Acceptable Use

Updated: July 28, 2017

Connectria, LLC. (“Connectria”, “us” or “we”) provides a variety of information, Internet, network and technology related services (collectively, “Services”). This Acceptable Use Policy (“AUP”) is applicable to any and all access and use of the Services and/or the Connectria network (the “Network”) including, without limitation, use and access by (a) Connectria’s customers, (b) Connectria’s customers’ customers, members, and end-users, and (c) any other parties who use or access the Services or Network (collectively, “Users”). All Users must comply with this AUP.

BY ACCESSING OR USING THE SERVICES OR THE NETWORK, EACH USER AGREES TO THIS AUP. A USER IS NOT AUTHORIZED TO ACCESS OR OTHERWISE USE THE SERVICES OR THE NETWORK UNLESS SUCH USERS FULLY COMPLIES WITH THIS AUP.

Each customer of Connectria agrees that it is responsible for violations of this AUP by itself and by any User that uses or access the Services or the Network through such customer, whether authorized by such customer or not.

Changes to this AUP
WE MAY REVISE THIS AUP AT ANYTIME. WHEN WE DO, WE WILL ALSO REVISE THE “LAST UPDATED” DATE AT THE TOP OF THIS AUP. EACH USER IS RESPONSIBLE FOR REGULARLY REVIEWING THE CURRENT AUP. THE MOST CURRENT VERSION OF THE AUP CAN BE REVIEWED AT https://www.connectria.com/acceptable-use. A USER’S CONTINUED USE OF THE SERVICES AND/OR NETWORK AFTER WE POST ANY REVISED AUP CONSTITUTES SUCH USER’S AGREEMENT TO ANY SUCH REVISED AUP.

General Restrictions
Users shall not use the Services or Network (a) to transmit, distribute or store material in violation of any applicable law, regulation, or judicial order, (b) in a manner that violates the terms of this AUP, the terms of any applicable agreement with Connectria, or any other Connectria policy applicable to such Users, (c) in a manner that interferes with or adversely affects the Services or Network or use of the Services or Network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks, or (d) in a manner that may expose Connectria to criminal or civil liability. Users shall cooperate with Connectria in investigating and correcting any actual or alleged breach of this AUP.

Specific Restrictions
Without limiting the generality of any other provision of this AUP, Users shall:

(1) not, directly or indirectly, use the Services and/or Network to monitor data or traffic on any network or system without the authorization of the owner of the system or network,

(2) not, directly or indirectly, use the Services and/or Network to access or use an Internet account or computer without the owner's authorization, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, security hole scanning, and port scanning;

(3) not, directly or indirectly, use the Services and/or Network to transmit, distribute or store information or material that (a) is inappropriate, offensive, obscene (including, without limitation, child pornography), defamatory, threatening, abusive, advocating violence or which violates a law, regulation or public policy, (b) is harmful to or interferes with Connectria's provision of Services, the Network, or the provision of any third party's networks, equipment, applications, services, or web sites (e.g., data mining software, viruses, worms, web crawlers, robots, cancelbots, spiders, Trojan horses, or any data gathering or extraction tools, etc.), (c) might infringe, dilute, misappropriate, or otherwise violate any privacy, intellectual property, publicity or other personal rights including, without limitation, any copyright, patent, trademark, trade secret or other proprietary right (including, without limitation, unauthorized use of domain names), (d) is fraudulent or contains false, deceptive, or misleading statements, claims, or representations (such as "phishing"), and/or (e) violates generally accepted standards of Internet usage,

(4) not, directly or indirectly, use the Services and/or Network to forge any TCP/IP packet header or any part of the header information in an e-mail or a newsgroup posting,

(5) not, directly or indirectly, use the Services and/or Network to engage in any conduct that is likely to result in retaliation against the Network or Connectria's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack,

(6) not, directly or indirectly, use the Services and/or Network to gain unauthorized access to or use of data, systems or networks, including attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures (including those belonging to Connectria and its customers),

(7) comply with the CAN-SPAM Act of 2003, as may be amended from time-to-time and all other laws and regulations applicable to bulk e-mail, and refrain from sending “Unsolicited Bulk Email” which shall also be referred to as SPAM interchangeably within this AUP. For purposes of this section, Connectria defines (a) “Unsolicited” to mean a message where the Recipient has not granted verifiable permission for the message to be sent, and (b) “ Bulk” to mean that the message is sent as part of a larger collection of messages, all having substantively identical content. A message is considered SPAM, and therefore unacceptable, only if it is both Unsolicited and Bulk. Unsolicited Email may be normal email (examples: first contact enquiries, job enquiries, sales enquiries). Bulk Email can be normal email (examples: subscriber newsletters, customer communications, discussion lists). An electronic message is SPAM if: (1) the recipient’s personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent. In order for the sending of bulk email to be acceptable, and therefore not considered SPAM, User must comply fully to the processes forth by SPAMHAUS (the “SPAMHAUS Processes”) found on the following webpage:

http://www.spamhaus.org/whitepapers/permissionpass.html

Whether User is compliant with the SPAMHAUS Processes shall be determined by Connectria in Connectria’s sole discretion. In addition, all Users must obtain Connectria’s advance approval for any bulk e-mail before using the Service or Network to send such e-mail, which may be withheld for any reason whatsoever.

(8) not, directly or indirectly, use the Services and/or Network to violate any charters, policies, rules or agreements promulgated by any search engines, blogs, subscription Web services, chat areas, bulletin boards, Web pages, USENET, or other services accessed via the Services or Network (“Usenet Rules”), including, without limitation, any cross postings to unrelated news groups, continued posting of off-topic messages, and disrupting newsgroups with materials, postings, or activities that are inappropriate (as determined by Connectria in its sole discretion), unless such materials or activities are expressly allowed or encouraged under the Usenet Rules,

(9) not, directly or indirectly, use the Services and/or Network to violate the applicable acceptable use policies of other Internet Service Providers (“ISPs”) when data, content, or other communications are carried across,

(10) not, directly or indirectly, use the Services and/or Network to provide “shell account” hosting, or the resale of “shell accounts” to third party entities that are not approved customers of Connectria, nor re-sell direct access to your hosted server via telnet, ssh or other shell binary,

(11) not, directly or indirectly, use the Services and/or Network to run any type of IRC software including, but not limited to, IRC client software, IRC server software, IRC bots such as “eggdrop” and “chaos,” and/or IRC software that is embedded within a web interface,

(12) not, directly or indirectly, deny server log-in access to Connectria’s staff, nor disable or demote the Administrator or Root accounts (sometimes called RedShield01 and RedShield02 accounts by Connectria) from being Administrator or Root accounts, nor hide any prohibited files on the server(s), and

(13) not, directly or indirectly, use the Services and/or Network to engage in any other conduct that Connectria believes, in its sole and reasonable discretion, to be illegal, abusive, or irresponsible behavior.

Restrictions On The Use Of Virtual Machine Technology.
In the event Customer utilizes virtualization technologies within the Services or Network, the following terms shall apply: (a) Customer shall not utilize any virtualization technology within the Services or Network other than those provided by Connectria without the prior written consent of Connectria; (b) Customer shall provide Connectria with full administrative rights and administrative access to all Virtual Machines deployed within the Services or Network and provide Connectria with these access privileges within 4 hours of deploying a new Virtual Machine; (c) Connectria will only provide support to Customer for a specific Virtual Machine if that Virtual Machine was created and setup by Connectria and only if Customer has also purchased Connectria’s Managed Hosting support plan (or a higher support plan) for that specific Virtual Machine; (d) Connectria shall only provide Operating System support within a Virtual Machine for those Operating Systems installed and provided by Connectria; (e) Any network support provided to Customer by Connectria for a Customer-provided Virtual Machine will be provided on a time and materials basis at Connectria’s then current hourly rates, and Customer may not utilize Systems Administration hours bundled within their support plans for this network support; (f) Connectria requires that the primary IP address assigned to a physical server must not be changed, and this IP address must at all times remain on the physical server and may not be moved to a Virtual Machine; (g) Connectria’s 100% Secure Guarantee contained within the Connectria Service Level Agreement shall not apply to a Virtual Machine unless Customer has purchased Connectria’s Managed Hosting support plan or a higher support plan for that specific Virtual Machine. Failure to comply with these restrictions shall be considered a violation of the Connectria AUP, and Customer expressly acknowledges and understands that Connectria may shut down any or all of Customer’s physical server(s) until the violation with any Virtual Machine is brought back into compliance.

Cooperation with Investigations & Legal Proceedings.
Connectria may, without notice to you (a) report to the appropriate authorities any conduct by you that it believes violates applicable criminal law, and (b) provide any information it has about you in response to a formal or informal request from a law enforcement or government agency, or in response to a formal request in a civil action that on its face meets the requirements for such a request.

Other
You must have valid and current information on file with your domain name registrar for any domain hosted on the Network. You may only use IP addresses assigned to you by Connectria staff in connection with your Connectria services. You may not take any action which directly or indirectly results in Connectria IP space being listed in any of the various abuse databases.

Consequences of Violation of AUP
Without limiting any other right or remedy Connectria may have, the methods of resolution below will typically form the framework for resolving violations of Connectria's AUP. Timing for resolution differs according to the degree of the violation, the nature of the violation, involvement of law enforcement, involvement of third party litigation, or other related factors. Overall, Connectria is dedicated to working with you in resolving all potential violations prior to any service interruptions.

Step 1: First notice of alleged or actual AUP violation: A support ticket is generated within the Connectria Customer Portal under the primary user account with information regarding the alleged or actual violation of the AUP. This may be a fact-finding message that requests further information or notification to you of an alleged or actual violation and the required actions you must take to resolve the issue.

Step 2: Second notice of alleged or actual AUP violation: If a support ticket has been disregarded, not properly addressed, or not resolved by you within the specified period of time requested by Connectria, Connectria's staff will disable access to the Network for the specified Services. If the violation is addressed within an acceptable period of time as determined in Connectria's sole discretion, Network access to the Services will be restored and will continue as normal.

Step 3: Suspension of Services: If you fail to address the violation and/or resolve the violation, a Suspension of Services will occur. This is a last resort for Connectria and requires a complete failure in the resolution process on your part. Connectria will, in its sole discretion determine, whether a Suspension of Services is permanent or temporary. In either case, a Suspension of Services may include reclamation of all Services. All content and/or data used in the Services will be destroyed upon reclamation. Customer understands and agrees that Connectria

assumes no liability whatsoever, either express or implied, for any lost data or lost use of the Services due to Suspension of Service. No service credits will be issued for any interruption in service resulting from violations of this AUP.

The aforementioned list of actions shall not be construed in any way to limit the actions or remedies that Connectria may take to enforce and ensure compliance with this AUP. Connectria reserves the right to recover any and all expenses, and apply any reasonable charges, in connection with a Customer's violation of this AUP. While Connectria will attempt to follow the procedures listed above, Connectria may, without notice to you, suspend your service and/or remove any content transmitted via the Services and/or Network if Connectria discovers facts that lead it to reasonably believe your service is being used in violation of this AUP. You must cooperate with Connectria's reasonable investigation of any suspected violation of the AUP. Connectria will attempt to contact you prior to suspension of network access to your server(s), however, you understand and agree that prior notification by Connectria is not assured nor required. Connectria reserves the right at all times to investigate any actual, suspected, or alleged violations of this AUP, with such investigation to include accessing of data and records on, or associated with, the Services.

Except as otherwise expressly provided under the Agreement, you are solely responsible for the use of the Services and Network in violation of this AUP including, without limitation, (a) use by your customers and (b) any unauthorized use. Connectria may charge you (and you agree to pay) Connectria's hourly rate (the "Connectria Security Rate") to correct any violation of this AUP or to repair any security breach (currently $195.00 billed in one-hour minimum increments), plus the cost of equipment and materials, if needed, to: (w) investigate, correct or otherwise respond to any violation or suspected violation of this AUP, (x) remedy any harm caused to Connectria or any of its customers by the use of your service in violation of this AUP, (y) respond to complaints, and (z) have Connectria's Internet Protocol numbers removed from any "blacklist" such as SPEWs or other abuse databases. If Connectria's administrative accounts are disabled or demoted from Administrator or Root accounts, you understand that in addition to any other remedies available to Connectria, you will be charged the hourly Connectria Security Rate to correct this situation, and no support can be provided to you without these accounts being enabled. Connectria retains the right, at its sole discretion, to refuse new service to any individual, group, or business. Connectria also retains the right to discontinue service with notice for repeated violations of this AUP over time.

Security and Disclaimer
You must take reasonable security precautions in light of your use of the Services and/or Network. You are solely responsible for any breaches of security affecting the servers under your control, unless a security breach is directly caused by the

willful misconduct by Connectria. You must protect the confidentiality of your password(s), and you should change your password(s) periodically. A compromised server is potentially disruptive to Connectria's network and other customers. Therefore, Connectria may take your server off line if it is accessed or manipulated by a third party without your consent.

Connectria has no responsibility for any material or information created, stored, maintained, transmitted or accessible on or through the Services or Network and is not obligated to monitor or exercise any editorial control over such material. In the event that Connectria becomes aware that any such material may violate this AUP and/or expose Connectria to civil or criminal liability, Connectria may block access to such material and suspend or terminate any Services without liability. Connectria further reserves the right to cooperate with legal authorities and third parties in investigating any alleged violations of this AUP, including disclosing the identity of any User that Connectria believes is responsible for such violation. Connectria also reserves the right to implement technical mechanisms to prevent AUP violations. Nothing in this AUP shall limit in any way Connectria' rights and remedies at law or in equity that may otherwise be available. Connectria is under no duty, and does not by this AUP undertake a duty, to monitor or police our customers' activities and disclaims any responsibility for any misuse of the Connectria network. Connectria disclaims any obligation to any person who has not entered into an agreement with Connectria for services.

Subscription Software Provided by Connectria
We may provide software to you on a monthly basis (the "Subscription Software") from Microsoft, RedHat, or VMware, among others (the "Subscription Software Vendors"). By utilizing any Subscription Software provided by us, you agree to utilize such Subscription Software according to such Subscription Software Vendor's licensing terms and conditions. Should a Subscription Software Vendor change its Subscription Software products, business model, licensing terms, or costs to us, you agree that (a) we may modify the Subscription Software we can provide to you and how we can provide it to you and (b) we may revise our Subscription Software offerings and our fees and costs to you with 30 days notice to you. Should you not agree to our revised Subscription Software offerings or fees, you may terminate your use of such Subscription Software according to the terms of any written agreement between you and Connectria.

Policy, Notices and Procedures Regarding Claims of Copyright Infringement
Connectria respects the intellectual property right of others, and we ask our customers to do the same. We respond to notices of alleged copyright infringement in accordance with the procedures protecting service providers set forth in the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512 (the text of which can be found at the U.S. Copyright Office Web Site, http://www.copyright.gov/).

Designation of Registered Agent
Pursuant to Title 17, United States Code, Section 512(c)(2), Connectria designates Rusty Putzler as its agent designated to receive notifications of claimed copyright infringement ("Copyright Agent"). The address of the Copyright Agent is:

Connectria Hosting
Attention Rusty Putzler
10845 Olive Blvd. – Suite 300
St. Louis, Missouri 63141 U.S.A.

The telephone number of the Copyright Agent is (314) 549-8988. The facsimile number of Copyright Agent: (314) 587-7090. The email address of the Copyright Agent is copyright@connectria.com.

Notification of Claimed Infringement
If you believe that your work has been copied in a way that constitutes copyright infringement, please provide our Copyright Agent (as designated above) with written notice at the postal, email, and/or facsimile address above that includes all of the following information:

1. A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that has allegedly been infringed.
2. Identification the copyrighted work that you claim has been infringed (e.g., "The copyrighted work at issue is the text that appears on www.companyname.com").
3. Identification of the material that you believe infringes your copyrighted work, and provide sufficient detail to allow Connectria to locate the material (e.g., any URL's, file names or other identifying information). If some but not all of the material on any given web page allegedly infringes your rights, please specifically identify which material is infringing.<
4. Information reasonably sufficient for us to contact you such as your address, telephone number and e-mail address.
5. A statement by you that you have a good faith belief that the use of the material in the manner complained of is not authorized by the copyright property owner, its agent, or the law.
6. A statement by you, made under penalty of perjury, that the information in the notice is accurate and that you are authorized to act on behalf of the copyright owner of an exclusive right that has been infringed.

Termination of Services
Connectria may terminate the account of any customer of Connectria, if Connectria believes that such customer is infringing the intellectual property rights of others or is aiding or threatening such infringement.

Contact
Please direct all questions regarding this AUP to info@connectria.com.