



root S.A.

35, rue John F. Kennedy
L- 7327 Steinsel
Luxembourg

T: +352 20 500 • F: +352 20 500-500
E: info@server.lu • W: http://www.server.lu

VAT: LU23370883 • 2009 2213 049 • R.C.
B92268

AUP

§ Acceptable Use Policy §

1. General

Each customer who operates a server from root S.A. is solely responsible for all stored and transmitted data of the server and all actions which emanate from the server. The customer must take adequate measures which comply with the current state of technology to ensure that any misuse of the server is effectively prevented. root S.A. reserves the right to block any server at any time which causes a loss of network integrity or affects the network operation of other servers without prior warning including those actions which are not specifically referred to below. root S.A. further reserves the right to remove a server from the network if it is deemed to be causing excessive load or traffic over an unacceptably long period. If a customer does not respond and/or take the appropriate action to an abuse notification within an adequate time frame, root S.A. may suspend or remove the server without further notice. A refund is not possible. root S.A. further reserves the right, as far as permitted by legal regulations, to maintain logs of impermissible actions and to preserve the contents of servers as well as the right to hand over such logs or contents in accordance with legislation, on Order of the Court or orders from any other body appointed by law.

2. Prohibited actions and consequences of infringements

2.1 IP Spoofing

IP spoofing refers to the falsification of the IP sender address for outgoing IP packages. This technology is generally used to conceal the origin of IP packages. root S.A. has installed anti-spoofing filters in order to prevent IP spoofing. All attempts at IP spoofing are automatically logged. Any attempt at IP spoofing will lead to the immediate blocking of the server without prior warning.

2.2 MAC Spoofing and MAC Flooding

MAC spoofing refers to the falsification of a sender address of an Ethernet framework. This technology is often used to give a false identity in the local network or for a router. MAC flooding refers to the sending of Ethernet frameworks with a number of different sender addresses for the purpose of flooding MAC databanks of switches thus causing a malfunctioning of these switches. root S.A. has put in place measures which in the event of any attempt at MAC spoofing or MAC

flooding trigger an immediate and automatic blocking of the server without prior warning. All attempts at MAC spoofing and MAC flooding are automatically logged.

2.3 ARP Spoofing and ARP Flooding

ARP spoofing refers to the falsification of an ARP entry on a router by unsolicited ARP replies. This technology is often used to prepare a man-in-the-middle attack. ARP flooding refers to the mass transmission of ARP replies for the purpose of flooding the ARP databank of a router and thus causing a malfunctioning of this switch. All attempts at ARP spoofing and ARP flooding are logged and will lead to the immediate blocking of the server without prior warning.

2.4 Transmission of Switch Protocol Frameworks

The transmission of switch protocol frameworks, in particular spanning tree protocol frameworks (BPDUs) will lead to the immediate and automatic blocking of the server without prior warning. All attempts to transmit switch protocol frameworks are logged.

2.5 Transmission of Spam and Malware

Spam refers to the mass transmission of unsolicited or unrequested email advertisements. Malware refers to any type of injurious software e.g. viruses, worms, trojans, backdoors, spyware or illegal dialers. The sending of spam can lead to a warning being sent to the server operator or to the immediate blocking of the server without prior warning depending upon the gravity of the infringement. The sending of malware will lead to the immediate blocking of the server without prior warning.

2.6 Phishing

Phishing refers to illegal attempts to release access data for security areas to a wide distribution of users. Well known websites are often imitated so as to appear deceptively genuine for this purpose. The websites are reached under domain names which are similar to the original domain names. Users are invited by misleading emails to enter their access data on such hoax websites. Phishing will lead to the immediate blocking of the server without prior notice.



root S.A.

35, rue John F. Kennedy
L- 7327 Steinsel
Luxembourg

T: +352 20 500 • F: +352 20 500-500
E: info@server.lu • W: http://www.server.lu

AUP

VAT: LU23370883 • 2009 2213 049 • R.C.
B92268

2.7 Denial of Service Attacks

Denial of Service attacks (DoS) refers to an attack on a server with the purpose of disabling one or more of its services. This generally occurs by overloading e.g. by attacks with a number of small UDP packages or TCP-SYN packages. Where the attack is coordinated by a larger number of other systems this is referred to as a Distributed Denial of Service (DDoS). root S.A. has put in place measures which permit the empirical recognition of Denial of Service attacks. All Denial of Service attacks are logged. A Denial of Service attack will lead to the immediate blocking of the system without prior warning.

2.8 Scanning of External Computers

The Scanning of computers refers to the systematic searching for services on this computer with the purpose of detecting weaknesses in the services in order to utilize them for hacking at a later time. The scanning of external computers can lead to a warning being sent to the operator of the service or to the immediate blocking of the server without prior notice according to the seriousness of the infringement.

2.9 Non Authorized Access or Attempts of Hacking

All non authorized or illegal access to IT systems (e.g. "hacking") will lead to the immediate blocking of the server without prior warning.

2.10 Offering of Unlawful Information

The offering of unlawful or abusive, child pornographic, racist, politically radical, defamatory or offensive information as well as information which contravenes the rights of third parties in whatever form will lead to the immediate blocking of the server without prior warning.

2.11 Breach of Copyright

The Customer is prohibited either from offering or distributing any information which is protected by copyright without lawful authority. The operating of so called P2P exchanges, download services or streaming services over which copyright protected information could be distributed without lawful authority is not permitted. It is also prohibited to make available links which connect to P2P exchanges, download services, streaming services or information provided by them. In case of infringement root S.A. reserves the right to remove the server from the network without prior warning and to terminate the agreement.

3. Further possible consequences

Depending on the gravity of the infringement, root S.A. reserves the right to report the offense to the police and hand over all necessary information to law enforcement authorities.

Should server hardware be seized due to the criminal activity or negligence of the customer or a third party authorized by the customer to use the server or a service running on the server, the customer agrees to compensate root S.A. appropriately.

Last updated: 26.08.2009