Aruba Services User Policy

Recitals

Failure to comply with this AUP will result in the immediate suspension or interruption of the service in accordance with the corresponding conditions of supply. All requests for information regarding the content of this document must be addressed by opening a specific ticket on the page https://assistenza.aruba.it/home.aspx.

List of articles

1. Breaches

It is forbidden to use the Aruba network and services to engage in and/or promote illegal, abusive or irresponsible behaviour, such as:

The following are prohibited, amongst other things:

- unauthorised access to or use of data, systems or networks, including any attempt to examine or test the vulnerability of a system or network or to breach security or authentication measures without the express permission of the owner of the system or network;
- any misuse of the service(s), including those described on the "Report Abuse" page, aimed at:
  1) the publication and/or distribution of inappropriate or intimidating content, the use and/or dissemination of any false, misleading or deceptive information, including by email or via newsgroups;
  2) the creation of phishing and/or spam campaigns or, more generally, unwanted messages;
  3) the distribution of malware and/or viruses;
  4) copyright/brand/trademark infringement;
  5) engaging in and/or facilitating identity theft;
  6) carrying out and/or facilitating cyberattacks on the confidentiality, integrity or availability of the data or infrastructure of Aruba and/or third parties;
  7) violating and/or circumventing any national and international legislation;
- engaging in or attempting computer fraud; creating situations of danger and/or instability and/or other problems of a technical nature as a result of programming activities and/or methods of use that impact on the quality of the service of the customer or other users, causing damage to them, to Aruba and/or to third parties;
- the collection or use of email addresses, names or other identifiers without the consent of the person concerned (including but not limited to: spamming, phishing, internet scams, password theft, spidering);
- the collection or use of third party information without the necessary authorisation;

- the processing of personal data of third parties in an unlawful manner or in any case in violation of Regulation (EU) 2016/679 and the legislation on the processing of personal data;
- use of the service for the distribution of software that fraudulently collects information about a user or fraudulently transmits information about the user;
- use of the service for the distribution of so-called "adware", unless: (i) it has the user's explicit consent to download and install the software on the basis of a clear and clearly visible notice about the nature of the software; (ii) it is software that can be easily removed with the use of standard tools for this purpose, included in the main operating systems (such as, for example, Microsoft "ad blockers");
- using Aruba services to offer anonymous communication systems, without adequate maintenance of identity as required by current legislation, such as, but not limited to, so-called "TOR" or "anonymiser";
- accessing Aruba services from untrusted networks such as, but not limited to, so-called "TOR" or "anonymiser".
- constituting, depicting, encouraging, promoting or referring in any way to paedophilia, racism, fanaticism, terrorism, or pornography content that does not comply with current regulations on the subject and accessible only to people of legal age.

2. Handling of breach reports

In accordance with the provisions of the Digital Services Act (Reg. (EU) 2022/2065), all users will have the opportunity to report possible violations detected in connection with the use of Aruba services, through the following "Report abuse" channel or the corporate channels specified on the "About us" page.

How to report a breach

All users may proceed to report a detected breach through the Aruba services, taking care to provide the following details:

- an adequately argued explanation of the facts for which it is assumed that what is reported is against the law;
- a precise indication of the exact electronic location in relation to the reported content, for example the exact address or URLs or additional information that allows identification of the illegal content appropriate to the type of content and the specific type of information storage service;
- all the information required in the specific form on the "Report abuse" page.
- a statement whereby the person or entity submitting the report confirms its belief, in good faith, regarding the accuracy and completeness of the information and statements contained therein.

Management of reports

A notification will be sent to the reporting party for all reports and these will be promptly managed by informing the parties involved of the findings regarding the decisions taken in reference to the subject of the report and executing what is within our competence in accordance with Italian Legislative Decree 70/2003.

Option to file a complaint

The customer who is the owner of the services that are the subject of the report may submit a complaint on the basis of the provisions in the manner indicated in the General Conditions of Services published on the Aruba.it website or via the service area.

3. Use of the system resources

The user may neither use the service in a way that interferes with the normal operation of Aruba's services nor make improper use of system resources such as, but not limited to, using software that saturates the performance capacity of the network, disk system and CPU on a shared platform (e.g. cloud, hosting, email, etc.) for extended periods of time, except for services offered by Aruba that are dedicated or with a 100% guarantee (such as dedicated servers and private clouds).

In such circumstances, Aruba may request that the level of normal operation be restored if, at its sole discretion, such non-compliant use conflicts with the use of other users.

The user undertakes not to use defective or non-approved equipment in accordance with European standards, or that has malfunctions that may damage the integrity of the network and/or disturb services and/or create risks for the physical safety of people.

Aruba does not provide any guarantee concerning the compatibility of the equipment and programs (hardware and software) used by the customer with the service, as all related checks are the sole responsibility of the customer.

Aruba S.p.A.
Via San Clemente no. 53, Ponte San Pietro 24036 (BG)
V.A.T. number 01573850516 | **Tax ID No.** 04552920482
REA BG 434483 | **ShareCapital**. €4,000,000 fully paid up |
Certified email aruba@aruba.pec.it | **Website** aruba.it

Furthermore, the user must use any web space purchased from Aruba solely for the publication of the website and not as a repository, i.e. as a tool for the mere storage of its files and/or movies/videos and/or own material and/or for material that can also be downloaded from other sites.

4. Commercial emails

The dissemination of commercial messages is prohibited if it is not possible to demonstrate that:

- recipients have given their prior free and specific consent to receive email through an express opt-in

procedure (without prejudice to the cases provided for by law where such consent is not necessary, e.g. soft spam);

- the consent collection procedures include appropriate tools for ensuring that the person who has given their consent is the holder of the receiving email address;
- evidence of the recipient's consent in a form that can be readily produced upon request is retained, at the expense of the recipient of Aruba's requests, in this regard, to produce such evidence, within 72 hours of receipt of the request;
- procedures are in place that allow a recipient to withdraw their consent, such as, but not limited to, a link in the body of the email or instructions to reply with the word "Remove" in the subject line, and it is possible to comply with the withdrawal of consent within 48 hours of receipt, informing recipients that the withdrawal of their consent will be processed within a maximum of 48 hours;
- an email address for complaints is always highlighted in a clearly visible place on each website associated with the email and messages sent to that address are promptly found.

It is not permissible to hide the sender of the email in any form. The sender email address must appear in the body of the message or in the "From" line of the email.

These provisions apply to messages sent through the service or to messages sent from any network by the user or any person acting on its behalf that directly or indirectly relates to the recipient of a site hosted through the services.

In addition, you will not be able to use a “third party” email service that does not apply similar procedures to all of its customers. These requirements shall apply in the same way to distribution lists created by third parties as if the list had been created by the customer.

Aruba reserves the right to verify and monitor compliance with the provisions listed above at any time, which includes requesting sample information by the opt-in method. Aruba may suspend the sending of e-mail messages that breach these provisions.

5. SMTP Authentication - Policy

In complement to the above provisions, it will not be permissible to send email messages of similar content to more than one hundred and fifty (150) recipients through the Aruba SMTP servers, except for the PEC service, for which there is a limit of five hundred (500) recipients. Attempts to circumvent this limit by creating multiple accounts or by any other means will be deemed a breach of this restriction and this policy.

Aruba reserves the right to suspend the sending of messages that breach these provisions. In addition, mail services may be suspended or interrupted if a breach of this AUP is found, in accordance with the general conditions of supply.

6. Mail Relay

In general, mass sending or the sending of commercial information by email to more than 8,000 (eight thousand) recipients per day are not permitted, with limitation thresholds at increasing intervals. To send more than 8,000 messages per day, please contact our support team for more information.

7. Vulnerability Testing

The user may not attempt, examine, penetrate or test the vulnerability of the Aruba network system or breach the security of Aruba or its authentication procedures using either passive or invasive techniques without Aruba's express written consent, nor may they carry out said activities through the service provided by Aruba to third-party networks and/or information without their express consent.

8. Newsgroups, discussion forums, other networks

The customer acknowledges and accepts that the contents of commercial messages, messages on any electronic bulletin board, group chat or other forums in which the customer participates, such as, but not limited to, IRC and USENET groups, will be subject to compliance with the laws and regulations in force.

The customer must also comply with the rules of any other network (network or circuit) which it accesses or in which it participates using the Aruba services.

9. Offensive content

It is prohibited to publish, transmit or store on or through the Aruba network and devices any content or links to content that Aruba reasonably believes:

- to constitute, depict, encourage, promote or refer in any way to paedophilia, racism or pornography content that does not comply with current regulations on the subject and is accessible only to people of legal age;
- to be excessively violent, incite violence, contain threats, harassment or hate speech;
- to be unfair or misleading in relation to the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
- to be defamatory or violate a person's privacy;
- to create a risk to personal safety or health, a risk to public safety or public health, to compromise national security or to interfere with investigations by the judicial authority;
- to improperly disclose trade secrets or other confidential or proprietary information belonging to third parties;
- to have the purpose of helping third parties circumvent copyright regulations;
- to infringe the copyrights of third parties, and the trademarks, patents or other proprietary rights of others;
- to refer to (or present links to) gambling and/or online casinos, to promote illegal drugs, or to violate laws controlling exports, illegal gambling or illegal arms trafficking;
- to be otherwise unlawful or to solicit unlawful conduct under applicable laws in the relevant jurisdiction of Aruba's customer;
- to be otherwise harmful, fraudulent or capable of bringing legal action against Aruba.

Content “posted or transmitted” via the Aruba network or infrastructure includes web content, email, chat, and any other type of publication or transmission that is internet based.

10. Copyrighted material

It is forbidden to use the Aruba network to download, publish, distribute, copy or use in any way any text, music, software, art, image or other work protected by copyright except in the case where:

- it has been expressly authorised by the copyright holder;
- it is otherwise permitted by applicable copyright laws in the relevant jurisdiction.

11. Final provisions

The customer undertakes to provide Aruba with the personal data necessary for the full and correct execution of the contract; he also gives an assurance, under his own personal and exclusive responsibility, that the aforementioned data are always correct, up-to-date and truthful and that they allow his true identity to be identified.

The customer undertakes to inform Aruba of any change in the data provided, promptly and in any case no later than 15 (fifteen) days from the occurrence of the aforementioned change, and to provide Aruba, at the latter's request at any time, with adequate proof of their identity, domicile or residence and, where appropriate, their capacity as legal representative of the requesting legal entity or holder of the service.

Upon receipt of the aforementioned communication, Aruba may ask the customer for additional documentation aimed at demonstrating the changes reported. If the customer fails to send Aruba the aforementioned communication or the requested documentation, or if they have provided Aruba with data that is false, outdated or incomplete or data that Aruba has reason, in its sole discretion, to consider as such, Aruba reserves the right to:

a) reject the customer's request concerning operations to be carried out in reference to the service;
b) suspend the services with immediate effect, without notice and for an indefinite period;
c) to cancel and/or interrupt, without notice, any operations for modifying the data associated with the service;
d) to terminate the contract.

The customer accepts that if the public IP addresses assigned to their account are included on a blacklist (abuse database) such as that onwww.spamhaus.org, this AUP will be automatically breached; consequently, Aruba may take all measures it deems appropriate for protecting its IPs, including suspension and/or termination of the service, regardless of whether the IPs have been reported/blacklisted for reasons attributable to the customer.

The customer agrees that data stored on a shared system may be quarantined or deleted if such data is infected with a virus or otherwise corrupted, and has, at Aruba's sole discretion, the potential to infect or damage the system or data of other customers that are placed on the same infrastructure.

The customer undertakes to observe the rules of proper use of network resources commonly referred to as "Netiquette".

12. SLA

No refund under Aruba's Service Level Agreement, when present, will be granted for service interruptions resulting from breaches of this AUP.