

This Acceptable Use Policy specifies certain actions prohibited by TexinsWeb for users of the TexinsWeb network. TexinsWeb reserves the right to modify this Policy at any time to stay in compliance with any laws, regulations and security requirements. By using TexinsWeb services, any customer, employee or third party unconditionally accepts the terms of this policy.

## ILLEGAL USE

The TexinsWeb Network may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation coming to or from any unauthorized network or system is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property rights used without proper authorization; government and military data protected by law and national security; university and academic data protected by public policy; and material that, in TexinsWeb's sole discretion, is obscene, defamatory, constitutes an illegal threat, or violates export control laws. Any violation of the above which compromises the integrity of the TexinsWeb Network or any other network is strictly prohibited.

## NETWORK AND MACHINE RESOURCES

TexinsWeb reserves the right to monitor and allocate network and machine resources. IP addresses are allocated per server and according to virtual server specifications. TexinsWeb in its sole discretion and upon reasonable notice to customer reserves the right to discontinue any hosting account and/or any script which causes excessive server load and/or uses excessive server and network resources.

To protect Internet, network, and machine resources on behalf of the entire TexinsWeb customer base, no individual customer may do the following:

1. Resell or give away web space under a domain name, or create "sub-domain" web sites on behalf of other companies, groups, or individuals;
2. Use their web site to store web pages, files, or data for other IP addresses or domain names, or as a repository for files, data, or "Warez group" download transfer;
3. Use their web site for data transfer from any database server, or for streaming audio and/or video downloads; or use their web site as a storage area for files that are not linked to the customer's web pages hosted on the same web site on TexinsWeb's servers;
4. Offer adult content, mp3 downloads, or software downloads; or
6. Utilize CGI/PERL chat, JAVA chat, or any other chat scripts in a manner that adversely affects the operations or performance of other TexinsWeb customers, or of the TexinsWeb system or network. The adverse effect of such use shall be determined by TexinsWeb in its sole discretion.

TexinsWeb may immediately suspend service without prior notice to any web site that violates these rules. In the event of any dispute regarding these rules, TexinsWeb may determine violations of these rules in its sole discretion.

Customers utilizing bandwidth in excess of plan limitations, or in violation of these rules, will owe TexinsWeb compensation therefor at the applicable rate for excess bandwidth.

## SYSTEM AND NETWORK SECURITY

Violations of system or network security are prohibited, and may result in criminal and civil liability. TexinsWeb will investigate incidents involving such violations and may involve and cooperate with law enforcement authorities if a criminal violation is suspected. TexinsWeb respects the privacy of customer data and vigilantly protects that data and ALL customers who host with TexinsWeb. If any violation of the law or this AUP is suspected, TexinsWeb reserves the right to investigate. Use of the TexinsWeb network

constitutes consent to monitoring. Examples of unlawful acts, system, or network security violations include, without limitation, the following: Unauthorized access to or use of data, systems or networks, including any attempt to probe, damage, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network. Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks. Unauthorized access to any data, system, or network from an unauthorized system or network for any purpose which is not lawful or which is intended to do harm. Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting. Electronic forging of any kind to include but not limited to IP addresses, domains, business names, etc.

## EMAIL

Sending unsolicited email messages, including, without limitation, unwanted advertising and informational announcements, is explicitly prohibited, whether sent in bulk or not, and whether commercial in nature or not. The use of TexinsWeb resources to sell or enable the sale of "bulk" and/or "stealth" email software (to include so-called "spoof" software) is strictly forbidden. The use of TexinsWeb resources to sell or enable the sale of software designed to "harvest" email addresses is also categorically prohibited. A user shall not use another site's mail server to relay mail without the express permission of the site owner. Legitimate mailing lists and subscriber lists are acceptable. Otherwise, it is spam.

## USENET

Posting the same messages to multiple newsgroups (excessive cross-posting or multiple-posting, also known as "SPAM") is expressly prohibited.

**INDIRECT OR ATTEMPTED VIOLATIONS OF THE POLICY, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A TEXINSWEB CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THE POLICY BY SUCH CUSTOMER OR END USER.**

For Example: If you are hosting a bulk email site on TexinsWeb servers and you use another ISP to SPAM from in order to reference your TexinsWeb site by IP address or domain name, you are violating TexinsWeb policy and possibly the law. Forgery is against the law. Any type of denial of service attack from valid or invalid addresses is a violation of TexinsWeb security policy and against the law. If you have been granted password privileges for FTP or telnet, sharing your password with an unauthorized user or third party is strictly prohibited. Complaints regarding illegal Use or System or Network Security issues should be sent to support@texinsweb.com. Complaints regarding email abuse should be sent to support@texinsweb.com. Complaints regarding USENET abuse or SPAM should be sent to support@texinsweb.com.

## INTERACTION WITH STAFF

Any threat, vulgar and profane language directed at any TexinsWeb staff member through phone or email may result in immediate termination of an account. Any violation of this policy by any employee, contractor or third party programmer of TexinsWeb should be reported immediately. Bottom line is let's work together toward a mutually beneficial relationship and create a prosperous and responsible Internet community.