

## **Acceptable Use Policy**

White River Technologies, LLC dba White River Connect, LLC (Connect) has established an Acceptable Use and Network Management Policy ("AUP") for the protection of Connect and its customers for the use of its products and services. Connect can be contacted at 417-318-2628 regarding any questions you have about this AUP, Connect, or its products and services. By using services provided by Connect you agree to be bound by the terms of this AUP. This policy may be updated from time to time. Customers are encouraged to frequently check this page for any changes to this policy. Continued use of the Services after a change to this policy indicates your agreement with the updated terms.

Phone and Internet Service. This AUP applies to customer use of any Connect Voice Over Internet Protocol (VoIP) service (phone service) or Internet service (collectively, Service(s)) regardless of technology or the Internet-based application utilized. It is not acceptable to use Connect's network for any purpose that violates local, state, or federal laws or to transmit communications that might be highly offensive or damaging to any recipients or to use the services in a manner that is unintended. It is not acceptable to interfere with, violate, circumvent, misuse, distribute or disrupt network users, equipment, or services. A customer may not:

- 1. Use any Connect Services or use or permit the use of Service for unlawful purposes or purposes that Connect believes to be unacceptable;
- 2. Use any Service to transmit, post or receive material that is threatening, abusive, libelous, defamatory, obscene, pornographic, or otherwise in violation of any local, state, federal or international law or regulation;
- 3. Transmit any information or software that contains a virus, worm, Trojan Horse, or other harmful component;
- 4. Transmit or download any information, software or other material that is protected by copyright or other proprietary right without the permission of the person owning that protected right;
- 5. Transmit SPAM or other bulk email;
- 6. Add, remove, or modify identifying network heading information (aka "spoofing") to deceive or mislead, or any impersonation of another person using forged headers or other improper identifying information;
- 7. Engage in any activity which would compromise customer privacy or system security or gain access to any system or data without required permission (e.g., "hacking") of the owner;
- 8. Engage in any activity which would result in third-party charges to Connect:

- 9. Resell or otherwise share Connect's Service, account information, or passwords;
- 10. Attempt to obtain unauthorized access to any network or account. This includes accessing data not intended for end user customers, logging into a server or account without being expressly authorized to access or probing the security of other networks;
- 11. Attempt to interfere with the Service of others including users, hosts, and networks. This includes "denial of service" attacks, "flooding" of networks, deliberate attempts to overload a service and attempts to "crash" any host;
- 12. Distribute Connect Services beyond the scope of your end-user account:
- 13. Attach equipment, accessory, apparatus, circuit or devices that are harmful to the network and are attached to or connected with Connect facilities;
- 14. Use Connect's Service for web or email hosting without making special written subscription arrangements with Connect;
- 15. Undertake, plan, encourage, assist, or accomplish any unlawful, deceptive, or fraudulent activity or purpose. This includes, but is not limited to conduct which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or international law, order, or regulation;
- 16. Use auto-dialers or predictive-dialing to dial sequentially, including rapid dialing or data pumping for the purpose of generating revenue directly or indirectly:
- 17. Violate any of the federal, state, or local telemarketing regulations including but not limited to the Telephone Consumer Protection Act of 1991 ("TCPA"), the Telemarketing Sales Rules ("TSR"), the Junk Fax Prevention Act of 2005, and Truth in Caller ID Act of 2009:
- 18. Send unsolicited calls, messaging, e-mailings (including, without limitation, commercial advertising and informational announcements) if such unsolicited activities could reasonably be expected to or do in fact provoke complaints;
- 19. Engage in any form of Robo calling as defined by the Federal Trade Commission's Telephone Sales rule (TSR) that are unlawful:
- 20. Engage in any unlawful form of calling utilizing pre-recorded audio or non-live-human communications;
- 21. Engage in continuous or extensive chat line or conference call participation;
- 22.Use an open telephone line as a monitoring, intercom, or similar service;
- 23. Fail to monitor outbound call campaigns to minimize complaints which may be generated by repetitive and/or continuous messaging or calling to the same destination or number within a short period of time;
- 24.Use Services to record or monitor a phone call or other communication without securing consent from the call participants as required by applicable federal and state laws (including, as applicable, California's Invasion of Privacy Act and similar laws):

25.Engage in extensive call forwarding or use of call forwarding or conferencing features to act as a bridge to chat lines or other conferencing facility;

26.Operate a business (including a home-based business, a non-profit business, governmental or any other enterprise) under a residential service account:

27. Operate a call center or conference line;

28. Transmit or receive broadcasts over teleconferencing facilities or other means.

Connect does not screen in advance any specific content accessible using its Services. Connect disclaims any liability for any act or omission with regard to content the customer finds objectionable or unsuitable. Use of information accessed by the Services is at the customer's own risk. Connect disclaims any responsibility for the accuracy, privacy, or quality of the information. By using the Services, the customer agrees to hold Connect harmless for content accessed using the Services.

Any IP address assigned to a customer on either a dynamic or static basis remains the property of Connect and may not be appropriated for any use other than as intended by Connect or transferred to any other party. Connect will not ask you for your password in an unsolicited telephone call or email. If you believe your password has been compromised, you should immediately change your password to prevent the unauthorized use of it.

**Indemnification.** The customer agrees to indemnify, defend, and hold Connect harmless of and from any and all claims, damages, liabilities, losses, and/or expenses (including attorneys' fees, expert fees, and other legal expenses and costs) resulting from the customer's use (or misuse) of Connect's Services whether or not such use is found to be in violation of any statute, regulation or rule.