

---

### Acceptable Use Policy

This Acceptable Use Policy applies to all persons and entities (collectively, "customers") using the products and services of Cywest Communications, Inc., ("Cywest") including Internet and Infrastructure services. The policy is designed to protect the security, integrity, reliability, and privacy of both the Cywest network, cloud infrastructure, and the products and services Cywest offers to its customers. Cywest reserves the right to modify this policy at any time, effective immediately upon posting of the modification. Your use of Cywest's products and services constitutes your acceptance of the Acceptable Use Policy in effect at the time of your use. You are solely responsible for any and all acts and omissions that occur during or relating to your use of the service, and you agree not to engage in any unacceptable use of the service.

#### Uses That Are Prohibited

Unacceptable use includes, but is not limited to, any of the following:

1. Posting, transmission, re-transmission, or storing material on or through any of Cywest's products or services, if in the sole judgment of Cywest such posting, transmission, re-transmission or storage is: (a) in violation of any local, state, federal, or non-United States law or regulation (including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations); (b) threatening or abusive; (c) obscene; (d) indecent; or (e) defamatory. Each customer shall be responsible for determining what laws or regulations are applicable to his or her use of the products and services.
2. Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by customer.
3. Resale of Cywest's products and services without the express prior written consent of Cywest (unless you are an authorized wholesaler).
4. Deceptive marketing practices.
5. Actions that restrict or inhibit anyone - whether a customer of Cywest or otherwise - in his or her use or enjoyment of Cywest's products and services, or that generate excessive network traffic through the use of automated or manual routines that are not related to ordinary personal or business use of Internet services.
6. Introduction of malicious programs into the Cywest network or servers or other products and services of Cywest (e.g., viruses, trojan horses and worms).
7. Causing or attempting to cause security breaches or disruptions of Internet communications. Examples of security breaches include but are not limited to accessing data of which the customer is not an intended recipient, or logging into a server or account that the customer is not expressly authorized to access. Examples of disruptions include but are not limited to port scans, flood pings, packet spoofing and forged routing information.
8. Executing any form of network monitoring that will intercept data not intended for the customer.
9. Circumventing user authentication or security of any host, network or account.
10. Interfering with or denying service to any user other than the customer's host (e.g., denial of service attack).
11. Using any program/script/command, or sending messages of any kind, designed to interfere with, or to disable a user's terminal session.
12. Failing to comply with Cywest's procedures relating to the activities of customers on Cywest-owned facilities.
13. Furnishing false or incorrect data on the order form contract (electronic or paper) including fraudulent use of credit card numbers or attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization or other methods to document "use" of Cywest's products or services.
14. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers of the customer or with whom the customer does not have an existing business relationship (e.g., E-mail "spam"); or distributing, advertising or promoting software or services that have the primary purpose of encouraging or facilitating unsolicited commercial E-mail or spam.

15. Harassment, whether through language, frequency, or size of messages.
16. Unauthorized use or forging of mail header information.
17. Solicitations of mail or any other E-mail address other than that of the poster's account or service, with the intent to harass or collect replies.
18. Creating or forwarding "chain letters" or other "pyramid schemes" of any type.
19. Use of unsolicited E-mail originating from within the Cywest network or networks of other Internet Service Providers on behalf of or to advertise any service hosted by Cywest or connected via the Cywest network.
20. Exporting, re-exporting, or permitting downloads of any content in violation of the export or import laws of the United States or without all required approvals, licenses and exemptions.
21. Any action that Cywest deems as outside the normal or intended use of the Cywest network, cloud infrastructure, and any element related to Cywest services furnished to, and for customer.
22. Any Customer Premise Equipment (CPE) supplied to customer must be maintained by customer under proper conditions that meet the following specifications:

Operating Temperature and Altitude	-32 to 104 °F (0 to 40 °C)  Derate max operating temperature 1.5 °C per 1000 ft above 5000 ft  10,000 ft maximum except CCC1 only up to 2000 meters.
Humidity	Maximum 85% non-condensing RH
Transportation/Storage Conditions:	
Temperature	-40 to 158 °F (-40 to 70 °C)
Humidity	5-95%
Altitude	Altitude

No failure or delay in exercising or enforcing this policy shall constitute a waiver of the policy or of any other right or remedy. If any provision of this policy is deemed unenforceable due to law or change in law, such a provision shall be disregarded and the balance of the policy shall remain in effect.

Abusable Resources

Upon notification of the existence of an abusable resource (e.g., open news server, unsecured mail relay, or smurf amplifier), the customer shall immediately take all necessary steps to avoid any further abuse of such resource. Any abuse of an open resource that occurs after the customer has received such notification shall be considered a violation of this policy and enforced as such.

Enforcement

Cywest may immediately suspend and/or terminate the customer's service for violation of any provision of this policy upon verbal or written notice, which notice may be provided by voicemail or E-mail. Prior to suspension or termination, Cywest attempts to work with our customers to cure violations of this policy and ensure that there is no re-occurrence; however, Cywest reserves the right to suspend or terminate based on a first offense. Cywest reserves the right to charge fees arising from management or handling of complaints related to alleged violations of the AUP.

Electronic Communications Privacy Act Notice

Cywest makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon Cywest technology, and makes no guarantee that any other entity or group of users will be included or excluded from Cywest's



Cywest Communications, Inc.  
26741 Portola Parkway, Suite 1E-224  
Foothill Ranch, CA 92610

---

network. In addition, Cywest may periodically monitor transmissions over its network for maintenance, service quality assurance or any other purpose permitted by the Electronic Communications Privacy Act, P.L. No. 99-508, as amended.

Questions?

If you are unsure of whether any contemplated use or action is permitted, please contact Cywest through the Cywest ticketsys portal or cell phone app.