



IVANTI ACCEPTABLE USE POLICY

This Ivanti Acceptable Use Policy (this “**Policy**”) describes prohibited uses of the cloud-based services offered by Ivanti (the “**SaaS Offerings**”) to you (a “**Customer**”). The examples described in this Policy are not exhaustive. Ivanti may modify this Policy at any time by posting a revised version. By accessing or using the SaaS Offerings, Customer agrees to the latest version of this Policy. If Customer violates the Policy or authorizes or helps others to do so, Ivanti may suspend or terminate Customer’s use of the SaaS Offerings.

No Illegal, Harmful, or Offensive Use or Content

Customer may not access, use, or authorize, encourage, promote, facilitate or help others to use, the SaaS Offerings for any illegal, harmful, fraudulent, infringing or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include any activities that are illegal, that violate the rights of others, or that can be harmful to others, or Ivanti’s operations or reputation; content that infringes or misappropriates the intellectual property or proprietary rights of others; content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable; or content or other computer technology that can damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, spyware or cancelbots. Further, Customer shall not use the SaaS Offering to: (i) harvest, collect, gather or assemble information or data regarding other users without their consent; (ii) attempt to gain unauthorized access to the SaaS Offering, computer systems or networks related to the SaaS Offering; or (iii) interfere with another customer’s use and enjoyment of the SaaS Offering.

No Security Violations

Customer may not use the SaaS Offerings 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 accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System; monitoring of data or traffic on a System without authorization; or forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision. Customer will use commercially reasonable efforts to prevent unauthorized access to, or use of, the SaaS Offering, and notify Ivanti promptly of any such unauthorized use known to Customer. If Customer provides access to the SaaS Offering to any third party, then Customer agrees Ivanti shall not be responsible or have any liability for a data breach resulting from such third party access.

No Network Abuse

Customer may not make network connections to any users, hosts, or networks unless Customer has permission to communicate with them. Prohibited activities include monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled; inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective; interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques; operating network services like open proxies, open mail relays, or open recursive domain name servers; or using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions, or to avoid incurring fees.

No E-Mail or Other Message Abuse

Customer must not access or use the SaaS Offerings to distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”), including commercial advertising and informational announcements. Customer will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. Customer will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

Ivanti’s Monitoring and Enforcement & Violations of this Policy

Ivanti reserves the right, but does not assume the obligation, to investigate any violation of this Policy or misuse of the SaaS Offerings. Ivanti may investigate violations of this Policy or misuse of the SaaS Offerings; or remove, disable access to, or modify any content or resource that violates this Policy or any other agreement Ivanti has with Customer for use of the SaaS Offerings.

Ivanti may report any activity that Ivanti suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Ivanti’s reporting may include disclosing appropriate Customer information or content. Ivanti 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 Policy.

If Customer becomes aware of any violation of this Policy, Customer must immediately notify us and provide Ivanti with assistance, as requested, to stop or remedy the violation.