testing, or demonstrating interoperability functionality between a Partner product and a Product offered by Verkada. Integration partners must enter into a separate agreement with Verkada that governs their access to and use of the APIs in connection with their activities.

1. Your organization's license to Command enables you to access and use the API, including through third-party integrations, in accordance with the Agreement. To use and access the API, you must obtain an API key (a "Key") from an organizational administrator. Once you receive a Key from an organizational administrator, you may not share the Key and must keep it secure. Your Key is the only means through which you are authorized to access the APIs.

2. In addition to complying with the restrictions on the use of Products set forth in the Agreement, you agree not to: (i) circumvent, or attempt to circumvent, any rate limits for the APIs ("**API Limits**") described in the documentation for the APIs and available at: https://apidocs.verkada.com/reference# ("**API Documentation**"), or otherwise engage in excessive or abusive usage of the APIs; (ii) use the APIs to access, or attempt to access, data or functionality other than as expressly allowed by the API Documentation; or (iii) access the APIs in any manner that (1) compromises, breaks, or circumvents any technical processes or security measures for the APIs, (2) poses a security vulnerability to other Verkada end customers or end users, or (3) tests the vulnerability of Verkada systems or networks. Each of (i) through (iii) are deemed to be a Prohibited Use.

3. If you run any application that uses or accesses the APIs to transmit Customer Data outside of Command, you acknowledge and agree that you, not Verkada, are responsible for the privacy, security, accuracy, or integrity of Customer Data once it is transmitted outside of Command. Verkada is not responsible for the performance, security, availability, accuracy, timeliness, validity, latency, or any other aspect of any third party application or system that uses the APIs, or their handling of any Customer Data, for any reason.

4. Data you submit to the APIs will be considered Customer Data. You warrant that neither the application that uses or accesses the APIs nor the data it transmits to Verkada will introduce or contain any viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs.

5. Verkada may monitor your use of the APIs for compliance with this Policy, and we may deny you access to the APIs if you violate this Policy. Verkada may modify, suspend, or discontinue the APIs, or any part thereof, at any time without prior notice.