cynetel

Acceptable Use Policy (AUP)

Last Revised: February 15, 2023

14.1 IN ORDER TO PROVIDE HIGH QUALITY CUSTOMER SERVICE AND TO ENSURE THE INTEGRITY, SECURITY, RELIABILITY, AND PRIVACY OF CYNETEL'S INTERNET NETWORK, CYNETEL HAS CREATED THIS ACCEPTABLE USE POLICY (AUP). THIS AUP APPLIES ALONG WITH THE TERMS OF SERVICE (TOS) GOVERNING THE CUSTOMER'S USE OF CYNETEL'S INTERNET AND RELATED SERVICES.TO SPECIFY USE RESTRICTIONS APPLICABLE TO USERS OF THE SERVICE. THE CUSTOMER RECOGNIZES AND AGREES THAT THE THEN CURRENT VERSION OF THE AUP TO BE MAINTAINED BY CYNETEL AND POSTED ON CYNETEL'S WEBSITE WILL SUPERSEDE ALL PREVIOUS VERSIONS OF THIS DOCUMENT AND THAT CUSTOMER'S CONTINUED USE OF CYNETEL'S INTERNET SERVICE WILL CONSTITUTE CUSTOMER'S ACCEPTANCE OF THIS POLICY AS IT MAY BE AMENDED. BY USING THE SERVICE, THE CUSTOMER AGREES TO ABIDE BY, AND REQUIRE EACH USER OF THE SERVICE TO ABIDE BY, THE TERMS OF THIS AUP AND ASSOCIATED. ANY USER WHO DOES NOT AGREE TO BE BOUND BY THESE TERMS, CUSTOMER MUST IMMEDIATELY CEASE USE OF THE SERVICE.
CYNETEL RESERVES THE RIGHT AT ITS SOLE DISCRETION TO IMMEDIATELY SUSPEND, TERMINATE, OR RESTRICT USE OF THE SERVICE WITHOUT NOTICE IF SUCH USE VIOLATES THE AUP OR ANY ASSOCIATED AND POSTED TOS, IS OBJECTIONABLE OR UNLAWFUL, INTERFERES WITH CYNETEL'S SYSTEMS OR NETWORK OR THE INTERNET OR OTHERS' USE OF THE SERVICE.

14.2 **USE**

14.2.1 The Service is designed solely for End Customer's commercial use. Customer is responsible for any misuse of the Service that occurs through Customer's account, whether by guest user of the Customer or an authorized or unauthorized third-party end users of the Service. Customer must take steps to ensure that others do not gain unauthorized access to the Service. Customer is responsible for the security of (i) any device Customer chooses to connect to the Service, including any data stored or shared on that device and (ii) any access point to the Customer's Service. Cynetel reserves the right to suspend or terminate the Service for failure to comply with any portion of this provision or this Policy, without prior notice.

14.3 PROHIBITED ACTIVITIES USING THE SYSTEM, NETWORK, AND SERVICE

14.3.1 Any activity or use of the Service which violates system or network security or integrity are strictly prohibited and may result in criminal and civil liability. Such violations include, without limitation, the following:

14.3.1.a 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, relay communication through a resource, or to breach security or authentication measures without express authorization of the owner of the system or network.

14.3.1.b Unauthorized monitoring of data or traffic on any network or system without express written authorization of the owner or network.

14.3.1.c Interference with service to any user, host, or network, including but not limited to: mail bombing, flooding, or denial of service attacks.

14.3.1.d Forging the header of any transmitted information packet, email, or Usenet posting.

14.3.1.e Modifying or tampering with any hardware, software, or configuration provided by Cynetel including but not limited to: routers, switches, access points, wireless gateways, and devices configuration files.

14.3.1.f Disrupting any aspect of the Service through any means.

14.3.1.g Assuming or assigning a Cynetel IP address that was not allocated to the user by Cynetel or its network – all Cynetel Internet users must use an IP address or space provided explicitly by Cynetel.

14.3.1.h Running any type of server or service on Cynetel's Network or System that is intentionally used to disrupt other users of the Service or users of the Internet in general.

14.4 NO ILLEGAL OR FRAUDULENT USE

14.4.1 The Service may strictly be used only for lawful purposes.

14.4.2 Customer will not use or allow others to use the service in any manner that is in violation of any applicable federal, state, local or international laws or regulations or to promote, engage in, or enable illegal activity or conduct that violates or infringes upon the rights of any person.

14.4.3 Transmission or distribution of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene illegal, defamatory, constitutes an illegal threat, or violates export control laws.

14.4.5 Furthermore, use of the Service to impersonate or a person or entity is strictly not permitted.

14.5 **NO SPAM**

14.5.1 Users may not send any unsolicited bulk email or electronic communication including, but not limited to, instant messenger programs, IRC, Usenet, etc. that promotes or advertises a cause, opinion, money making opportunity, or the like that the recipient did not specifically request from the sender (“Spam”).These communications do not necessarily have to pass through the Service’s email infrastructure – it only needs to originate from a customer or service user of Cynetel.

14.5.2 Users may not send any type of communication to any individual who has indicated that he/she does not wish to receive messages from them.

14.5.3 Continuing to send electronic communication to anyone that has expressly requested not to receive email from a User is considered to be harassment or a threat.

14.6 **NO SYSTEM DISRUPTION**

14.6.1 Customer will not use, or allow others to use, the Service to disrupt degrade, and/or otherwise adversely affect or in any way negatively impact Cynetel’s network or Service Provider equipment, and any other IT equipment owned or Managed/Maintained by Cynetel or other Cynetel customers.

14.7 **SECURITY/ABUSABLE RESOURCES**

14.7.1 User is solely responsible for the security of any device connected to the Service, including any data stored on that device and Cynetel assumes zero responsibility for the integrity of the data on those devices that are connected to the network and zero liability.

14.7.2 Users shall take all necessary steps to avoid actions that result in the abuse of a resource on their network. Examples of abusable resources include but are not limited to: open news servers, open SMTP servers, insecure routers, wireless access and insecure proxy servers, insecure or outdated software or operating systems, etc.

14.7.3 Upon notification from Cynetel, Users are required to address the problem in a timely fashion. Failure to address an issue after notification will be considered a violation of this AUP.

14.8 **NO “HACKING”**

14.8.1 Customer will not use, nor allow others to use, the Service to access the accounts of others or to attempt to penetrate or compromise security measures of the Service, Service Provider, or other computer systems (“hacking”) or to cause a disruption of the Service to other on-line users.

14.8.2 Customer will not use, nor allow others to use, tools designed for compromising network security, such as password-guessing programs, cracking tools, packet sniffers or network probing tools. Subsequent detection of these services on the network will be sent with a immediate warning, and if not met with a resolution of 2 Business Days, will have services disconnected until further notice and subsequent action is taken on behalf of the customer to ensure these activities have been removed or subsequently blocked. Furthermore, if additional detection of these activities are discovered from Cynetel, or reported from Cynetel's customers, or any other user, Service user may be subject to automatic termination and immeadiate subsequent legal action.

14.9 NETWORK MANAGEMENT

14.9.1 Cynetel reserves the right to use a changing variety of reasonable network management techniques including but not limited to (i) allocation of a fixed maximum amount of bandwidth to non-customers seeking to upload peer-to-peer files from customers; (ii) utilizing routing techniques to prioritize traffic during times of peak congestion; and (iii) implementing filtering and spam detection techniques to manage reliable electronic communication sources and mitigate spam. In limited instances, these techniques may affect the throughput rate at which customers may send and receive data, non-customers' ability to establish session connections within the network (such as peer-to-peer sessions),or result in the delay of certain traffic during times of peak congestion.

14.10 Viruses and Ransomware

14.10.1 Users must take appropriate action to prevent their systems from becoming infected with and/or distributing computer viruses such as but not limited to worms, "Trojan horses", denial of service attacks bots, Ransomware, and any other type of malicious file that may potentially put Cynetel or the customers network at risk.

14.10.2 Cynetel will take appropriate (as decided by Cynetel's sole discretion) action against Users infected with computer viruses or worms to prevent further spread. Cynetel will use industry standard techniques to ensure that the problem may be remediated from there end and customer understands that they Cynetel may use whatever method they choose to remedy the issue.

14.11 ENFORCEMENT

14.11.1 Cynetel reserves the right to investigate violations of this AUP, including the gathering of information from the Customer or other Users

involved and the complaining party, if any, and the examination of material on Cynetel's servers and network. Customer understands that Cynetel may have background processes that run data collection on the web results that are being searched from the customer, and may randomly screen or check the results for any potential violations of the AUP.

14.11.2 Cynetel prefers to advise Users of AUP violations and any necessary corrective action but, if Cynetel, in its sole discretion, determines that a User has violated the AUP, Cynetel will take any immeadiate responsive action that is deemed appropriate without prior notification. Such action includes but is not limited to: temporary suspension of service, reduction of service resources, and immediate termination of service.

14.11.3 Cynetel is not liable for any such responsive action and these actions are not exclusive.

14.11.4 Cynetel may take any other legal or technical action deemed appropriate for resolution.

14.12 **NO WAIVER**

14.12.1 The failure by CYNETEL or its affiliates to enforce any provision of this Policy at any given point in time shall not be construed as a waiver of any right to do so at any future time thereafter.

14.13 **REVISIONS TO POLICY**

14.13.1 Cynetel reserves the right to update or modify this Policy at any time and from time to time with or without prior notice.

14.13.2 Continued use of the Service will be deemed acknowledgment and acceptance of this Policy.

14.13.3 Notice of modifications to this Policy may be given by email or by conventional mail and will be effective immediately upon posting or sending.

14.13.4 Customers should regularly visit Cynetel's website at https://www.cynetel.com/legal/aup and review this Policy to ensure that their activities conform to the most recent version.

14.13.5 In the event of a conflict between any customer or customer agreement and this Policy, the terms of this Policy will govern.

14.13.6 Questions regarding this Policy or complaints of violations of it by Cynetel customers can be directed to aup-violations@cynetel.com