Globalgig Acceptable Use Policy (AUP)

globalgig
Orchestrating Hyperconnectivity

GLOBALGIG's goal is to provide its clients with the best commercial Internet service possible. To accomplish this, GLOBALGIG has adopted this Acceptable Use Policy (the "Policy"). This Policy outlines acceptable use of GLOBALGIG's network. All GLOBALGIG clients and all others who use the Service (the "client", "user", "you", or "your") must comply with this Policy. If your business or organization does not agree to comply with this Policy, it must immediately stop all use of the Service and notify GLOBALGIG, so that it can close your account.

GLOBALGIG's clients who provide services to end users are responsible for such end users compliance with the terms of this AUP and must take steps to ensure compliance by their users. By using or accessing GLOBALGIG's services, Clients agree to be bound by the terms of the AUP.

GLOBALGIG reserves the right to modify, the Policy at any time, effective upon posting at https://www.globalgig.com. Clients are responsible for monitoring this website for changes. Use of GLOBALGIG's Services after changes to the AUP are posted on the website shall be deemed to constitute Clients' acceptance of such new or additional terms of the AUP.

1. ILLEGAL USE

The GLOBALGIG network may be used only for lawful purposes. Transmission, distribution or storage of any materials in violation of any applicable law or regulation is prohibited. This includes, without limitation:

- Material protected by copyright, trademark, trade secret, software piracy, patents or other intellectual property right without proper authorization.
- Engaging in activity that violates privacy, publicity or other personal rights of others.
- Material that is obscene, abusive, defamatory, harassing, or threatening language constituting an illegal threat or violates export control laws.
- Exploitation of vulnerabilities in hardware or software for malicious purposes such as exploitation of scripts presented on web pages (i.e., forms for answering questions or entering data).

2. SYSTEM AND NETWORK SECURITY

Violations of system or network security are prohibited, and may result in criminal and civil liability. GLOBALGIG will investigate incidents involving such violations and may involve and will cooperate with law enforcement, if a criminal violation is suspected.

Examples of system or network violations include, without limitation the following:

- Unauthorized access to or use of computers, data, systems, accounts or networks, including any attempt to probe, scan, or test the vulnerability of a

system or network or an attempt to penetrate security measures of another individual's system (known as 'hacking') is prohibited.

- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mail-bombing, flood, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting or otherwise engaging in any monitoring or interception of data not intended for the User without authorization is prohibited.
- Engaging in or permitting any network or hosting activity that results in the blacklisting or other blockage of GLOBALGIG IP space is prohibited.
- Also, attempting to circumvent Client authentication or security of any hosts, network, or account ('cracking') without authorization is prohibited.
- Simulating communications ("phishing") from and/or to a website or other service of another entity in order to collect identity information, authentication credentials, or other information from the legitimate users of that entity's service is prohibited.
- Exporting encryption software over the Internet or otherwise in violation of ITAR, to points outside the United States is prohibited.
- Using malware, DNS cache poisoning or other means ("pharming") to redirect a user to a website or other service that simulates a service offered by a legitimate entity in order to collect identity information, authentication credentials, or other information from the legitimate users of that entity's service is prohibited.
- Activities that disrupt the use of or interfere with the ability of others to effectively use the GLOBALGIG network, system, service, or equipment by utilizing programs, scripts, or commands to abuse a website (i.e., DDOS, SYN Floods or similar attacks).

3. EMAIL

Sending unsolicited mail messages is prohibited, including without limitation,

a. Client is prohibited from sending unsolicited bulk and/or commercial messages over the Internet ('spamming'). This includes receiving replies from unsolicited emails, (i.e., 'drop-box' accounts) or configuring any email server in such a way that it will accept third party emails for forwarding (i.e., open mail relay). Bulk email may only be sent to recipients who have expressly requested receipt of such email messages through a 'verified opt-in' process. Users that send bulk email messages must maintain complete and accurate records of all email subscription requested, specifically including the email and associated headers sent by every subscriber, and shall immediately provide GLOBALGIG with such

records upon request. If a site has roaming users who wish to use a common mail server, the mail server must be configured to require user identification and authorization.

b. The Service must not be used to:
    i. Send messages to any individual or entity who has indicated that they do not wish to receive a message from you.
    ii. Collect or redirect responses from unsolicited messages sent from accounts on another Internet hosts or messaging services which violates this policy, or the equivalent policy or any other policy of any other Internet service provider or website. Moreover, unsolicited messages sent from accounts on other Internet hosts or messaging services may not direct the recipient to any website or other resource that uses GLOBALGIG's network.
    iii. Purchase lists of email addresses from third parties for mailing to or from any GLOBALGIG hosted domain, or referencing GLOBALGIG account, is prohibited.
    iv. Distribute Internet Viruses, Worms, Trojan Horses, flooding, mail bombing, or denial of service attacks or distributing information regarding the creation of such viruses, worms, etc. for reasons other than mitigation or prevention is prohibited. Also, activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service or equipment is prohibited. Transmitting, distributing or storing information or material, that, as reasonably determined by GLOBALGIG, is threatening, abusive, violates the privacy of others or which violates any applicable law or regulation, that is harmful to or interferes with GLOBALGIG's provision of Service, the GLOBALGIG network or any third party's network, equipment, applications, services or websites, that is fraudulent or contains false, deceptive or misleading statements, claims or representations (i.e., phishing), and deceptive marketing practices including, without limitation to, practices that violated United States Federal Trade Commission's guidelines for proper online marketing schemes is prohibited.

4. SENDING HIGH VOLUME OF TRAFFIC TO PARTICULAR AUTONOMOUS SYSTEM

If the traffic to and from a particular ASN exceeds 10% of client's monthly Committed Data Rate (CDR) then GLOBALGIG makes no guarantee of performance towards packet loss and/or latency to and from that ASN.

The above is also applicable to "Transit" Autonomous systems which are used to reach the end user destinations

5. OBSCENE SPEECH OR MATERIAL

Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. Using GLOBALGIG's network to advertise, transmit, store, post, display or otherwise make available child pornography or obscene speech or materials is prohibited. GLOBALGIG does not prohibit any material allowed by law. GLOBALGIG is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through GLOBALGIG's network.

6. RISKS OF THE INTERNET

a. Some activities that clients can perform when accessing the Internet may be harmful or cause loss to client, other people that may access client's service, or client's equipment including, without limitation:
    i. Downloading content (including receiving emails) from the Internet which may introduce viruses or other harmful features to the client's computer,
    ii. Purchase goods or services using the Internet
    iii. Transmitting confidential information over the Internet (such as credit card numbers or other business information), or
    iv. Accessing and viewing content on the Internet or otherwise available through the service that may be offensive to some individuals, or inappropriate for children.

b. Client shall bear all risk associated with the activities referred to in paragraph (a) above and GLOBALGIG does not have any liability for any claims, losses, actions, damages, suites or proceeding arising out of or otherwise relating to such activities.

c. Client may minimize the risk of accessing illegal or offensive content as well as managing use of the Internet by using a filtering solution. GLOBALGIG does not provide these filtering solutions as part of the Service and it is the client's responsibility to implement these measures.

7. ADDITIONAL TERMS AND CONDITIONS

The use of the GLOBALGIG network by a Client is subject to the terms and conditions of any agreements entered into by such Client with GLOBALGIG. This AUP is incorporated into such agreements by reference.

8. COMPLAINTS/VIOLATIONS OF AUP

Any complaints regarding prohibited use of other abuse of the GLOBALGIG Network, including violations of this AUP, should be sent to mailto:AUP@globalgig.com. Please include all applicable information that will assist GLOBALGIG in investigating the compliant.