

---

## Cirion's Acceptable Use Policy

Effective August 2022

This Acceptable Use Policy ("AUP") defines acceptable practices relating to the use of Cirion's network, websites, systems, facilities, products and services (collectively, the "Services") by Cirion customers and by users that have gained access to the Services through customer accounts (collectively, "Users"). The Services must be used in a manner that is consistent with the intended purpose of the Services and the terms of the applicable agreement with Cirion. By using the Services, Users consent to be bound by the terms of this AUP. For purposes of this AUP, "Cirion" includes all other affiliates, including direct and indirect subsidiaries of Cirion Technologies Solutions, LLC.

### Prohibited Conduct

- **General.** Users will not use the Services to transmit, distribute or store material in a manner that: (a) violates any applicable law or regulation; (b) may adversely affect the Services or Users; (c) may expose Cirion to criminal or civil liability or (d) violate, infringe upon or otherwise misappropriate any third-party rights, including intellectual property rights, rights of publicity and privacy rights. Users are prohibited from facilitating the violation of any part of this AUP or applicable third-party policies, including, but not limited to transmitting, distributing, or otherwise making available any product or service that violates this AUP or another provider's policy.
- **Inappropriate Content.** Users will not use the Services to transmit, distribute or store material that Cirion reasonably determines is inappropriate, obscene, indecent, defamatory, libelous, tortious, threatening, abusive, hateful, or excessively violent. Users will also not use the Services to host terrorist-related web sites, including sites that advocate human violence and hate crimes based upon religion, ethnicity, or country of origin.
- **Intellectual Property.** Material accessible through the Services may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users will not use the Services in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights. If a domain name is used with any of the Services, it may not be used in violation of the trademark, service mark, or other rights of any third party.
- **Harmful Content.** Users will not use the Services to transmit, distribute or store material that may be harmful to or interfere with the Services or any third party's networks, systems, services, or websites. Such prohibited harmful content includes, but is not limited to, viruses, worms, or Trojan horses, root kits, password crackers, adware, and key stroke capture programs.
- **Fraudulent/Misleading Content.** Users will not use the Services to transmit or distribute material containing fraudulent offers for goods or services, or any advertising or promotional materials that contain false, deceptive, or misleading statements, claims, or representations. In addition, Users are prohibited from submitting any false or inaccurate data on any order form, contract or online application, including the fraudulent use of credit cards.
- **Email and Unsolicited Messages.** Users will not use the Services to (i) transmit unsolicited e-mail messages, including, without limitation, unsolicited bulk email, where

such emails could reasonably be expected to provoke complaints, and (ii) send e-mail messages which are excessive and/or intended to harass or annoy others ("Spam"). Further, Users are prohibited from using the service of another provider to send Spam to promote a site hosted on or connected to the Services. In addition, Users will not use the Services to (a) continue to send e-mail messages to a recipient that has indicated that he/she does not wish to receive them, (b) send e-mail with forged TCP/IP packet header information, (c) send malicious e-mail, including, without limitation, "mail-bombing", (d) send or receive e-mail messages in a manner that violates the use policies of any other Internet service provider, or (e) use an e-mail box exclusively as a storage space for data.

- **Third-Party Rules; Usenet.** Users will not use the Services in violation of the rules, guidelines or agreements associated with search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, or other services accessed via the Services.
- **Inappropriate Actions.** Users will not use the Services to conduct activities that may be harmful to or interfere with the Services, a user's terminal session or any third party's networks, systems, services, or websites. Users will not engage in any activities designed to harass, or that will preclude or interfere with the use of Service (e.g., synchronized number sequence attacks) by any other User on the Cirion network or on another provider's network. In addition, Users will not use the Service (a) by any means or device to avoid payment; (b) to access User's account or Cirion Services after User has terminated User's account; (c) on behalf of persons or firms listed in the Spamhaus Register of Known Spam Operations database at [www.spamhaus.org](http://www.spamhaus.org); or (d) to engage in phishing activities. Users will not use the Service to engage in any activities that may interfere with the ability of others to access or use the Service or the Internet.
- **Illegal Use:** Customer will not use the Services in a manner that constitutes illegal activities, including but not limited to, death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, HYIP or Ponzi schemes, invasion of privacy, credit card fraud, racketeering, defamation, slander, child pornography and violations of the Child Protection Act of 1984, or any other applicable law.
- **Security Breaches and Obligations.** Users are prohibited from violating or attempting to violate the security of the Services or the computers, accounts, or networks of another party, including but not limited to, circumventing the user authentication or security of any host, network or account. Users will not use the Services to cause security breaches or disruptions of Internet communication and/or connectivity. Security breaches include, but are not limited to, accessing data, accounts or systems without authorization or logging into a server or account that the Customer is not expressly authorized to access and denial of service attacks. Disruptions include port scans, flood pings, email-bombing, packet spoofing, IP spoofing, forged routing information. Customer must use reasonable care in keeping its software on the Cirion's servers up-to-date and patched with the latest security updates.
- **IP Allocation.** Users are prohibited from using IP addresses not originally allocated for use or on unassigned VLANs or servers. All IP Addresses are currently owned and registered to Cirion and are non-transferable. Customer retains no ownership or transfer rights.

## Rights of Cirion

- Cirion may suspend or terminate Service of any User which Cirion believes has violated any element of this AUP. Cirion will suspend Service for violation of the AUP on the

most limited basis as Cirion determines is reasonably practical under the circumstances to address the underlying violation. Cirion will attempt to notify Users via email or other method prior to suspending Service for violation of the AUP; provided, however, Cirion may suspend Service without notice if Cirion becomes aware of a violation of any applicable law or regulation or activity, including but not limited to a violation of the AUP that exposes Cirion to criminal or civil liability or that exposes the Cirion network or Cirion customers' network or property to harm. Such harm to a network may include, but is not limited to, risk of having an IP address placed on blacklists. Cirion may take such further action as Cirion determines to be appropriate under the circumstances to eliminate or preclude repeat violations.

- Cirion reserves the right to take down any material—or otherwise block access thereto—created or accessible on or through the Services and suspend or terminate any User creating, storing or disseminating such material where Cirion becomes aware that the material violates this AUP and/or exposes Cirion to civil or criminal liability, including without limitation, under applicable copyright laws. Cirion reserves the right to avail itself to the safe harbor provisions of the Digital Millennium Copyright Act.
- Access the [Service Provider/Designated Agent Information](#) pursuant to the Digital Millennium Copyright Act, 17 U.S.C., Section 512(c).
- Users are responsible for configuring their own systems to provide the maximum possible accountability. Cirion shall not be liable for any damage caused by such system configurations regardless of whether such configurations have been authorized or requested by Cirion. For example, Users should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. Users should also configure their Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange and should generally present header data as clearly possible. As another example, Users should maintain logs of dynamically assigned IP addresses. Users are responsible for educating themselves and configuring their systems with at least basic security. Should systems at a user's site be violated, the User is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) Server, the User is responsible for re-configuring the system to stop the abuse.
- Cirion reserves the right to cooperate with legal authorities and third parties in the investigation of any alleged wrongdoing related to this AUP, including the disclosure of the identity of the User that Cirion deems responsible for the wrongdoing. Cirion will not be liable for any damages of any nature suffered by any User, or any third party resulting in whole or in part from Cirion's exercise of its rights under this AUP.
- Cirion reserves the right to install and use, or to have you install and use, any appropriate devices to prevent violations of this Policy, including devices designed to filter or terminate access to the Service. By accepting and using the Service, Users consent to allowing Cirion to collect service information and routing information in the normal course of our business, and to use such information for general business purposes. Users may not use the Service to monitor any data, information or communications on any network or system without authorization. Users may not attempt to gain unauthorized access to the user accounts or passwords of other Users.
- In most cases, Cirion will notify Users of complaints received by Cirion regarding an alleged violation of this Policy. You agree to promptly investigate all such complaints and take all necessary actions to remedy any violations of this Policy. Cirion may inform the complainant that you are investigating the complaint and may provide the complainant with the necessary information to contact you directly to resolve the complaint. You shall identify a representative for the purposes of receiving such communications.

- Cirion reserves the right to modify this AUP in its discretion at any time. Such modifications will be effective upon posting, and use of the Services after such modification constitutes acceptance of such modifications.

### **Responsibility for Content**

Cirion takes no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. Cirion is not obligated to monitor such material but reserves the right to do so.