



Terms of Use

Luxembourg Web Services

Disclaimers

This document is the proprietary and exclusive property of LuxNetwork S.A. S.A. except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes without the prior written permission of LuxNetwork S.A. S.A.

Term of Uses

Our Terms of Use sets out simple common sense guidelines for permitted use of our services. The following examples are non-exhaustive; we encourage you to contact us if you are in any doubt or if there is any likelihood that your intended actions could pose a problem.

Forbidden usage of our service

You will not use the service wilfully or otherwise for:

- §= Virtual currency (*coin) mining, Internet Relay Chat (IRC) (servers or clients),
- §= torrent, peertopeer, camfrog, TOR nodes (exit or relays), proxy servers (local reverse proxy servers used for performance and/or caching of content hosted by us are permitted);
- §= Sending, relaying or promoting any form of phishing, intrusive network marketing, nuisance individual or bulk messages sent via any method such as via email, USENET, forums, chat rooms, social media or similar methods;
- §= Hosting "spamvertised" websites or other services advertised by spam email or by posting unwanted links to your website on thirdparty websites, whether or not the advertising was performed using our services;
- §= Distribution, storage, modification or development of malware or any files or data in violation of copyright or trademark infringement laws;
- §= Any phishing web page or any activity promoting phishing web pages;
- §= Committing or promoting illegal activities including those of a fraudulent, violent, threatening, harassing or terrorist nature, hacking, fraudulent misrepresentation, publishing defamatory or knowingly false material, anything in breach of the Computer Misuse Act in Luxembourg, child pornography, obscene speech or materials, or anything we deem to be inciting crime;
- §= Promoting or participating in any illegal or nuisance activities;
- §= Exploiting children or other vulnerable groups;
- §= Testing our infrastructure or any services for vulnerabilities, except as where agreed in advance by our technical support team and strictly restricted to your own services;
- §= Any activity resulting in noncompliance with the law of either the country your services are hosted in or in any legal jurisdiction binding upon you or us;
- §= Any activity that shall place an undue burden on our servers, infrastructure, or that of any of our upstreams;
- §= Any other activity that we deem to be harmful to other customers or our goodwill, reputation, operations or customer relations.
- §=

Email sending policy

- §= Sending, relaying or promoting any form of unsolicited email is strictly prohibited and we consider this to be "spamming", even if you are sending each email individually;
- §= When subscribing a user to a bulk email list or database you will perform a separate check to verify that they own the email address. You must not require a user to optout, they must explicitly optin before being added to your live email list. This can be done by sending an email to the owner with a unique, onetime link to click before they are fully subscribed.

- § We may request evidence of optin requests at any time and you will provide such evidence within 72 hours;
- § Any bulk email sent by you will include a working method to unsubscribe from your email database and your physical contact address;
- § Any unsubscription requests must be processed within 72 hours whether this is automatically or manually performed;
- § You agree to comply with any relevant antispam laws in any applicable jurisdiction which is binding upon you or us, such as CANSPAM legislation and the European Union's Privacy and Electronic Communications Regulations.

Network attacks

A network attack is any form of network traffic which attempts to maliciously or negligently disrupt, degrade, deny or destroy legitimate data flow to or from our infrastructure or services or those belonging to a thirdparty. If any network attacks occur which are targeting your service, or your services are found to be attacking our infrastructure, other customers or any third-party we will promptly react to remedy the situation.

1.
 - o Inbound attacks (from the Internet to your service)

If you are the subject of an attack we will use reasonable efforts to:

mitigate against the attack but cannot accept any responsibility for being unable to fully stop the attack. If the attack is causing problems which have the reasonable potential to affect the services of other customers we reserve the right to immediately suspend all or part of your services in order to ensure a high quality of service for all customers.

2.
 - o Outbound attacks (from your service to other servers or the Internet).

If outbound attacks are being performed from our services we will:

investigate the issue and attempt to block such attacks, but often these are a result of insecure code for your website, or weak passwords allowing malicious thirdparties access, and therefore we cannot prevent these. For onetime attacks we will provide you with advice as to how to block such attacks, but for repeated attacks we may find it necessary to suspend or terminate your service.

If we identify a breach of this policy

- § For any breach of this Term of Uses Policy we will endeavour to notify you via email with details of the breach, but to protect thirdparties may not be able to disclose all information reported to us.
- § Where possible we will allow a period of time for you to resolve any breach but if we, at our sole discretion, consider the severity of the issue to require it we may immediately suspend all or part of your subscription, and for serious issues this may include suspension of other subscriptions in your account. For repeat or serious offenders we will refuse to supply you or your associates with new services in the future and may terminate any existing subscriptions.
- § If notified of a breach of this Term of Use Policy you must reply stating the immediate steps you will be taking to prevent an ongoing breach within 24, 48 or 72 hours (at our sole discretion and as stated in the notification email) or we will act to remedy the situation or suspend your subscription using any means necessary. If we do not state a maximum response time in our email to you then you shall reply within 48 hours.
- § No refunds or credits will be provided for any services terminated due to a breach in our Terms of Use Policy, and you are not entitled to participate in our Money Back Guarantee scheme
- § We may additionally suspend services upon request by any competent legal authority which is binding upon us.