

Acceptable Use Policy

Version 2.1

Introduction

This Acceptable Use Policy (“**AUP**”) applies to Customer’s (defined below) access, use, and/or provision of certain 11:11 System, Inc. or its affiliates’ (together, “**11:11**”) products, services, computers, equipment, software, networks, and/or information systems (collectively, “**Systems**”) and supplements Customer’s definitive agreement with 11:11 (“**Customer’s Agreement**”). The term “**Customer**” includes 11:11’s direct customers and any authorized wholesale partner that provides the Systems to its customers, including, in each case, their end-users of the Systems. If there is a conflict between this AUP and the Customer’s Agreement, the Customer’s Agreement will control for that conflict.

11:11 may make changes to this AUP from time to time. If 11:11 makes changes, 11:11 will provide Customer with notice of such changes, and the updated AUP will be effective on the 30th day following the date on which such notice is provided to Customer, or such later time as specified by 11:11. Customer’s continued access, use, and/or provision of the Systems after such notice effective date will confirm Customer’s acceptance of the changes.

Customer is responsible for the activities of its end-users or customers and their end-users and, by accessing, using, and/or providing the Systems, agrees to inform its customers and/or end-users of this AUP or its own acceptable use policy, which must be co-extensive and consistent with these terms.

Compliance with Supplemental Carrier Terms

In addition to this AUP, additional guidelines, policies, terms, or rules of third-party carriers (the “**Supplemental Carrier Terms**”) may apply to Customer’s use of the Systems. Customer’s use of the Systems will comply with such Supplemental Carrier Terms, as applicable. Any violation of the Supplemental Carrier Terms is considered a violation of this AUP and the Customer’s Agreement. If there is a conflict between this AUP and any Supplemental Carrier Terms, the Supplemental Carrier Terms will control for that conflict. Links for additional carrier AUP policies are provided at the end of this Policy.

Notification Responsibilities

In addition to Customer’s obligations under the Customer’s Agreement, Customer will timely prepare for and react to notifications of actual and alleged violations of this AUP by complying with the following:

- 1) Customer will identify, and provide to 11:11 the contact information of, a customer representative to receive communications regarding possible violations of this AUP. Customer will keep such contact information current and up to date at all times and promptly provide any changes to 11:11 during the term of the Customer’s Agreement.
- 2) Customer will timely and professionally respond to and address the concerns of each complainant that sends a complaint to Customer (including any third-party complaints that may be forwarded by 11:11) regarding possible violations of this AUP (“Complaints”).

Acceptable Use Policy

Version 2.1

- 3) Customer will promptly investigate all such Complaints and take all necessary actions to remedy any violations of this AUP.
- 4) Promptly upon 11:11's request, Customer will provide true and complete copies of all Complaints to 11:11 at abuse@1111systems.com. Customer acknowledges that 11:11 is not required to, and will not, act as intermediary between Customer and a complainant.

Prohibited Conduct

Customer will only access, use, and/or provide the Systems for lawful purposes, their intended purposes, and the purposes set forth in Customer's Agreement. Customer will not violate any applicable law, contract, intellectual property right or other third party right or commit a tort in connection with its access, use, and/or provision of the Systems. Customer is solely responsible for Customer's and as applicable, its end-users and customers and their end-users,' conduct in connection with the Systems. Without limiting the foregoing, Customer will not:

1) **Access, Use, and Provision of the Systems**

- a) **Unauthorized Access.** Illegally or without authorization: access or attempt to access other computers, accounts, networks, or computer resources belonging to any third party or user; attempt to penetrate security measures of the Systems or other systems; devise ways to circumvent security in order to access unsubscribed Systems; encumber disk space, processors, or other System resources beyond amounts allowed by the applicable System's product or service guidelines provided by 11:11; or interfere with any System, overload a System, or disable, tamper with, take down, or attempt to disable, tamper with, or take down, any host not owned by Customer.
- b) **Usage Restrictions.** Place an unusually large burden on the Systems or exceed credit or usage limitations associated with the Systems without 11:11's express written consent.
- c) **Resale.** Sell or resell the Systems or provide the Systems as a service bureau, unless Customer is an authorized wholesale partner in good standing and Customer's Agreement allows for such additional uses of the Systems.
- d) **Modifications.** Modify any of the Systems, remove any proprietary rights notices or markings, or otherwise make any derivative works based upon the Systems.
- e) **Reproduction.** Copy, reproduce, distribute, publicly perform, or publicly display all or portions of the Systems, except as expressly permitted in writing by 11:11 or its licensors.
- f) **Reverse Engineering.** Reverse engineer any aspect of the Systems or do anything that might discover source code or bypass or circumvent measures employed to prevent or limit access to any part of the Systems.

Acceptable Use Policy

Version 2.1

- g) **Customer Applications.** Except as expressly permitted by Customer's Agreement, develop, or use any applications that interact with the Systems without 11:11's prior written consent.
- h) **No High-Risk Activities.** Use of the Systems in connection with aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support devices, Class III medical devices under the Federal Food, Drug and Cosmetic Act, or any other situation where failure or fault of the Systems could lead to death or serious bodily injury of any person or environmental damage.

2) Illegal Activities

- a) **Child Pornography.** Violate federal child exploitation statutes or possess, produce, receive, transport, or distribute by any means, including computer, visual depictions of "sexual intercourse," and/or "sexually explicit conduct" involving persons under the age of 18.
- b) **Illegal or Unauthorized Acts.** Use the Systems for any illegal or unauthorized purpose, or engage in, encourage, or promote any activity that violates Customer's Agreement or this AUP.
- c) **Fraudulent Activities.** Commit fraudulent activities including, but not limited to, intentional misrepresentations or misleading statements, writings, or activities made with the intent that the person or entity receiving it will act upon it; obtaining services with the intent to avoid payment; and hosting of phishing websites.

3) Prohibited Activities

- a) **Harassment.** Use any of the Systems to engage in any harassing, threatening, intimidating, predatory or stalking conduct.
- b) **Distribution of Viruses.** Distribute viruses, malware or other harmful code, or any other software, programs or messages that may cause damage or annoyance to persons, data, and/or computer systems. Any hosts owned by Customer and not timely secured or removed by Customer may be blocked by 11:11 from accessing the Systems.
- c) **Denial of Service.** Use any of the Systems in any manner that could interfere with, disrupt, negatively affect, or inhibit other users' use and full enjoyment of the Systems or that could damage, disable, overburden, or impair the functioning of the Systems in any manner. Customer is also prohibited from activity considered a precursor to attempted security violations including, but not limited to, any form of scanning, probing, or other testing or information gathering activity, without prior express written consent from 11:11's Chief Information Security Officer.

Acceptable Use Policy

Version 2.1

- d) **Data Mining.** Use any data mining, robots or similar data gathering or extraction methods designed to scrape or extract data from the Systems.
 - e) **Blacklisting.** Behave in any manner that causes blacklisting, and any such blacklisting must be remedied within 48 hours of written, electronic or telephonic notice from 11:11; or engage in any activities that result in re-listing.
 - f) **Vulnerability Testing.** Attempt to probe, scan, penetrate or test the vulnerability of the Systems or to breach 11:11's or any System's security or authentication measures, whether by passive or intrusive techniques, without 11:11's express written consent.
 - g) **Facilitating a Violation of This AUP.** Advertise, transmit, or otherwise make available any software, program, product, or service that is designed to allow a user to violate this AUP, including, but not limited to, facilitating the means to spam, initiating pinging, flooding, mail bombing, denial of service attacks, and piracy of software.
- 4) **Misrepresentation and Impersonation.** Impersonate any person or entity, or falsely state or otherwise misrepresent you or your affiliation with any person or entity, including by altering source IP address information and/or forging or misrepresenting a message header of an electronic transmission originating or passing through the Systems. Any attempt to fraudulently conceal, forge, or otherwise falsify a Customer's identity in connection with use of the Systems is prohibited.
- 5) **Spam and Emails**
- a) **Email Spamming.** Transmit, send, distribute, or post unsolicited or unauthorized advertising, promotional materials, "spam", bulk emails, "chain letters", or pyramid schemes or any similar form of solicitation; send large amounts of email repeatedly that annoys, harasses, or threatens another person or entity; or attempt to use the Systems as a mail drop or name server for any of the foregoing prohibited unsolicited or unauthorized advertising, promotional materials, "spam," bulk emails, "**chain letters,**" or **pyramid schemes.**
 - b) **Non-email Based Spamming.** Post messages to newsgroups/blogs/services that are irrelevant, blanket posting of messages to multiple newsgroups/blogs/services, or post annoying, harassing, and/or threatening messages; or violate any rules, policies, or charters posted online by any search engine, subscription web service, chat area, bulletin board, webpage, or any other service accessed via the Systems.
 - c) **Email Relay.** Use a third party's electronic email server to relay email without express permission from such third party.

Acceptable Use Policy

Version 2.1

Prohibited Content

Customer will not create, post, store, share, transmit, retransmit, redirect, or store any content, data, material, or information ("**Content**"), or cause the Systems to transmit, retransmit, redirect, store, provide, or receive any Content that, in 11:11's sole discretion:

- 1) **Inappropriate Content.** Is unlawful, pornographic (including child pornography), sexually explicit, indecent, lewd, suggestive, offensive, inflammatory, harassing, fraudulent, inappropriate, obscene, defamatory, libelous, threatening, abusive, hateful, or which contains or incites violence or discrimination or invades privacy or publicity rights.
- 2) **Violation of Law.** Would constitute, encourage, or provide instructions for a criminal offense, constitute an illegal threat, violate the rights of any person or entity or otherwise create liability or violate any applicable local, state, national, or international law, regulation, or order, or industry or community standards (including, without limitation, export control laws).
- 3) **Intellectual Property Rights.** May infringe any patent, trademark, trade secret, copyright, or other intellectual or proprietary right of any person or entity.
- 4) **Dangerous Activities.** Would constitute, encourage, or provide instructions for dangerous activities or self-harm.
- 5) **Provocation.** Is deliberately designed to provoke or antagonize people, especially trolling and bullying, or is intended to harass, harm, hurt, scare, distress, embarrass, or upset people; any material that is racist or discriminatory, including discrimination on the basis of someone's race, religion, age, gender, disability, or sexuality.
- 6) **Solicitations.** Contains any unsolicited promotions, political campaigning, advertising, or solicitations.
- 7) **Private Information.** Contains any private information of any third party, including addresses, phone numbers, email addresses, number and feature in the personal identity document (e.g., driver's license numbers, passport numbers), or credit card numbers.
- 8) **Viruses.** Contains any viruses, corrupted data, or other harmful, disruptive, or destructive files or content.
- 9) **Objectionable Content.** Is objectionable, restricts or inhibits any other person from using or enjoying the Systems, or may expose 11:11 or others to any harm, liability, or disrepute of any type.

Acceptable Use Policy

Version 2.1

Bulk Emailers

Customer will not, nor permit its end-users nor its customers' end-users (as applicable) to, send unsolicited bulk email from another Internet service provider's network advertising or implicating any Systems hosted or provided by 11:11, including, without limitation, email, web hosting, FTP and DNS services, or send email with added words/characters in an attempt to bypass Bayesian filters. If Customer uses bulk emailers on the Systems, Customer will: (1) remove complainants immediately upon request, and if required by law, provide the complete confirmed opt-in information for each complainant within 24 hours of the request; (2) establish and maintain an accurate and current master no-send list; (3) demonstrate a definitive prior business relationship between the sender and the recipient; and (4) if Customer utilizes an affiliate program to generate leads, Customer will: (a) remain fully responsible and liable for the actions of its affiliates, and (b) establish control over its utilized affiliates, including, but not limited to, blocking affiliate links and sending the affiliate traffic to a 404 error type page. ***11:11 may, in its sole discretion, rely upon information obtained from anti-spamming organizations (including, for example and without limitation, spamhaus.org, spamcop.net, sorbs.net, and abuse.net) as evidence that a user is an active "spam operation" for purposes of taking remedial action under this AUP.***

Violations and Enforcement

Violation of this AUP is a violation of Customer's Agreement. Penalties for violation of this AUP may include, but are not limited to: immediate suspension or termination of the Systems or any part thereof, removing or disabling Customer's access to the Systems or any part thereof, deletion and removal of Customer's content, data, materials, and/or information from the Systems, and /or termination of Customer's Agreement and/or Customer's account with 11:11, in each case with or without notice, without any refund, and subject to any applicable Early Termination Fee identified in Customer's Agreement. 11:11 may assess time and materials charges to resolve any actual or alleged violations of this AUP by Customer that are not timely, professionally, or fully resolved by the Customer and Customer will timely pay such charges to 11:11 in accordance with the terms of Customer's Agreement. In addition, 11:11 may exercise any other rights or remedies available to it for violations of this AUP or Customer's Agreement. Enforcement of this AUP is solely at 11:11's discretion, and failure to enforce this AUP in some instances does not constitute a waiver of 11:11's right to enforce it or Customer's Agreement in other instances. 11:11 is not liable for damages of any nature suffered by Customer, its end-users, or any third party resulting in whole or in part from 11:11 exercising its rights under this AUP or Customer's Agreement.

Inquiries

Customer will submit any inquiries regarding this AUP via email to: abuse@1111systems.com.

Acceptable Use Policy

Version 2.1

Other related documents:

CARRIER AUP LINKS

[Airtel](#)

[AT&T](#)

[Astound Broadband](#)

[Amazon Web Services](#)

[Colt Technology Services Group](#)

[Comcast](#)

[Conterra](#)

[Cogent Communications](#)

[Crown Castle](#)

[Entelgent](#)

[Extenet](#)

[Equinix](#)

[Flexential](#)

[Frontier](#)

[GTT](#)

[Hurricane Electric](#)

[INAP](#)

[DartPoints \(formerly Immedion\)](#)

[Lightpath](#)

[Nitel](#)

[CenturyLink / Lumen](#)

[Megaport](#)

[Momentum](#)

[NTT](#)

[Optus](#)

[QTS](#)

[Singtel Mobile](#)

[Spectrum Enterprise](#)

[Spectrum Broadband](#)

[Spectrotel](#)

[Tata Communications Transformation Services](#)

[Telia Company](#)

[Telstra Global](#)

[Unitas Global](#)

[Uniti](#)

[Verizon](#)

[Vocus](#)

[Zayo](#)