Abuse Policy (Domain Names)

The intended purpose of this policy is to ensure that third parties understand what constitutes Abuse (specifically Domain Name related Abuse), as well as to provide information on how to submit such reports to Instra.

This Abuse Policy only applies for domain names where Instra is the sponsoring registrar or is operating as an up line registration provider for the domain name record.

Our Abuse Reporting mechanism allows us to assist with the rapid suspension of a domain name where a domain name is found to be affecting the integrity of the Internet/DNS, or where there is factual evidence of unlawful activity.

This policy has been prepared to assist the reporting process and does not modify and/or amend our Terms of Service.

Provided below is a summary definition of what constitutes Domain Name Abuse:

1. 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.

We do understand that these matters may be open to interpretation, or may be in conflict with other aspects of law. For this reason, we will only take appropriate action where supporting evidence is compelling and clear. We do recognise the existence of various dispute resolution processes, and our Abuse Reporting mechanism will not be used to override dispute resolution where we deem that a dispute resolution is a more appropriate course of action.

2. Spamming

Spamming is defined as the use of electronic messaging systems to send unsolicited bulk messages. The term also applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums. Unsolicited emails advertising any products, services, and even charitable requests or requests for assistance are also considered as spam by this policy.

As spamming can be done without the use of any domain names, the scope within this Abuse Policy is limited when submitting complains about domain names. In most cases, you should verify email meta data and/or email header data, and report the issue to the carriage service which physically sends the spam. We are willing to examine how a domain name is being used for spamming

purposes, and we may take any appropriate action where we can identify a close and substantial connection between the Spam Abuse and the Domain Name.

3. Phishing (and various forms of identity theft)

Phishing is usually done by operating a fake web site that it is meant to look like the actual web site usually for the purpose of obtaining details by deception. As the domain name registrant could potentially have their web site compromised by a third party exploiting a security vulnerability, we generally suspend the use of any domain name where Phishing has been confirmed to protect both the integrity of the Internet, and in many cases, assist with protecting the registrant against any potential liability issues too.

4. Pharming and DNS Hijacking

Redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login credentials to legitimate services.

There are various methods of how Pharming/DNS hijacking is done. In many cases, this may be done without a domain name, however if we receive such a report and the report identifies and close and substantial connection to the alleged abuse, we may consider suspending the domain name from the DNS.

5. Distribution Of Viruses Or Malware

Distribution of viruses or Malware most commonly occurs when a web server has been compromised by a perpetrator that has installed a virus or “malevolent” piece of software meant to infect computers attempting to use the web service. Infected computers are then security compromised to participate in nefarious purposes such as gaining stored security credentials or personal identity information such as credit card data. Additionally compromised computers can sometimes be remotely controlled to inflict harm on other internet services.

If we receive such a confirmed report that a domain name under our sponsorship is being used for distributing Viruses or Malware, we may consider suspending the use of the domain name to protect the integrity of the Internet/DNS.

6. Child Pornography

Child pornography refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.

If a domain name is being used to point to a web site containing child pornography/child abuse, we are not permitted by law to verify these claims. We recommend that you contact your local law enforcement to report such claims. We will immediately suspend any domain name upon receiving a written confirmation from a verified law enforcement provider that the domain name is being used to point to servers containing illegal child abuse material.

7. Using fast flux techniques

A methodology for hiding multiple source computers delivering malware, phishing or other harmful services behind a single domain hostname, by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.

For the purpose of protecting the integrity of the Internet/DNS we may consider suspending the use of a domain name if it is proven that it is being used in such a method. We may perform our own tests to validate the use of these methods.

8. Running botnet Command and Control operations

A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services 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. The Command and Control refers to a smaller number of computers that issue and/or distribute subsequent commands to the Botnet. Computers that have been compromised as a part of the botnet will periodically check in with a Command and Control computer that hides behind a list of date triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.

Where there is evidence that a domain name or the DNS zone is being used in this way, we will consider suspending the use of the domain name should sufficient evidence be provided to us.

Usually a series of domain names are used which don't have a particular meaning – are often used in botnets, and we as a registrar also take an active role in identifying these patterns.

9. Hacking

Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of other parties. It includes any activity that might be used as a precursor to an attempted system penetration.

Due to continual developments in the domain name industry, it is unlikely that domain names are used or required for hacking. If evidence that a domain name is being used as a means for hacking, we may investigate these claims (upon being provided with sufficient explanation), and we are willing take any action we deem appropriate including suspending the use of the domain name.

10. Financial and Other Confidence Scams

Financial scams, including but not limited to the cases defined below, are operated by fraudsters to lure investors into fraudulent money making schemes. Prominent examples that will be treated as abusive are:

1. Ponzi Schemes: A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays dividends to initial

investors using the principle amounts invested by subsequent investors. The scheme generally fails when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of dividends

2. Money Laundering: Money laundering, the metaphorical cleaning of money with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source, and⁄or destination of money, and is a main operation of the underground economy
3. 419 Scams: 419 scam (aka Nigeria scam or West African scam) is a type of fraud named after an article of the Nigerian penal code under which it is prosecuted. It is also known as Advance Fee Fraud. The scam format is to get the victim to send cash (or other items of value) upfront by promising them a large amount of money that they would receive later if they cooperate

When we receive reports of illegal activity, we will require sufficient factual evidence and a means to investigate these claims before taking action resulting in the suspension of domain names.

Where the registrant is providing financial services, banking or insurance services we may request further verification information.

Only when there is obvious evidence of unlawful activity will we proceed with an immediate suspension of a domain name, and in no way should an Abuse Report be used as a means to circumvent proper due diligence. Reports of unlawful activity should also be reported to police. We may be willing to co-operate with any recognised local law enforcement in relation to domain names being used for unlawful purposes.

11. Illegal Pharmaceutical Distribution

Due to a variety of rules and regulatory requirements amongst various jurisdictions, we believe that the onus is on the registrant to comply with laws relevant to their jurisdiction that they are domiciled, and within the laws of our jurisdiction, namely the Commonwealth of Australia.

In the event that we receive a report in relation to Illegal Pharmaceutical Distribution claim, we would immediately comply with any request to validate if the registrant is either a verifiable natural person or a legally constituted organization or legally verifiable entity. We will not immediately suspend and/or policy delete the domain name in the absence of solid evidence confirming that the registrant is acting unlawfully. With this in mind, if we receive a confirmed report from a recognised law enforcement agency or a court order from a competent court of law requesting our assistance to intervene, we would provide all necessary assistance, which may include surrendering our contact data, suspending and or policy deleting the domain name record.

We do understand that the distribution of prescriptions drugs locally within a nation or overseas, without prescription and appropriate licenses would generally be considered to be unlawful in many countries including Australia, however we will not immediately suspend any domain name unless there is actual proof that services deemed unlawful are actually being provided.

Where we can identify a rogue trader, or a trader that deliberately conceals their identity, we may suspend or cancel the domain name registration in accordance with our Terms of Service.

12. Other Violations

Other violations that will be expressly prohibited include:

- Maintaining inaccurate contact details on the WHOIS record of the reported domain name
- Nominating a local presence service as a registrant proxy for the purpose of operating a "rogue" business
- Network attacks
- Other Illegal Adult/Pornographic content
- Distribution of malicious tools promoting or facilitating hacking, unsolicited bulk emails or SMS, fake anti-malware products, phishing kits, unauthorized data banks violating individual privacy rights
- Content which violates any export, re-export or import laws and regulations of any jurisdiction
- Violation of any federal, state or local rule, regulation or law, or for any unlawful purpose, or in a manner injurious to Instra, its service providers and partners, or their reputation, including but not limited to the above mentioned activities mentioned as part of this policy

Other Considerations

1. If an Abuse Report requests that we disclose confidential details provided by the domain registrant or requests the suspension of domain services due to a violation of our Terms of Service and it is not formally accompanied by a related written legal instrument of appropriate means and venue, additional supporting information may be requested by us in order to facilitate such a request.

2. Instra generally provides registrants with 15 days notice of a pending domain action due to a violation of our Terms of Service in order to provide them with the opportunity to remedy the alleged violation. If the registrant is not in violation of our Terms of Service at the end of the 15 day notice period, we may cancel any pending action and consider the matter resolved. This notice period may change depending on the circumstances.

3. In cases where you have asserted that you own copyright over material - we may not have the means to verify this assertion and in many cases, we lack the authority to verify claims of others or to verify the identity of the claimants (as is many times the case with copyright, trademark, service mark, and intellectual property matters). In these circumstances it may be more appropriate that you seek other means to file a dispute, which include, but are not limited to:

   Uniform Domain Dispute Resolution Policy (uDRP)

   Digital Millennium Copyright Act (i.e. filing a DMCA takedown)

   Please note that if the domain registrant fails to get back to us regarding a Registrant Warranty Check, or a material breach of our Terms of Service, Terms violation notification, we take that issue very seriously. Our Terms specifically require the registrant to get back to us regarding these matters in a timely manner and failure to do so can result in domain

suspension. We use all forms of available contact information to contact the registrant and their failure to respond may result in us suspending or policy deleting their domain name.

Generally supporting information must demonstrate/include the following:

- You must include your name, address, and email or telephone number (preferably both). If you have legal counsel actively representing you in the matter, please include their contact information as well. If you provide false or misleading contact details, we may discard your report.

- You must include specific details concerning the alleged Terms violation, 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

- The terms violation must currently be in active and verifiable use at the time we investigate the matter. If we cannot see/download/use/access the violation, then we cannot verify it. For example, if you report that malware is being distributed via a domain, but the reported URL where it is downloaded from/distributed does not work, then we cannot verify the violation. If the violation is restricted to certain subnets (eg: geographical region), information about supporting open proxies must be provided to ensure we can also verify such claims

- If requesting a domain suspension, it must be the proper course of action compared to other means/remedies. For example, lets assume that you own the copyright on music being sold by Google. Assuming google.com was registered at Instra Corporation Pty Ltd, taking down the whole domain is NOT the proper course of action; rather filing a DMCA takedown or filing an applicable lawsuit against Google would be called for.

- You must be qualified to determine the violation of Terms and be associated with any parties affected by the outcome of any action taken. For example, lets say you notice that a site is republishing documentation written by Microsoft and file a suspension request with us based on Microsoft's copyrighted material being misappropriated by a 3rd party without Microsoft's knowledge, but that you neither work for Microsoft nor have their specific written consent to represent their interests in these matters. We will not suspend the domain because:

    a. it will probably be impossible or improbable to accurately identify you are who you say you are,
    b. you are not qualified to file this complaint since there is no way for you to know that the site does not have Microsoft's permission and

c. you are not associated with Microsoft or the site publishing the information. In this case, you should bring your complaint to Microsoft or the site supposedly violating Microsoft's copyright.

There are some special scenarios related to domain suspension which require additional supporting information:

- When the domain in question is allegedly supporting a violation of our Terms of Service by acting as a name server host for other domains (wherein the other domains are found to be violating our Terms of Service, Acceptable Use Policy "AUP", or this Abuse Policy (Domain Names) we will require clear demonstration that the request will not affect domain names using the name server hosts that are not in violation of our Terms of Service. In these circumstances, we will require a list of all domains which are using these name server hosts before taking any measures to suspend a domain name. In general, we will only consider suspending the use of the domain name if the Abuse report is serious (i.e. malware, phishing etc.). It is assumed that someone reporting such a violation understands that such actions can undermine the global DNS system and therefore we expect they have performed appropriate due diligence to ensure innocent domains will not be harmed; such diligence would require TLD zone file access in order to determine the entire list of possible domains affected. Failure to perform such due diligence may result in us dismissing the complaint. In the event such due diligence cannot be taken, we will likely recommend instead pursuing suspension of the domains which are directly violating the Terms of Service, AUP, or ARP, which may very well not be registered with Instra Corporation Pty Ltd.

- When the domain in question is used to allegedly impersonate another entity as a means to commit fraud (i.e. as in a phishing scheme), the person filing the abuse report must:

    a. legally represent the interests of the impersonated entity and/or
    b. offer evidence of fraudulent solicitation (i.e. provide a copy of a phishing email with headers referencing the domain in question).

Additional Information

If the request to take down a domain name relates to invalid WHOIS contact details, we recommend that you visit the InterNIC web site for further information. Their web site maybe found online at:

http://www.internic.net/

InterNIC provide specific services for gTLD domain names.

If the request to take down a domain name relates to a civil matter such as IP infringement, we will not intervene by taking down a domain name on the request of a third party. We will however abide by a decision from a recognized arbitrator or competent court of law.

Reservation of Rights

Instra expressly reserves the right to deny, cancel, suspend, lock or transfer any Domain Name registration that it deems necessary in its discretion:

a. to protect the integrity and stability of the Internet and/or DNS
b. to comply with any applicable laws, government rules or requirements, requests of law enforcement;
c. in the event a Domain Name is used in violation of these policies and any other policies regarding recognised domain name regulatory authorities and;
d. in compliance with any dispute resolution process, or to avoid any liability, civil or criminal, on the part of Instra and its affiliates, licensors subsidiaries, officers, directors and employees.