

Qlik Hosted Services Acceptable Use Policy

This Hosted Services 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 and the terms of Your applicable agreement with Qlik for the products and/or services being hosted. By using the Services, You consent to be bound by the terms of this AUP. We may modify this AUP at any time by posting a revised version on the Qlik website under Legal Policies at 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."

Security

- 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"), which may include your use of additional encryption technology to protect the Content from unauthorized access. 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 encrypt any Content.
- You may not take any action that imposes or may impose (as determined in Our sole discretion) an unreasonable or disproportionately large load on Our (or Our third-party providers') infrastructure.
- 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:
 - Unauthorized Access. Bypassing, circumventing, or attempting to bypass or circumvent any measures Qlik 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.
 - 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.
 - 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.
 - Using manual or automated software, devices, or other processes to harvest or scrape any content from the Services.

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, harmful, fraudulent, infringing or offensive use, or to transmit, store, display, distribute, post or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include:

- 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 Qlik's operations or reputation.
- Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others or that violates any law or contractual duty.
- Offensive Content. Content that is illegal, harassing, libelous, fraudulent, defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable.
 - 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.
 - 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 telecommunications equipment or to damage or obtain unauthorized access to any system, data, password, or other information of ours or any third party.

- Competitive Content. Attempting to collect and/or publish performance data for the purposes of benchmarking, or developing a product that is competitive with any Qlik product or services.

Our 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, with immediate effect:

- Warnings;
- Suspending or terminating access to the Services;
- Removing, disabling or prohibiting access to content that violates this AUP and/or your applicable agreement with Qlik; and/or
- 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.

Qlik takes no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. Qlik is not obligated to monitor such material, but reserves 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.

Reporting of Violations of this Policy

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.