

The use of the Artesian Service is subject to the following terms and conditions of use:

User Conduct

You must not use any Artesian software application, including website, API or mobile (i.e. phone and tablet) in any way that causes, or is likely to cause, that application or access to it to be interrupted, damaged or impaired in any way;

Users may download and view company data within limits which are considered reasonable for business use. For avoidance of doubt, reasonable business use is defined as a user adding up to 400 new companies per day, or downloading up to 20,000 companies per day through the Artesian Prospector module. These thresholds may be temporarily exceeded following written agreement from a director of Artesian Solutions.

You must ensure that any content you upload to Artesian owned or administered servers or associated infrastructure (including photographs) is not obscene, offensive, defamatory or racist and does not breach any law or regulation or any intellectual property rights of a third party or any right or duty owed to a third party. This means that if any of the content you upload is copyright protected, you must obtain the copyright owner's written permission in order to use it;

In the event that you become aware of any content which breaches any of the above rules, please notify us immediately by emailing info@artesian.co;

You must not attempt to modify, adapt, translate, sell, reverse engineer, decompile or disassemble any portion of Artesian software or the Artesian service, including but is not limited to, the application website, APIs, mobile applications or any associated client installed applications provided by Artesian.

You must not attempt to bypass the network firewall;

You must not use any part of any provided application or application interface which you are not authorised to use or devise ways to circumvent security in order to access part of the Artesian platform, including but is not limited to the application website, API's, mobile applications or client installed applications which you are not authorised to access. This includes but is not limited to scanning networks with the intent to breach and/or evaluate security, whether or not the intrusion results in access.