



Instra Anti Abuse Policy

Last Updated: December, 2020 - © CentralNic Group PLC. All Rights Reserved.

All services of Instra ("Service Provider" or "We") are provided on the basis of this policy. This policy is in effect pursuant to the terms of the Registration Agreement and/or Service Agreements between Service Provider and its customers. This policy is effective in its current form as of its first publication on the website of Service Provider and may be updated or amended by Service Provider from time to time by providing reasonable notice on its website or in its newsletters. This policy has been prepared to assist the reporting process and inform customers about prohibited use of our services.

This policy applies to all services provided by Service Provider, including domain name registration and management services, DNS services, hosting services, email services, certificate services, routing services, and other services ("the Services" or "a Service").

Service Provider recognises the rights of its customers, and will generally not impose any restriction in relation to how the Services are being used. The customer is obliged to comply with the published policies that relate to their particular service. Service Provider uses all reasonable means to ensure that the customer complies with published policies of the applicable regulatory authorities such as ICANN's published policies. Customers are also required to agree to our Terms of Service when they apply for a Service.

Service Provider is committed to contribute to the maintenance of a safe, secure online environment and to limiting the potential for significant harm to internet users. A key component of this commitment is to investigate and respond appropriately to all substantiated reports of malicious, illegal or fraudulent use of its services. Abuse in the context of this Policy shall be defined as an action that causes or is likely to cause actual and substantial harm to third parties, is a material predicate of such harm, or is illegal, illegitimate, or otherwise contrary to this Policy.

All customers of Service Provider and its resellers agree to abide by the terms of this policy by agreeing to the terms and conditions of the Service Provider, of which this policy is an integral part. Customers using the Services to provide services to third parties are required to bind said parties to the terms of this Policy.

The intended purpose of this policy is to ensure that third parties understand what constitutes Abuse, as well as to provide information on how to submit such reports to the Service Provider.

The Services may not be used in contravention of applicable laws or regulations, good morals or this policy. The Policy is intended to enable the Service Provider to investigate and to take swift action in case of abusive or otherwise prohibited use and to deter Customers from engaging in illegal or fraudulent use of the Services. The Service Provider may enforce this

policy against its customers by disabling customer access to the Service or suspending the Service as needed to enforce this policy.

Service Provider expressly reserves the right to deny, cancel, suspend, disable, lock or transfer any Service where it deems necessary and at its sole discretion: (a) to protect the integrity, security and stability of the Internet and/or DNS, (b) to protect against cyber-security threats, (c) to comply with any applicable laws, government rules or requirements, requests of law enforcement; (d) in the event a Service is used in violation of this policy and any other applicable policies by regulatory authorities and; (e) in compliance with any dispute resolution process, or to avoid any liability, civil or criminal, on the part of Service Provider and its affiliates, licensors subsidiaries, officers, directors and employees. Such actions may include requesting the removal of the offending content by the Customer or the deactivation of the hosted resource or the partial or complete suspension or termination of the affected service. We further reserve the right to terminate all agreements with customers that repeatedly violate this policy. We further reserve the right to act directly and immediately in cases of obvious and significant malicious conduct and without prior notice where necessary to prevent harm.

Service Provider may identify Anti Abuse Policy violations by any means, including without limitation, a private complaint, public alert, government or enforcement agency outreach, third party notification, and on-going monitoring by Service Provider or its partners. At its discretion, Service Provider or its designee, through an automated system or otherwise, may view any website made available through a domain name, for the purpose of identifying violations of this policy.

Service Provider will implement all valid court orders or seizure warrants from courts, arbitration tribunals, or law enforcement agencies of applicable jurisdictions, provided the court orders and seizure warrants are enforceable at the domicile of Service Provider.

Provided below is a summary definition of what constitutes abuse and prohibited use. The list is non-exhaustive and may be amended at any time by publishing a new version of this policy.

A) DNS Abuse:

DNS Abuse is use of domain name registration and management services that is composed of five broad categories of harmful activity that intersect with the Domain Name System: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse). Where there is evidence that our services are being used for DNS Abuse, we will consider suspending the use of the service should sufficient evidence be provided to us to protect the integrity of the Internet and - in cases where the resource of the customer was compromised - assist with protecting the customer against any potential liability issues.

- a) **Malware** (also includes spyware, botware, keylogger bots, viruses, worms, trojans) is malicious code or software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information,

and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.

- b) **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator to enact various forms of harm – ranging from unsanctioned spam to placing high transaction traffic on valid computer services such as DNS or web services. This prohibition also refers to the operation of botnet command and control functions (a smaller number of computers that issue and/or distribute subsequent commands to the Botnet).
- c) **DDoS attack** refers to the use of the Service in the initiation or intentional participation in denial-of-service attacks (DOS or DDoS attacks, mail bombing, etc).
- d) **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites.
- e) **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning or the use of redirects. DNS hijacking occurs when attackers use malware to redirect victims to the attacker's site instead of the one initially requested. DNS poisoning causes a DNS server or resolver to respond with a false IP address bearing malicious code. This also includes unauthorized fast flux techniques.
- f) **Spam** is the use of the infrastructure or services of Service Provider to send unsolicited bulk messages by email or other means, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content. This also applies to instant or mobile messaging spam and the spamming of web sites and online forums. Spam is only considered DNS Abuse when it is used as a delivery mechanism for the other four forms of DNS Abuse.
- g) **Fast Flux Hosting** is the sheltering of phishing, pharming, botnet and malware sites and networks from detection, and the frustration of methods employed to defend against such practices, whereby the IP addresses associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find.

B) Content Abuse:

Content abuse is use of our web hosting services in furtherance of the following activities:

- a) Intellectual Property, Trademark, Copyright, and Patent Violations, including Piracy: Intellectual property (IP) is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized in the corresponding fields of law. Under intellectual property laws, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary,

and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights and trade secrets in recognized jurisdictions. Any act resulting in theft, misuse, misrepresentation or any other harmful act by any individual or a company is categorized as Intellectual Property violation.

- b) Hate Speech is the distribution and/or publication of hateful, defamatory, extremist or derogatory content based on racial, ethnic, or political grounds, intended or generally able to cause or incite injury, damage or harm of any kind to any person or entity, whether or not it includes general or specific incitements to violence.
- c) Violation of privacy rights is the publication of content invading the privacy rights of a third party without legal justification such as by publishing their personal information without consent or legal basis.
- d) Child Abuse Materials (CAM) and child pornography refer to the distribution of, linking to or otherwise making accessible of films and/or images, films and, in some cases, writings depicting sexually explicit activities involving a minor or depicting minors engaged in any activity of a sexual nature or which may otherwise harm minors.

If we receive reports that our services are being used in relation with content containing child abuse material, we are not permitted by law to verify these claims ourselves. We recommend that you contact your local law enforcement to report such issues. We also work with organizations such as INHOPE (<https://www.inhope.org/EN#hotlineReferral>) to identify such content. We will immediately suspend any domain name upon receiving a written confirmation from a verified law enforcement provider or recognized partner organization that the domain name is being used to point to servers containing child abuse material.

- e) Contribution to the sale or distribution of prescription medication or controlled substances without a valid prescription and/or distribution license as well as the sale and distribution of unlicensed or unapproved medications.
- f) Human trafficking is the the action or practice of illegally transporting people from one country or area to another, typically for the purposes of forced labour or sexual exploitation. This also includes slavery in any form or shape.
- g) DNS Abuse as defined above.

We do understand that some of these uses may be open to interpretation, or may be in conflict with other aspects of law. For this reason, we can only take appropriate action where supporting evidence is compelling and clear. We may also act upon certain forms of content abuse even if we are not the hosting service provider.

C) Other illegal or prohibited use

The use of our services is further prohibited abusive, malicious, or illegal conduct in use of a domain name such as:

- a) when it violates any local, state, national or international law or regulation applicable to us or the service. A law or regulation is applicable when it is effective in the jurisdiction of [Company], Customer or any other jurisdiction targeted by Customer with his use of the service.
- b) when it is used for the promotion of, involvement in or assisting with illegal activity of any kind, as well as the promotion of business opportunities or investments that are not permitted under applicable law
- c) when it is used to impersonate another entity as a means to commit fraud.
- d) Any other advertisement or offer for sale of any unlawful goods or services in breach of any national or international law or regulation
- e) when it violates any national or international sanctions that [Company] its affiliates and/or suppliers are subject to.
- f) when used for hacking. Hacking is the use of the Service in activities intended to gain illegal access to other computers or networks, as well as any activity to prepare for such illegal system penetration. This does not include activities to gain legal access or test the security of the third party with their consent.
- g) when it is identified as illegal or otherwise unlawful in a court order or by request by an authority of appropriate jurisdiction.

D) Restricted Use

The following areas may not necessarily constitute abuse, but may be treated as such unless they follow certain requirements:

- a) Distribution of erotic or pornographic or otherwise sexually explicit content is only permitted in observance of the applicable legal requirements. For example, the use of any Service for publication or distribution of such content without sufficient age verification techniques (thereby allowing minors to view such content without appropriate barriers) as well as use in violation of the requirements and directives of the authorities or appropriate registration authorities is strictly prohibited.
- b) Chat or messaging services on our hosting services are only permitted if the customer obtains a prior explicit written approval from Service Provider.
- c) Use of hosting services download or streaming server, online file repository, P2P-Trackers, P2P-Client or P2P-Host or otherwise using the hosting services to participate in file-sharing activities.
- d) Use of domain names must comply with the policies of the appropriate registry operators and jurisdiction.
- e) Use of our hosting and mail services to send any form of Spam is prohibited. It may be impossible for us to determine in every case whether a message is actually spam, a newsletter or legal business email. For further information, see our Anti-Spam policy.
- f) Use of our services in furtherance of activities that violate our company policies and/or values.

E) Trusted Notifier Reports

Any reports of abuse from entities that we in our sole judgement consider to be 'trusted notifiers' due to their recognized subject matter expertise and reputation for report accuracy may result in immediate action without prior consultation with or notification of the customer and without investigation of the complaint. The same applies to reports from law enforcement agencies and other properly authorized enforcement agencies. Authorities reporting abuse must be prepared to verify their provided credentials and should communicate through proper legal channels.

III) How to report abuse to us:

We maintain a dedicated public abuse contact at:

abuse@instra.com

All abuse reports received by the abuse point of contact will be tracked internally in a ticketing system to ensure accountability and ease of reference, and a tracking number will be provided to the reporter. Each report will be reviewed and evaluated regarding its credibility, to determine whether the reported issue is an abuse concern and to assess the required action(s), if any. While a specific remedy may be requested, it must be the proper course of action compared to other means/remedies and we reserve the right to choose the best action.

When reporting abuse the reporter should provide sufficient information and documentary evidence about the reported issue to allow proper and appropriate review of the report. The report should start by prominently indicating the domain name, link and/or specific service offered by Service Provider giving rise to the report and providing a short summary of the issue, including, but not limited to:

- a. exact URL(s) where we can see the violation
- b. for matters where URLs cannot be used (i.e. spam and/or phishing allegations), copies of files used as part of the violation and evidence as to their origins (i.e. emails including full headers).
- c. any other supporting evidence such as screen shots and/or server log files. Upon request, the reporter should provide additional supporting information to help us investigate and assess the issue.

We aim to respond to each report as soon as possible. Depending on the current volumes of reports, it may sometimes take some time to respond to your message. Please note that we may bundle responses to multiple reports by one reporter. Please do not send unrequested follow-ups or reminders to avoid delaying overall ticket response times. For legal or data protection reasons we may not be able to specify the actions taken as a result of the report. In case of high ticket volumes or multiple reports about the same issue, we may elect not to provide individual responses to each reporter. Failure to follow these reporting guidelines may result in disregarding your report.

The abusive use must be active and verifiable at the time we investigate the matter. If we cannot review/download/use/access the violation, then we cannot verify it. If the violation is restricted to or only accessible from certain subnets (eg: geographical region), or access methods (eg: mobile devices), this information must be provided to ensure we can verify such claims.

The reporter agrees that we may provide the complaint to the Customer or intermediary third parties for review and further action. We will then work in cooperation with the affected parties to

rapidly address identified threats or confirmed abuse. In case the reporter objects to the forwarding of their complaint this should be made clear in the initial abuse report.

In case of multiple complaints about the same service, hosting resource or domain name, the reporter shall bundle such complaints into one report. Please do not send multiple reports or messages about the same resource.

The reporter shall identify himself by providing his name, telephone number and email address as in some cases we may need to follow up on the report with further questions. We may disregard or close anonymous complaints and complaints including false or misleading contact details.

The reporter shall maintain a civil tone. We may disregard reports that violate basic rules of etiquette or civil conversation.