



Acceptable Use Policy

Summary

This policy sets forth general and specific information regarding the use of the infrastructure of Segra's Data Centers. Customers, a.k.a. client(s) of Segra's Data Centers are prohibited from transmitting over any of Segra's Data Centers's services any material that Segra's Data Centers deems to be unlawful, obscene, threatening, abusive, defamatory, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state or federal laws. Segra's Data Centers reserves the right to use its sole discretion to make the determination of what material falls under this prohibited material, and further reserves the right to modify this document at any given time. All Segra's Data Centers clients are responsible for making themselves and their employees familiar with the information contain herein.

Segra's Data Centers's services are designed to be utilized for lawful purposes only. Any storage of information, distribution of information, transmission, of any material or data that is in violation of common law, state law, or United States Federal law or regulation on any level is strictly prohibited. Materials protected by trademark, trade secret, copyright, or any other statute are included in the list of prohibited materials, as well as other materials not listed here. As a result of identifying such material, Segra's Data Centers reserves the right to immediately terminate any client's services and remove the material in question. The client in violation may also be subject to criminal or civil liability.

Accurate Information/Notification

Clients of Segra's Data Centers are responsible for providing Segra's Data Centers with accurate information regarding their billing data, and updating that information whenever a change occurs. Segra's Data Centers will utilize a client's information to notify them of any issues that may arise during the lifetime of their contract with Segra's Data Centers. Supplying inaccurate or false information on any application or contract is grounds for immediate termination, and may also result in criminal or civil liability. This may include penalties for fraudulent credit card information.

Client is responsible for administering proper use of their account with Segra's Data Centers. Regardless of the actual person(s) that conduct inappropriate behavior, the responsibility of prudent behavior lies directly with the owner of the account. Segra's Data Centers reserves the right to terminate the contract of any client that it deems to be engaging in any activity that is inappropriate.

Email

Segra's Data Centers strictly adheres to the Digital Millennium Copyright Act (DCMA) 17 USC § 512. Any violation of this act will result in a client notification requiring the client to take immediate action. If the client does not respond in a timely manner the material in question will be blocked or filtered. Segra's Data Centers may also suspend a client's access or privileges until the client addresses the concern regarding the material in question. Client abuse or misuse of electronic mail (email) may result in the termination of service with Segra's Data Centers.

Acts that fall under the category of email abuse include:

- Unsolicited bulk email (UBE) or unsolicited commercial email messages; also known as "spam"
- Using a third party to send out unsolicited email (commercial or bulk); also known as "spamvertising"
- Removal, forgery, or alteration of electronic mail headers
- Sending huge volumes of email (or enormous files) to an address in an attempt to overflow the mailbox or overwhelm a server resulting in a "denial of service" attack; also known as mailbombing
- Use email that can be deemed as harassing or intimidating to others.
- Any bulk email that is not compliant with the "CAN-SPAM" Act; which directly and clearly addresses guidelines for the delivery of email from businesses.
- Being identified on the list of "Register Of Known Spam Operations" (ROKSO) database at www.spamhaus.org/rokso/
- Operating in any manner with any relation to any company or anyone listed in the ROKSO database
- Sending bulk email to any recipient that has not chosen to opt-in. (All bulk email must be opt-in and the client must retain details of the date and time an email address opted-in, along with the IP address they opted-in from. Upon request these details must be made available to Segra's Data Centers. Segra's Data Centers reserves the right to inspect the confirmation email headers from recipients that "opt-in" to ensure that they are authentic. Any campaign that is found to be using third party lists where "opt-in" confirmations are not found to be authentic will be suspended.)
- Clients are required to configure any email server that leverages Segra's Data Centers's services so that it will not accept any third party emails that can be forwarded.
- Infrastructure in this regard will consist of, but not be limited to, bandwidth, transport, servers, switches, IP address and any other equipment that will transmit, receive or otherwise be a vehicle of transmission of data of any sort.



Use Prohibited

Child Pornography

Federal law 18 U.S.C. §§ 2256 defines child pornography as any visual depiction, including any photograph, film, video, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct of anyone under the age of 18. Federal child exploitation statutes clearly state that the production, reception, transportation, possession, or distribution of any sexually explicit depiction of children is illegal.

Clients found to be in violation of this law will immediately have their service suspended until clarifications have been made to prove that the material is not in violation of the law. Segra's Data Centers reserves the right to terminate any client that it deems to be in direct violation of the law, or anyone that it deems to be repeatedly under scrutiny for possible violations of the law.

Illegal Activity

Any activity that is deemed to be in violation of any state or federal law that occurs on Segra's Data Centers's network is in violation of this policy and will result in swift termination of services from Segra's Data Centers. Clients may not store or transmit/retransmit any materials in violation of any laws or regulations.

Clients are prohibited from using Segra's Data Centers's services for any illegal activities including but not limited to phishing, network DoS or DDoS, hacking, virus distribution, spamming, marketing pyramid schemes, and any and all other illegal activities denoted by federal, state, or local laws. Segra's Data Centers reserves the right to terminate any client it deems to be engaged in such activities.

Segra's Data Centers will also not tolerate any abuse of Segra's Data Centers's network resources by any customer that negatively affects other Segra's Data Centers clients. Deliberate impairment and reckless use of network resources is prohibited and is grounds for termination of services by Segra's Data Centers. Any client that is unsure about what activities constitute a "misuse of resources" should contact Segra's Data Centers before engaging in the task in question. Segra's Data Centers will provide information to the client regarding prohibited use.

Clients will be held accountable for, and are responsible for properly establishing a secure configuration for services through Segra's Data Centers. Client may be held liable for any damages that result from their negligence, exposure, or vulnerabilities regardless of whether their actions are deemed intentional or not.

Release of Liability

Client is responsible for any and all information that is communicated using any and all formats of Segra's Data Centers's services. Segra's Data Centers does not routinely monitor website content, but may remove content if repeated complaints alert Segra's Data Centers to content that it deems objectionable. Segra's Data Centers reserves the right to use its sole discretion to determine if the material in question is objectionable. Objectionable material may include but is not limited to certain language, graphics, or other content.

Due to Segra's Data Centers's desire to maintain a positive reputation and protect its branding and image, Segra's Data Centers reserves the right to terminate a client's service as a result of any complaint lodged against a client that it deems to be acting in a manner that is unlawful, indecent, or objectionable including but not limited to descriptions, illustrations, images, logos, video and audio recordings, graphics, drawings, and executable programs.

Any violation of this AUP is strictly prohibited, and any failure of Segra's Data Centers to identify any violation of this AUP does not constitute a waiver of Segra's Data Centers's rights.

Hold Liable

All users that violate Segra's Data Centers's AUP or any provision of this policy may be held liable and possibly incur fees (including attorney's fees and other legal fees) for expenses incurred by Segra's Data Centers in defending itself from third party claims relating to any website content; regardless of who created the content on the client's website. Client may also incur fees for expenses incurred by Segra's Data Centers as a result of Segra's Data Centers remedying itself from damages it sustains as a result of client activities. These fees will be commensurate with the violation's severity.