Qlik Cloud Acceptable Use Policy

This Qlik Cloud® Acceptable Use Policy ("AUP") defines acceptable practices and prohibited uses relating to Qlik's network and systems that are used for hosting Qlik products and services or providing SaaS services (collectively, the "Services") by users ("You" or "Your"). The Services must be used in a manner consistent with the intended purpose of the Services, the terms of Your applicable agreement with Qlik for the products and/or services being hosted, and this AUP. Qlik may modify this AUP by posting a revised version to www.qlik.com. By using the Services, You agree to the latest version of this AUP. For purposes of this AUP, "Qlik" includes QlikTech International AB and its affiliates, and Qlik may be referred to as "We" or "Our."

A. Security

1. You agree to maintain appropriate security, protection and backup copies of any content that is included, transmitted, stored, published, displayed, distributed, integrated, or linked by You in the Services (collectively, "Content"). We will have no liability of any kind as a result of the deletion of, correction of, destruction of, damage to, loss of or failure to store or backup any Content.

2. You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

    i. Unauthorized Access. Bypassing, circumventing, or attempting to bypass or circumvent any measures We may use to prevent or restrict access to the Services (or other accounts, computer systems or networks connected to the Services), including any attempt to probe, scan, or test the vulnerability of the Services or to breach any security or authentication measures used by the Services.
    ii. Reverse Engineering. Deciphering, decompiling, disassembling, reverse engineering or otherwise attempting to derive any source code or underlying ideas or algorithms of any part of the Services, except to the limited extent applicable laws specifically prohibit such restriction.
    iii. Falsification of Origin or Identity. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route, or attempting to impersonate any of Our employees or representatives.
    iv. Using manual or automated software, robotic process automation, devices, or other processes to harvest or scrape any content from the Services.
    v. Denial of Service (DoS)/Intentional Interference. Flooding a System with communications requests so the System either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective, or interfering with the proper functioning of any System, including by deliberate attempts to overload the System.

B. Your Responsibilities

1. **No Illegal, Harmful or Offensive Use or Content.** You may not use, or encourage, promote, facilitate or instruct others to use, the Services for any illegal (under applicable law), fraudulent, infringing or offensive use, or to transmit, store, display, distribute, post or otherwise make available content that is illegal (under applicable law), harmful, fraudulent, infringing or offensive. Prohibited activities or content include:

    i. Illegal, Harmful or Fraudulent Activities. Any activities that are illegal, that violate the rights of others, that may be harmful to others, or that may be harmful to Our operations or reputation.

ii. Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others or that violates any law or contractual duty.
iii. Offensive Content. Content that is illegal, harassing, libellous, fraudulent, defamatory, obscene, pornographic, abusive, invasive of privacy, or otherwise objectionable.
iv. Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept or disrupt the Service, including viruses, Trojan horses, spyware, worms, time bombs, or cancelbots.
v. Unsolicited Content. Content that constitutes unauthorized or unsolicited advertising, junk or bulk e-mail ("spamming") or contains software viruses or any other computer codes, files or programs that are designed or intended to disrupt, damage, limit or interfere with the proper function of any software, hardware, or AUP March 2021 telecommunications equipment or to damage or obtain unauthorized access to any system, data, password, or other information of Ours or any third party.
vi. Competitive Content. Attempting to collect and/or publish performance data for the purposes of benchmarking, or developing a product that is competitive with any Our product or services.
vii. Violence or Incitement. Actions that directly or indirectly threaten, encourage, or incite violence against anyone, or promote harm, hatred, or abuse.

2. **Use of Generative AI**. It is Your responsibility to review and verify the output of any Qlik Product or Service using generative artificial intelligence ("AI Output") before using or sharing it, and to evaluate whether use of AI Output is appropriate for Your particular use case and complies with applicable laws.

3. **Generated Code and Talend Open Studio**. Generated Code refers to an independently executable program or binary code generated by the Services. Generated Code may only be used with Qlik Products under a current subscription. You may not (i) use Talend Open Studio (or other free open source software) to process or utilize Generated Code; or (ii) use the Services to process unsupported code generated from Talend Open Studio.

4. **Reporting**. If You become aware of any violation of this AUP, You will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. Violation of this AUP may be reported to security@qlik.com.

C. Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to monitor for, and investigate, any violation of this AUP or other misuse of the Services. Failure to comply with this AUP constitutes a material breach of the terms and conditions upon which You are permitted to use the Services, and at any time may result in Qlik taking any and all remedial actions in its sole discretion, up to and including:

i. Warnings;
ii. Suspending or terminating access to the Services;
iii. Removing, disabling or prohibiting access to content that violates this AUP and/or Your applicable agreement with Qlik; and/or
iv. Legal proceedings against You.

We may report any activity that We suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

We take no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. We are not obligated to monitor such material, but reserve the right to do so, as well as remove any content that We, in Our sole discretion, determine to be in violation of this AUP.

D. Subdomains

If You are permitted to choose a Qlik subdomain name for use with Qlik Cloud, such subdomain name may not infringe or violate third-party intellectual property rights or include offensive, obscene, vulgar or other objectionable or unlawful language, and be unique enough to prevent confusion with other entities, brands or trademarks. We reserve the right (but shall have not obligation to) to monitor, reject, revoke or cancel any Qlik subdomain name that is not in compliance with this Policy or any applicable laws.