

Uber Group Acceptable Use Policy

Overview

This Acceptable Use Policy (AUP) has been created by Uber Group to ensure the integrity, reliability and stability of the Uber Group network, associated networks and related services.

This AUP shall be effective from the time a service is initiated for the client, through to the time the service is ceased by either party. The client must ensure that the use of any service, product, or resource offered, provided, or controlled by Uber Group conforms to this AUP as well as Uber Group's Terms and Conditions. The Customer will be held responsible for its direct use of Uber Group's services, its systems, and any third-party use.

Uber Group may at its discretion modify this AUP at any time and in any way as and when it feels necessary. Notification of changes or amendments to this document will be posted on the Uber Group website.

This Acceptable Use policy replaces any previous AUP or agreements that may have been previously made with Uber Group in any form.

The use of Uber Group services is deemed to be in agreement with this and the standard Uber Group terms and conditions, or other terms and conditions for service of a business operating under the Uber Group of companies.

1. Acceptable Use

In addition to the other requirements of this AUP, the Service may be used only in a manner that, in Uber Group sole discretion, is consistent with the purposes of such Service. Customers should contact Uber Group if unsure of whether any contemplated use or action is permitted.

1.1 The usage of Uber Group services must comply with current laws and regulations; including but not limited to regulations pertaining to copyright, license agreements and patents, and must adhere to rules and regulations in Uber Group Terms and Conditions

1.2 Mail Services

The following mail limits are designed to enable Uber Group mail servers to operate at optimal efficiency thereby ensuring that all Uber Group clients receive the highest quality mail service possible.

- a) **Single Email Message Size Maximum 20MB:** The maximum size of a single message will be set to 20MB (20 Megabytes) in line with the mailbox size. You will be able to receive a message up to 20MB provided you have adequate space in your mailbox.
- b) **Maximum email Mailbox Size: 20 MB:** The maximum size of the Clients mailbox will be set to 20MB (20 Megabytes).
- c) **E-mail Message Lifetime 30 Days:** In order to maintain the performance of our mail server, guarantee new mail can be received, a continue to provide appropriate service standards, mail left on the server for more than 30 days may be deleted from the server.

1.3 Website Hosting Services

The following limits are designed to enable Uber Group' web servers to operate at optimal efficiency thereby ensuring that all Uber Group' clients receive the highest quality service possible:

- a) Website Traffic Allowance - Basic and Enhanced hosting plans only - 7GB / 28 days: Website traffic under 7GB (7 Gigabytes) per website per 28 days will be provided free. Traffic used above the allocated 7GB (7 Gigabytes) will be charged at \$25.00 + GST per 1GB (1 Gigabyte) block used per website.
- b) Warning Message for traffic quota: To ensure clients are aware that they are reaching 75% of their allowed website traffic limit, a warning message will be sent via e-mail to the contact address of the Uber Group account holder once their total traffic generated to their site exceeds 75% of their allowance.
- c) System Resources: Clients acknowledge that the website hosting service is provided on a multiple shared server environment and agrees not to engage in any activity that could overwhelm the server with heavy CPU, memory or network usage or that requires a disproportionate amount of the resources of the Uber Group Web servers, including without limitation, use of highly active CGI scripts or chat scripts.
- d) Security: It is the Clients responsibility to ensure that cgi scripts, any executable files or dynamic scripts uploaded to the Uber Group Web Servers are configured in a secure manner.

1.4 Database Hosting Services

- a) System Resources: The Client acknowledges that Database Service is provided on a multiple shared Database server environment and agrees not to engage in any activity that could overwhelm the Database server with heavy CPU, memory or network usage or that requires a disproportionate amount of the resources of the Uber Group Database servers, including without limitation execution of untested or badly written Database queries.

2. Unacceptable Use

By way of example, and not limitation, the following sections outline activities that are expressly prohibited. The service shall not be used to post, transmit, re-transmit or store material which, in the judgment of Uber Group Limited:

- a) Violates local, state, federal, foreign, or International Law;
- b) Could be considered threatening, obscene, indecent, defamatory, threatening or that otherwise could adversely affect any individual, group or entity.
- c) Deceptive or fraudulent practices.
- d) Any activity infringing on the intellectual property rights of others, including, but not limited to,
 - (i) copyrights, trademarks, service marks, trade secrets, patents,

- (ii) Actions that restrict or inhibit any Person, whether a customer, Uber Group, or otherwise, in its use or enjoyment of any Uber Group service.
- e) Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to spam, initiation of pinging, flooding, mailbombing, denial of service attacks, and piracy of software.
- f) Sending unsolicited bulk messages (spam) via any means, including, but not limited to, email, instant messenger services, and newsgroup postings. Uber Group reserves the right to determine in its sole discretion and based on the information available what constitutes spam as well as what measures are necessary in response to spamming complaints.
- g) The engagement of Uber Group services to promote deceptive and or illegal marketing practices, products or services.
- h) Connecting to IRC (Internet Relay Chat) services from within the Uber Group or associated networks).

2.1 System and Network:

- a) The deliberate transmission of computer viruses, worms, trojan software, or other malicious programs.
- b) Interfering with, disrupting, or denying service including, but not limited to, using any technique to intentionally degrade or disable the delivery of any legitimate data (eg, denial of service attacks).
- c) Attempting to gain unauthorized entry to any site or network including, but not limited to, executing any form of network probing, monitoring or other information gathering on the Uber Group or a third party site or network.
- d) Attempting to circumvent host or user authentication or other security measures of any host, network or account.
- e) Maintaining an Open Email Relay/Open Data Relay or allowing any data to be sent through one's system by an unrelated third party, including, but not limited to, via open email gateways and open proxy servers.
- f) Manipulate or bypass Uber Group usage limits.
- g) gain or attempt to gain access to a service or services not provided by Uber Group; this includes but is not limited to console, command line or shell.
- h) uploading and/or use of a file system manager of any description that provides the ability to access files outside of your allocated website space.

2.2 Mail Server Facilities

- a) Sending unsolicited mail messages.
- b) Harassment including, but not limited to, language, frequency or size of messages.
- c) Unauthorized use, or forging, of mail header information.
- d) Solicitation of mail for any other email address other than of the poster's account or service with the intent to harass or to collect replies.
- e) Creating or forwarding "chain letters" or other "schemes" of any type.
- f) Use of unsolicited email originating from within Uber Group' network, or networks of other Internet Service Providers, on behalf of, or to advertise any service hosted by Uber Group, or connected via Uber Group network.
- g) Infringement of mail service restrictions as outlined in Section 1.4 of this document

2.3 Newsgroups

- a) Posting the same or similar messages to large numbers of newsgroups ("newsgroup spam").
- b) Posting excessive numbers of identical or similar messages to any number of newsgroups from Uber Group' network or networks of other Internet Service Providers on behalf of, to advertise, any service hosted by Uber Group or sites hosted within, or via Uber Group network.
- c) Posting chain letters of any type.
- d) Posting encoded binary files to newsgroups not named for that purpose.
- e) Cancellation or superseding of posts other than your own.
- f) Forging of header information of the poster's account or service.

3. Additional Obligations

3.1 Bulk Email

Bulk email must provide recipients with an easy and effective mechanism for removal from bulk email lists. The source of the addressee's address must be included in each bulk email message. Senders of bulk email must take effective steps to confirm that the actual owner of each email address on a list has agreed to receive bulk mailings from the sender before sending email to that list. The utilization of web server SMTP services for the use of sending bulk emails is expressly prohibited.

- 3.1** **(i)** Comply with any instructions or requests made by Uber Group with regard to the hosting of a particular website (s) domain name or other service in a timely fashion.

3.2 Password Protection

The Customer is responsible for protecting passwords and for any authorized or unauthorized use of its systems and/or networks. All actions resultant from passwords being compromised will remain the sole responsibility of the Customer.

3.3 Content Protection

The Customer must provide appropriate protection to prevent minors (persons under 18 years of age) from accessing any unsuitable material published via any Service.

3.4 Content Ownership

The Customer is responsible for all content or information residing on, obtained or transmitted via the Service.

3.5 Vulnerable Systems

Uber Group reserves the right, without prior notice, to perform vulnerability tests on systems residing on its IP address range, which may be allocated for Customer use. The purpose of such testing includes, but is not limited to, testing of mail servers or proxy servers for unrestricted third party relaying. Uber Group will employ all reasonable efforts to ensure that such testing

- a) will be non-intrusive in nature, and
- b) will not adversely affect Service provided to Customer or compromise the security of Customer's network.

The Customer is responsible for correcting any system vulnerability upon notification. Customer must terminate operations of a known compromised system.

3.7 Service Provided Equipment

Customer is responsible for any modification of, alteration to, or other tampering with any hardware provided with the Service.

4. AUP Enforcement

4.1 Violation of this AUP may subject Customer to international, and/or civil and/or criminal liability. Customer activity that facilitates a violation of this AUP by any party constitutes a violation of this AUP by Customer.

4.2 Uber Group reserves the right to immediately, and without prior notice, filter, block, suspend, and/or terminate access to the Service at any time for any conduct that Uber Group, in its sole discretion, determines violates, or may violate, this AUP and/or Terms and Conditions or is otherwise harmful to Uber Group' interests or the interests of others.

4.3 If access is terminated, Uber Group, in its sole discretion, may refuse to accept all new email sent to the terminated email address and delete all or part of Customer's data stored on Service.

5. Third Party Complaint Process

5.1 If the Customer, or the public, wishes to notify Uber Group of a potential violation of this AUP they should do so by sending an email to support@ubernet.co.nz. Uber Group will review such communication as quickly as possible and take action as deemed appropriate by Uber Group.