Responsible Use Policy

1. Objective

The Responsible Use Policy (RUP) defines, in addition to current legal obligations and any specific contractual obligations, the rights and duties of Ar customers who use Internet access services, web hosting and other related IT services, with the aim of protecting their interests and those of Ar.
The RUP is non-contractual and its updated version is available on the Ar website.
The PUR may be revised periodically by Ar without prior notice to customers.
If Ar detects a violation of the PUR rules, it reserves the right to remove and/or disable access to illegal content or any other content that similarly constitutes a violation of the policy or hinders the normal functioning of the services provided.
For failure to comply with any obligations arising from the PUR, the customer shall be liable to compensate Ar, under the general terms of law.
Ar cannot be held liable for any breach by its customers of any rights or duties provided for in the PUR.

2. Scope

The policy applies to all Ar customers.

3. Policy

a. Internet Access Service

- The contracting of the Internet access service presupposes a reasonable level of use by each user in order to ensure a high quality of service for all customers.
- The contracted Internet access speeds are the maximum speeds for use by customers. However, download and upload speeds may vary depending on the type of connection used, computer configuration, applications being run, Internet traffic congestion, and the performance and access speed of the servers hosting the sites and content to be accessed. Whenever situations are detected that negatively impact the quality of services provided over the network, Ar may reduce access speeds in order to ensure high quality service for all customers.
- If Ar detects that a customer is downloading and/or uploading large files, *streaming* or performing other actions that may have a negative impact on the quality of the services provided over the network, it will inform the customer of this fact and may suspend the service under the applicable terms and conditions of the contract.

b. Content

The Customer undertakes not to use the services contracted from Ar:

i. To disseminate inappropriate, abusive, defamatory, scandalous or threatening messages.
ii. To disseminate information that may cause moral damage to third parties. To promote, encourage or defend violence against any state, organisation, group, individual or property, or to disseminate information, training or support in the implementation of such violence.
iii. In violation of the principles of Public Order and Good Morals or any fundamental right in force in the Legal Order, including laws on content or advertising that may be disseminated on the Internet, related to, in particular: alcohol, competition, protection of minors, illicit substances, export, armament, import, privacy, credit instruments, telecommunications and tobacco;
iv. In violation of any rules relating to intellectual property rights, industrial property and personal data protection, including copyright, patents, trademarks, trade secrets and software licensing agreements.
v. Public exposure of Ar, its directors, employees and/or shareholders to contempt or ridicule;
vi. Programmes, scripts or applications that jeopardise the normal functioning of the Services provided;
vii. Participating in or allowing games of chance or gambling.

Whenever Ar becomes aware that any of the activities mentioned in 3. b) are being carried out through contracted services, it reserves the right to immediately remove any applications without prior notice and to restrict or terminate the provision of such services accordingly.

c. Network and System Security

Customers or users of the services are not permitted to violate, or attempt to violate, any authentication or security system that protects access accounts, servers, services or networks. Cases of violation include, in particular:

i. Unauthorised access to third-party data (breach of privacy);
ii. Unauthorised searching for vulnerabilities in servers, services or networks, namely systematic detection of response to services (*Scan*);
iii. Entering or attempting to enter machines without the express authorisation of those responsible (break-in).

Users are not permitted to take intentional actions to disrupt the proper functioning of users, servers, services or networks, including:

i. Combined overload actions and/or actions exploiting system vulnerabilities, aimed at hindering or disrupting the functioning of services (*Denial of Service*);
ii. Massive sending of packets (*Flooding*);
iii. Attempts to hinder or disrupt servers, services or networks;
iv. Installation, use and provision of PROXYS for connectivity for purposes other than the use of the contracted service;
v. Maintenance of OPEN RELAY servers;
vi. Introduction of computer viruses, *worms*, harmful code and/or Trojan horses.

The interception of data on any network or server without the express authorisation of the legitimate owners is not permitted.

The falsification of data after its production with the intention of deceiving and misleading the recipients of such data is not permitted. Cases of falsification include, among others:

i. Changing IP addresses (IP Spoofing);
ii. Changing the identification of email or news messages.

d. Email

The misuse of email is not permitted, namely:

i. Sending emails to individuals who have expressly stated that they do not wish to receive them;
ii. Sending messages to more than 1,000 external recipients per day (addresses outside the sender's domain);
iii. Sending messages to more than 100 recipients simultaneously;
iv. Sending more than 20 emails per minute, each email containing multiple internal or external recipients;
v. Sending messages larger than 25 MB without the consent of the respective recipients;
vi. Using other email servers without the express authorisation of those responsible for them;
vii. The propagation of chain letters or pyramid schemes, whether or not the recipient accepts their delivery;
viii. The cancellation or revocation of posts made by others, except for cancellations or revocations made by newsgroup or *bulletin board* moderators in the exercise of their duties.

e. Web Hosting

The content of the pages/sites hosted is the sole responsibility of the customer and must not, under any circumstances, contain information that is:

i. Of an illegal, criminal, offensive, pornographic, paedophilic or discriminatory nature on the grounds of race, religion, politics and/or sex;
ii. That incites criminal acts;
iii. That promotes physical or moral harm against any person;
iv. That exploits or incites the exploitation of minors.
v. That contains "pirated" software, "pirated" audio (music) and video (films) files and/or others that violate copyright.

f. Ownership of IP Addresses

Ar maintains, controls and administers the ranges of IP addresses assigned to it by RIPE during the agreed contract period. Therefore, and with a view to the correct use of the Services, Ar reserves the right to change or remove the aforementioned IP addresses whenever their incorrect and/or illegal use is verified.

g. Domain and IP Blacklists

The customer acknowledges and accepts that the Internet access, email relay and electronic mail services provided by Ar may be affected by the registration of IP addresses or domains, on its own behalf or on behalf of its customers, in public anti-spam *blacklists*. These situations do not only occur with the services provided by Ar, but also with any other national or international ISP (*Internet Service Provider*).

To avoid the registration of a domain or IP address, of which it is the owner, on a given blacklist, the customer must not originate spam through Internet access contracted to Ar and must ensure that the configuration of its mail servers does not allow it to do so (open relay).

Blacklists of domains or IP addresses are predominantly managed by international institutions or groups that seek to prevent spam from spreading uncontrollably on a global scale. A customer who owns a domain or IP address included on a given blacklist will encounter problems, particularly when sending and/or receiving emails. Therefore, Ar undertakes, when this occurs, to make every effort to remove the IP addresses or domains from the blacklists on which they are included.

The customer acknowledges and accepts that there is no legal obligation or framework for domain and IP blacklist managers to comply with Ar's requests, so in some cases it may not be possible to guarantee the restoration of the service.

In the cases mentioned in 3.7.4, Ar undertakes to study joint solutions with the affected customers in order to restore the affected service in whole or in part.