Global[X]Digital Acceptable Use Policy

Last updated May 12, 2022

INTRODUCTION

This acceptable use policy (the "Policy") defines acceptable practices for the use of Global[x]Digital a/k/a Reno East LLC's ("GXD") hosting services, web site access, utilities, and other services as may be provided from time to time (the "Services"). "GXD Network" includes, without limitation, GXD'x constructed or leased transmission network, including all equipment, systems, facilities, services and products incorporated or used in such transmission network. You agree that this Policy is a legally binding agreement between you ("User", "you" or "your") and GXD, that this Policy is contractual in nature, and that by your continued use of the Services you agree to be governed by the Policy.

Prohibited uses

- You may use our Services only for lawful purposes. You may not use our Services to engage in activity that is illegal under applicable law, that is harmful to others, or that would subject GXD to liability, including, without limitation, in connection with any of the following, each of which is prohibited under this Policy:
    - To breach or violate any applicable local, national or international law or regulation.
    - To undertake any act that is unlawful or fraudulent, or has any unlawful or fraudulent purpose or effect, or in any way that promotes, or encourages illegal conduct or activities, including the dissemination of content that has been determined by a court of competent jurisdiction to be unlawful.
    - For the purpose of harming or attempting to harm any third party.
    - To send, knowingly receive, upload, download, use or re-use any material which does not comply with our content standards.
    - To transmit, or procure the sending of, any unsolicited or unauthorized advertising or promotional material or any other form of similar solicitation (spam).
    - To knowingly transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other malware, malicious code, harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.
    - To transmit, store, or facilitate the transmission or storage of any illegal, immoral, obscene, or objectionable materials, including pornography, adult related content, promoting or facilitating prostitution or escort services, hosting, distributing or linking to child exploitation material.
    - To disclose sensitive personal information or personally identifiable information about others.
    - To collect or to attempt to collect, personal information about third parties without their knowledge or consent
    - To promote or facilitate gambling, violence, terrorist activities or selling weapons or ammunition.
    - To engage in the unlawful distribution of controlled substances, drug contraband or prescription medications.

- To manage payment aggregators or facilitators such as processing payments on behalf of other business or charities.
- To facilitate pyramid schemes, FOREX, E-Gold Exchange, Second Life/Linden Exchange, Ponzi, MLM/Pyramid Scheme, High-Yield Interest Programs (HYIP) or related or other similar financial schemes.
- To threaten harm to persons or property or to conduct otherwise harassing behavior.
- To conduct manual or automatic credit card or other available payment methods testing using bots or scripts.
- To misrepresent or fraudulently represent products or services.
- To infringe the intellectual property or other proprietary rights of others.
- To attack, exploit, or manipulate any other computer system or code.
- To engage in any activity which requires licensure, permit, or other governmental approval or clearance without requisite license, permit or approval.
- To host or connect to any anonymous proxy server.
- To Infringe upon the Intellectual Property Rights of Others. This includes, but is not limited to, the unauthorized copying or distribution of movies, music, books, photographs, software/warez, or any other copyrighted work. Money laundering.
- To engage in phishing, pharming or other activities related to identity theft.
- To host or access any cite on the "dark web" that traffics or allows the purchase and sale of illegal substances, illegal acts, weapons or ammunition.
- To engage in any conduct that would harm GXD's reputation, other GXD users or GXD or other GXD Customers' operations.
- To deceptively impersonate another person or entity, including any spoofing.
- To violate any other person's property rights, including to use the Services in a manner that violates, infringes on or misappropriates the intellectual property or proprietary rights of any third party, including without limitation any rights in or to copyright, patent, trademark, trade secret, privacy or publicity, and publishing content intended to assist others in unlawfully circumventing technical measures intended to protect any such rights.
- To distribute or host any content that incites or threatens violence against any person, promotes terrorism, is intended to harass, abuse or invade the privacy of any individual, creates a risk to the physical safety or health of any individual or to public safety or health, or that threatens or encourages harm on the basis of race, ethnicity, national origin, religion, caste, sexual orientation, sex, gender, gender identity, serious disease or disability, or immigration status.
- To facilitate, aide, abet, or encourage any of the above activities through the Services.

You also agree:

- Not to reproduce, duplicate, copy or re-sell any part of our sites or any material provided with the delivery of Services in contravention of the provisions of our terms of website use or any other agreement.
- Not to access without authority, interfere with, damage, or disrupt:
    - any equipment or network on which our Services are stored or through which our Services are provided;
    - any software used in the provision of our Services; or
    - any equipment or network or software owned, controlled, leased, or used by any third party.

System Abuse

Any User in violation of the Services security is subject to criminal and civil liability, as well as immediate account termination. Examples of such violations include, but are not limited to the following:

- Use or distribution of tools designed for compromising security of this website and the Services.
- Intentionally or negligently transmitting files containing any malware, including any computer virus or corrupted data.
- Accessing another network without permission, including to probe or scan for vulnerabilities or breach security or authentication measures.
- Unauthorized scanning or monitoring of data on any network or system without proper authorization of the owner of the system or network.
- Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled, or other harvesting or scraping of any content of the Services.
- Introducing intentionally, knowingly or recklessly, any virus or other contaminating code into the Service, or collecting, transmitting, or using information, including email addresses, screen names or other identifiers, by deceit or covert means (such as phishing, spearphishing, Internet scamming, password robbery, spidering, and harvesting).
- Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, flooding techniques, or conducting a denial of service ("DoS") attack.
- Operating open proxies, open mail relays, open recursive domain name servers, Tor exit nodes, or other similar network services.
- Using manual or electronic means to avoid any use limitations placed on a System, such as access limits and storage restrictions.
- Any conduct that is likely to result in retaliation against GXD, including the Services, or GXD employees, officers or other agents, including engaging in behavior that results in any GXD server being the target of a DoS attack.
- Any activity intended to withhold or cloak identity or contact information, including the omission, deletion, forgery or misreporting of any transmission or identification information, such as return mailing and IP addresses.

Service resources

You may not consume excessive amounts of the resources of the Services or use the Services in any way which results in performance issues, or which interrupts the availability or delivery of Services for other Users. Prohibited activities that contribute to excessive use, include without limitation:

- Deliberate attempts to overload the Services and GXD resources, and broadcast attacks (i.e. denial of service attacks).
- Engaging in any other activities that degrade the usability and performance of the Services.
- Vulnerability testing, including attempts to probe, scan, penetrate, or test the vulnerability of any GXD system or network, or to breach the GXD security or authentication measures, whether by passive or intrusive techniques, or conduct any security or malware research on or using the Services, without GXD's prior written consent.

- Excessive Use of Shared System Resources, including the use of Services in a way that unnecessarily interferes with the normal operation of the Services, or that consumes a disproportionate share of the resources of Services. For example, we may require you to repair coding abnormalities in your cloud-hosted code if it unnecessarily conflicts with other customers' use of the Services. You agree that we may quarantine or delete any data stored on a shared System if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the System or other customers' data that is stored on the same system.

No spam policy

You may not use the Services to send spam or bulk unsolicited messages. We maintain a zero tolerance policy for use of the Services in any manner associated with the transmission, distribution or delivery of any bulk e-mail, including unsolicited bulk or unsolicited commercial e-mail, or the sending, assisting, or commissioning the transmission of commercial e-mail that does not comply with the U.S. CAN-SPAM Act of 2003 ("SPAM"). Your products or services advertised via SPAM (i.e. Spamvertised) may not be used in conjunction with the Services. This provision includes, but is not limited to, SPAM sent via fax, phone, postal mail, email, instant messaging, or newsgroups. Sending emails through the Services to purchased email lists ("safe lists") will be treated as SPAM.

Copyright

Copyrighted material must not be published via the Website and Services without the explicit permission of the copyright owner or a person explicitly authorized to give such permission by the copyright owner. Upon receipt of a claim for copyright infringement, or a notice of such violation, we may, at our discretion, investigate and, upon confirmation, may remove the infringing material from the Services. We may terminate the Service of Users with repeated copyright infringements. Further procedures may be carried out if necessary. We will assume no liability to any User of the Services for the removal of any such material.

Security

Users are fully responsible to maintain reasonable security practices including reasonable operational security and to protect and update any login information that may be provided to access or monitor the Services.

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:

- Harmful Software. Content, software, or any other technology that may damage, interfere with, surreptitiously intercept, or expropriate any computer system, program, or data, including any viruses, malware, spyware, adware, Trojan horses, worms, or time bombs.
- Unauthorized Access. 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.

- Interception. Monitoring of data or traffic on a System without permission.
- Falsification of Origin. Using fake or misleading TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route.
- Installation of cellular or wireless equipment/antennae on the GXD premises without prior written permission from GXD. Customer is responsible to pay GXD's reasonable expenses (including labor) to remove unauthorized equipment installed in violation of this policy.

Suspension and termination

We will determine, in our discretion, whether there has been a breach of this Policy through your use of our Services. Our right to suspend or terminate your use of the Services applies even if a violation is committed unintentionally or without your authorization. When a breach of this Policy has occurred, we may take such action as we deem appropriate.

- Failure to comply with this acceptable use policy constitutes a material breach of the terms of use upon which you are permitted to use our sites, and may result in our taking all or any of the following actions:
    - Immediate, temporary or permanent withdrawal of your right to use or receive our Services.
    - Immediate, temporary or permanent removal of any posting or material uploaded by you to our sites.
    - Interference with or blocking of your access to Services.
    - Issue of a warning to you.
    - Legal proceedings against you for reimbursement of all costs on an indemnity basis (including, but not limited to, reasonable administrative and legal costs) resulting from the breach.
    - Further legal action against you.
    - Disclosure of such information to law enforcement authorities as may be reasonably necessary.
- We exclude liability for actions taken in response to breaches of this acceptable use policy. The responses described in this policy are not limited, and we may take any other action we reasonably deem appropriate.

Changes to the Policy

- We may revise this Policy at any time by amending this page. The date of last update to this Policy is noted at the top of this webpage. We may also provide notice to you in other ways at our discretion, such as through the contact information you have provided. You are expected to check this page from time to time to take notice of any changes we make, as they are legally binding on you. Some of the provisions contained in this acceptable use policy may also be superseded by provisions of agreements with You, or by other notices published elsewhere on GXD's website.
- An updated version of this Policy will be effective immediately upon the posting of the revised Policy unless otherwise specified. Your continued use of the Website and Services after the effective date of the revised Policy (or such other act specified at that time) will constitute your consent to those changes.

Acceptance of this policy

You acknowledge that you have read this Policy and agree to all its terms and conditions. By accessing and using the Website and Services you agree to be bound by this Policy. If you do not agree to abide by the terms of this Policy, you are not authorized to access or use the Website and Services.

Contacting us

Any complaints regarding prohibited use or other abuse of the Services, including violations of this Policy, should be sent to GXD. Please include all applicable information that will assist GXD in investigating the complaint, including all applicable headers of forwarded messages.

If you have any questions, concerns, or complaints regarding this Policy, or wish to report a violation of this Policy, we encourage you to contact us using the details below:

partners@globalxdigital.com