Edged
Acceptable Use Policy

EDC Venture LLC and its subsidiaries and affiliates ("Edged") have adopted this Acceptable Use Policy (this "AUP") to govern the use of all services offered by Edged, including but not limited to internet services, Wi-Fi in Edged data centers, interconnection services, and other network services (the "Services"). This AUP applies to all aspects of the Services across Edged's network, including facilities, equipment, systems, services and products incorporated or used in such network (the "Edged Network"). By using the Services, you acknowledge that you are responsible for ensuring that your affiliates, agents and customers (together with you, "Users") comply with this AUP. Edged may modify this AUP at any time, effective immediately upon posting of the modification to its website.

Illegal Activity

Users may access and use the Services for lawful purposes only. Users must always use the Services in compliance with all applicable laws, rules and regulations. Edged strictly prohibits the use of the Services for the transmission, distribution, retrieval or storage of any information, data or other material in violation of any applicable law, rule or regulation. This prohibition includes, but is not limited to, the use or transmission of any data that is protected by copyright, trademark, trade secret, patent or other intellectual property right without proper authorization and the transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene, defamatory, harassing, or otherwise unlawful.

Security/Interference

A User may not attempt to gain unauthorized access to, or attempt to interfere with the normal functioning, operation or security of any portion of the Services. A User may not use the Services to engage in any activity that may interfere with the ability of others to access or use the Services or the Internet. A User is strictly prohibited from attempting to gain access to the user accounts of other Users, or violating system or network security, each of which may result in criminal and civil liability.

Examples of prohibited unauthorized access or interference include:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without the express prior authorization of the owner of the system or network.
- Intentionally revealing one's account password to others or allowing use of one's account by others.
- Unauthorized monitoring of data or traffic on any network or system without the express prior authorization of the owner of the system or network.
- Interference with service to any User, host or network including, without limitation, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks.
- Using, selling, or distributing in conjunction with the Services, any computer program designed to conceal the source or routing information of electronic mail messages in a

manner that falsifies an Internet domain, header information, date or time stamp, originating e-mail address, or other identifier.
- Disseminating or posting malicious content including, without limitation, viruses, Trojan horses, worms, time bombs, zombies or cancelbots.

Unsolicited Electronic Messaging

A User may not use the Services to transmit unsolicited messages or deliberately send excessively large attachments to one recipient by any means, including without limitation by email, text messages, instant messages or voice mail. “Spamming” or “mail-bombing” using the Services is prohibited. Users may not use the Services to transmit (1) unsolicited informational announcements; (2) chain mail; (3) numerous copies of the same or substantially similar messages; (4) empty messages; or (5) messages which contain no substantive content. Use of the service of another provider to send unsolicited messages, spam, or mail-bombs, to promote a site hosted on or connected to the Services, is similarly prohibited. Users may not use the Services to collect responses from mass unsolicited email messages. Users may not use another party’s mail server to relay mail without the express permission of such party.

Fraud/Spoofing

Users are prohibited from transmitting any electronic communications using a name or address of someone other than the User for purposes of deception. Any attempt to impersonate someone else by altering a source IP address information or by using forged headers or other identifying information is prohibited. Any attempt to fraudulently conceal, forge or otherwise falsify a User’s identity in connection with use of the Services is prohibited.

Other Prohibited Activities

Engaging in activities — whether lawful or unlawful — that Edged determines to be harmful to its customer relations, operations, reputation, or goodwill is prohibited. These activities include:

- Defamatory or abusive language.
- Any activity that disrupts, degrades, harms or threatens to harm the Services, including the Edged Network.
- Consuming excessive resources, including CPU time, memory, disk space and session time or using resource-intensive programs that negatively impact other Users or the performance of the Services or the Edged Network.

Edged's Rights

If a User engages in conduct that violates this AUP, Edged reserves the right to suspend or terminate the Services or the User's access to the Services. Edged will generally attempt to notify the customer of any activity in violation of this AUP and request that such customer take whatever steps necessary to cause such activity to cease. However, in cases where the operation of the Services is threatened or cases involving unsolicited commercial messaging, a pattern of violations, mail relaying, alteration of the User's source IP address information, denial of service attacks, illegal activities, suspected fraud in connection with the use of

Services, harassment, or intellectual property infringement, Edged reserves the right to suspend or terminate the Services or the User's access to the Services without notification. Edged reserves the right to install and use, or to have a User install and use, any appropriate devices to prevent violations of this AUP, including devices designed to filter or terminate access to the Services. Edged has no obligation to monitor or police activity occurring using the Services and will have no liability to any party, including a User, for any violation of this AUP. The actions described herein are non-exhaustive, and Edged reserves the right to take appropriate action to remedy any conduct it deems to be a violation of this AUP.

Cooperation with Law Enforcement

Edged reserves the right to cooperate with legal authorities and third parties in the investigation of illegal or inappropriate activity using the Services, including disclosing the identity of the customer and/or User that Edged deems responsible for the wrongdoing and any information related to such party's access and use of the Services.

Reporting Violations

Complaints regarding possible violations of this AUP should be sent to aupabuse@edged.us.

Last Updated: May 22, 2024