Updated and effective as ofDecember 7, 2018

zingfit API Security Policy (the "Security Policy")

This Security Policy is incorporated into and made part of the terms of (i) the App Hosting Agreement between zingfit and Client, and (ii) the API Agreement between zingfit and any API User. Capitalized terms not defined in this Security Policy will have the meanings given to them in the Glossary, which is located at the following URL: http://www.zingfit.com/legal-docs/glossary-terms/.

1. Security Guidelines: API User's and Client's use of the API is contingent on API User's and Client's agreement to be bound by, and compliance with, the following security guidelines:

    (a) API User and Client shall not share login credentials, including API User's and Client's password, with any other person without the prior written consent of zingfit, except in the event that API User and Client reasonably believe that API User and Client need to share API User's and Client's password with a colleague who has a need-to-know such information. Under no circumstances will zingfit contact you to request your password, and any such contact must be immediately reported to zingfit. API User's and Client's password must be stored in a secure location, meaning that it should not be stored in any location accessible to other individuals, and should not be stored in an unencrypted format (including without limitation on websites which utilize unencrypted services, such as Pastebin).

    (b) Any access to the API using API User's and Client's login credentials shall be deemed to have been done by API User and Client. For this reason, API User and Client are responsible to ensure that reasonable steps are taken to protect the confidentiality of API User's and Client's login credentials and to prevent fraudulent use of this information. API User and Client shall contact zingfit immediately if you believe that an unauthorized third party is in possession of, has used or attempted to use, or intends to use, API User's and Client's login credentials to access the API.

    (c) API User and Client will not access, attempt to access, use, or attempt to use, the API in any way or for any reason other than as expressly permitted in the API Agreement.

    (d) zingfit reserves the right to suspend access to API User's and Client's account if it reasonably believes that API User and Client (or another individual on API User's and Client's behalf) has violated the terms of this Security Policy.

2. Modifications to Security Policy: zingfit may modify the terms of this Security Policy at any time, and for any reason, in its sole and absolute discretion. Any modifications to the terms of this Security Policy shall become effective on the thirtieth (30^{th}) day following the posting of the modified Security Policy to zingfit's website. API User and Client may cease using the API, or terminate API User's and Client's account, before any such changes become effective if API User and Client do not agree to be bound by the terms of the modified Security Policy following the implementation of such modifications.