Aruba Service Usage Policy

Introduction

Failure to comply with this AUP will result in the immediate suspension or termination of the service in accordance with the relevant terms and conditions of service. All enquiries regarding the content of this document should be directed by opening a support ticket via the assistenza.aruba.it page.

Table of Contents

1. Violations

It is prohibited to use the Aruba network and services to engage in and/or promote conduct that is unlawful, abusive or irresponsible, such as, for example:

The following, amongst others, are prohibited:

- 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 authorisation of the system or network owner;
- 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, or the use and/or dissemination of any false, misleading or deceptive information, including via email or newsgroups;
  2) the creation of phishing and/or spam campaigns or, more generally, unsolicited messages;
  3) the distribution of malware and/or viruses;
  4) the infringement of copyright/brand/trademark rights;
  5) to commit and/or facilitate identity theft;
  6) to carry out and/or facilitate cyber attacks on the confidentiality, integrity or availability of data or the infrastructure of Aruba and/or third parties;
  7) violating and/or circumventing any national or international legislation;
- committing or attempting cyber fraud; creating situations of danger and/or instability and/or other technical problems as a result of programming activities and/or methods of use that impact the quality of service for the customer or other users, causing harm 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 third-party personal data unlawfully or in any case in breach of EU Regulation 2016/679 and the legislation governing the processing of personal data;
- the use of the service to distribute software that fraudulently collects information about a user or fraudulently transmits information about the user;
- the use of the service to distribute so-called “adware” software unless: (i) the user has given their explicit consent to the download and installation of the software on the basis of a clear and prominent notice regarding the nature of the software; (ii) the software is easily removable using standard tools for that purpose, included in the main operating systems (such as, for example, Microsoft "Add/Remove");
- using Aruba services to offer anonymous communication systems without adequate maintenance of identities as required by current legislation, such as, by way of example but not limited to, so-called "TOR" or "anonymizers";
- access Aruba services from untrusted networks such as, by way of example but not limited to, so-called “TOR” or “anonymizers”.
- to create, depict, encourage, promote or refer in any way to paedophilia, racism, fanaticism, terrorism, or pornographic content that is not published in accordance with the relevant legislation in force and accessible only to adults.

2. Management of reports of violations of the

In accordance with the provisions of the Digital Services Act (Reg. EU 2022/2065), all users will be able to report any suspected violations relating to the use of Aruba’s services via the “Report abuse” channel or the official channels listed on the “About us” page.

How to report a violation

All users may report a violation detected via Aruba services, taking care to include the following details:

- a properly substantiated explanation of the facts on which the presumption that the reported matter is contrary to the law is based;
- a precise indication of the exact electronic location of the reported content, such as, for example, the exact URL address or addresses, or additional information enabling the identification of the relevant illegal content the type of content and the specific type of data storage service;
- all the information requested in the specific form on the page: "Report abuse"
- a statement in which the person or entity submitting the report confirms their belief, in good faith, regarding the accuracy and completeness of the information and statements contained therein.

Handling of reports

For all reports, the reporter will be notified that the matter has been taken on board, and the reports will be handled promptly by informing the parties involved of the findings regarding the decisions taken in relation to the subject of the report and by carrying out our duties in accordance with Legislative Decree 70/2003.

Right to complain

The customer to whom the services covered by the report are registered may always lodge a complaint in accordance with the procedures set out in the General Terms and Conditions of Service published on the Aruba.it website or via the support area.

3. Use of system resources

The user must not use the service in a manner that interferes with the normal operation of Aruba’s services, nor must they misuse system resources, including, but not limited to, the use of software that overloads the performance capacity of the network, the disk system and the CPU on a shared platform (e.g. cloud, hosting, email, etc.) for prolonged periods, except for those services offered by Aruba in a dedicated format or with a 100% guarantee (such as dedicated servers and private clouds).

In such circumstances, Aruba may request that normal usage levels be restored if such non-compliant use, in Aruba’s sole discretion, conflicts with the usage of other users.

The user undertakes not to use equipment that is defective or not certified in accordance with European standards, or that has faults which could compromise the integrity of the network and/or disrupt services and/or pose a risk to the physical safety of persons.

Aruba S.p.A.
53 Via San Clemente, Ponte San Pietro 24036 (BG)
VAT No. 01573850516 | **Tax Registration No.** 04552920482
REA BG 434483 | Share Capital €4,000,000 fully paid up | **Certified**

Aruba, in fact, gives no guarantee regarding the compatibility of the equipment and programmes (hardware and software) used by the customer with the service, as all related checks are the sole responsibility of the customer.

Furthermore, the user must use the web space, if purchased from Aruba, exclusively for the publication of the website and not as a repository, i.e. as a tool for the mere storage of files and/or films/videos and/or their own material and/or material downloadable from other sites.

4. -commercial emails

The sending of commercial messages is prohibited unless it can be demonstrated that:

- the recipients have given their prior, free and specific consent to receive email via an explicit opt-in procedure (except in cases provided for by law where such consent is not required, e.g. soft spam);
- the consent collection procedures include appropriate measures to ensure that the person who has given their consent is the owner of the recipient email address;
- evidence of the recipient's consent is retained in a form that can be readily produced upon request, with the recipient bearing the burden of providing such evidence in response to Aruba's requests within 72 hours of receiving the request;
- procedures are in place to enable a recipient to withdraw their consent, such as, by way of example and without limitation, a link within the body of the email or instructions to reply with the word "Unsubscribe" in the subject line, and that the organisation is able to comply with the withdrawal of consent within 48 hours of receipt, informing recipients that the withdrawal of their consent will be processed within 48 hours at the latest;
- An email address for complaints must always be clearly displayed in a prominent position on every website associated with the email, and messages sent to that address must be dealt with promptly.

It is not permitted to conceal the sender of the email in any way. The sender's email address must appear in the body of the message or in the 'From' field of the email.

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

Furthermore, it will not be possible to use a third-party email service that does not apply similar procedures to all its customers. These requirements will apply equally 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, including by requesting information on a random basis via an opt-in method. Aruba may suspend the transmission of emails that breach these provisions.

5. SMTP Authentication - Policy

In addition to the provisions set out above, it is not permitted to send emails with similar content to more than one hundred and fifty (150) recipients via Aruba's SMTP servers, with the exception of the PEC service, for which the limit is five hundred (500) recipients. Any attempts to circumvent this limitation by creating multiple accounts or by any other means shall be deemed a breach of this restriction and of this policy.

Aruba reserves the right to suspend the transmission of messages that violate these provisions. Furthermore, email services may be suspended or terminated should a breach of this AUP be identified, in accordance with the general terms and conditions of service.

6. -Relay Mail

In general, mass mailings or the transmission of commercial information via email to more than 8,000 (eight thousand) recipients per day are not permitted, with increasing volume limits. If you wish to send more than 8,000 messages per day, please contact our support team for further information.

7. vulnerability testing

The user must not, under any circumstances, attempt to examine, penetrate or test the vulnerability of Aruba's network system, or breach the security of Aruba or its authentication procedures, whether through passive or invasive techniques, without Aruba's express written consent; nor, similarly, may the user carry out such activities via the service provided by Aruba in relation to third-party networks and/or information without their explicit consent.

8. Newsgroups, discussion forums, other web r networks

The customer acknowledges and accepts that the content of commercial messages, messages on any electronic bulletin board, group chat or other forums in which they participate, including but not limited to IRC and USENET groups, shall be subject to compliance with the applicable laws and regulations.

Furthermore, the user must comply with the rules of any other network (or circuit) they access or participate in whilst using Aruba's services.

9. Offensive or in t content

It is prohibited to publish, transmit or store on or via the Aruba network and equipment any content or links to content that Aruba reasonably considers to:

- constitute, depict, encourage, promote or refer in any way to paedophilia, racism or pornographic content that is not posted in compliance with applicable regulations and accessible only to adults;
- be excessively violent, incite violence, contain threats, harassment or expressions of hatred;
- be unfair or deceptive in relation to consumer protection laws in any jurisdiction, including chain letters and pyramid schemes;
- be defamatory or infringe upon a person's privacy;
- pose a risk to personal safety or health, a risk to public safety or public health, compromise national security or interfere with investigations by the judicial authorities;
- improperly disclose trade secrets or other confidential or proprietary information belonging to third parties;
- be intended to assist third parties in circumventing copyright;
- infringe the copyright, trademarks, patents or other proprietary rights of third parties;
- refer to (or provide links to) online gambling and/or casinos, promote illegal drugs, or violate laws relating to export controls, illegal gambling or illegal arms trafficking;
- be otherwise unlawful or encourage unlawful conduct under the applicable laws of the customer's or Aruba's relevant jurisdiction;
- be otherwise harmful, fraudulent or likely to result in legal action against Aruba.

Content "published or transmitted" via Aruba's network or infrastructure includes web content, emails, chats and any other type of publication or transmission based on the internet.

10. r copyright-protected material

It is prohibited to use the Aruba network to download, publish, distribute, copy or use in any way any text, music, software, art, images or other works protected by copyright, except where:

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

11. r final provisions

The customer undertakes to provide Aruba with the personal data necessary for the full and proper performance of the contract; the customer further guarantees, under their own personal and exclusive responsibility, that the aforementioned data is always correct, up to date and truthful, and that it enables their true identity to be established.

The customer undertakes to notify Aruba of any changes to the data provided, promptly and in any event no later than 15 (fifteen) days from the occurrence of such change, and also to provide, at any time upon Aruba's request, adequate proof of their identity, domicile or residence and, where applicable, of their capacity as the legal representative of the legal entity requesting the service or the service holder.

Upon receipt of the aforementioned notification, Aruba may request additional documentation from the customer to verify the changes reported. In the event that the customer fails to provide Aruba with the aforementioned notification or the requested documentation, or in the event that they have provided Aruba with data that proves to be false, out of date or incomplete, or data that Aruba has reason, at its sole discretion, to believe to be such, Aruba reserves the right to:

a) to reject the request submitted by the customer regarding operations to be carried out in relation to the service;
b) suspend the services with immediate effect, without notice and for an indefinite period;
c) cancel and/or suspend, without notice, any operations to modify data associated with the service;
d) terminate the contract.

The customer accepts that should the public IP addresses assigned to their account be included in a blacklist (abuse database) such as that found at www.spamhaus.org, this will constitute an automatic breach of this AUP; Consequently, Aruba may take all measures deemed appropriate to protect its IP addresses, including the suspension and/or termination of the service, regardless of whether the IP addresses have been reported/blacklisted for reasons attributable to the customer.

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

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

12. SLA

No refunds provided for in Aruba's "Service Level Agreement", where applicable, will be granted for service interruptions resulting from breaches of this AUP.