ACCEPTABLE USE AND TAKEDOWN POLICY
Version 1.0

("Acceptable Use Policy")

What is in the Acceptable Use Policy?

As the owner of a domain name, you are required to act responsibly in your use of that domain and in accordance with this policy.
Abusive or malicious conduct in registration of your domain name or in content on a website will not be tolerated by the Registry Operator.

The Registry Operator will act as set out in this Acceptable Use Policy to deal with abusive or malicious conduct of which it becomes aware or which is brought to its attention.

In all cases the Registry Operator reserves the right to bring offending sites into compliance using any of the methods set out in this policy, or others as may be necessary in exceptional cases, whether or not stated in this policy.

Should a complaint be made, the Registry Operator (or its designees) will alert its relevant Registrar partners about any identified threats, and will work closely with them.

Who can bring a complaint under the Acceptable Use Policy?

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the Registry Operator or its partners.

What actions can constitute abusive or malicious conduct?

"Abuse" or "malicious conduct" includes but is not limited to:

Infringement of Intellectual Property; which includes, but is not limited to, passing off as the brand of another, unauthorised distribution of copyrighted material or the sale of counterfeit goods.

Phishing; a criminal activity employing tactics to defraud and defame Internet users via sensitive information with the intent to steal or expose credentials, money or identities.

Malware; malicious software that was intentionally developed to infiltrate or damage a computer, mobile device, software and/or operating infrastructure or website without the consent of the owner or authorized party. This includes, amongst others, viruses, trojan horses, and worms.

P: + 44 845 5644650
E: info@grs.domains
W: www.grs.domains
327 Main Street
Gibraltar GX11 1AA

Domain Name or Domain Theft; the act of changing the registration of a domain name without the permission of its original registrant.

Botnet Command and Control; services run on a domain name that is used to control a collection of compromised computers or "zombies," or to direct Distributed Denial of Service attacks ("DDoS attacks")

Fast Flux Attacks / Hosting; a technique used to shelter phishing, pharming and malware sites and networks from detection and to frustrate 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.

Hacking; the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.

Pharming; the redirecting of unknown users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning.

Spam; the use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and spamming of websites and Internet forums.

Child Pornography; the storage, publication, display and /or dissemination of pornographic materials depicting individuals under the legal age in the relevant jurisdiction.

If the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry Operator, or any of its Registrar partners and /or that may put the safety and security of any registrant or user at risk, the domain name may be cancelled or suspended by the Registry Operator or any of the actions listed in the "what we can do" section below.

How do I complain?

Abuse Point of Contact

All complaints should be addressed to:
abuse@grs.domains

If you are a registrant.

Certain registries require an APM seal to be displayed on the homepage of your domain name. Implementing the seal is extremely easy and instructions will be provided to you when you register.

If you do not plan on using your domain for a website immediately, or at all or there are other reasons why this is not technically possible, please

let us know by completing a self-exception form, details of which will be sent to you upon registration.

Our automated systems will check any website hosted on your domain in 120 days from the registration of your domain. If your website is active, and the APM seal not be found, you will be notified and have 30 days to enact the seal. Should the seal not be enacted within that time, the Registry reserves the right to suspend your domain.

Should your domain be ready for testing before the 120 day period has elapsed, simply click the relevant link in the instructions sent to you to start the validation process immediately.

If you are a Registrar[1] these further obligations apply to you.

1. This Acceptable Use Policy has been incorporated into the Registrar's gTLD Registry-Registrar Agreement ("RRA") at clause 3.10 and the Registrar agrees to comply with all its requirements.

2. Registrar must publish the above Abuse Point of Contact ("POC") on its own website. In addition, the Registry Operator may require the registrant to publish its APM seal on the registrant's website as notified by the Registry Operator to Registrar.

3. Registrars must also notify the Registry Operator's technical services provider of any abuse or malicious conduct (as defined above) of which the Registrar has knowledge, if relevant.

4. Registrar or Registry Operator shall promptly notify the other, where permitted, about any investigation or compliance action (including the nature of the investigation or compliance action by ICANN or any outside party e.g., law enforcement, see relevant section below) and will take appropriate action as obligated by law or the RRA or this policy.

5. Registrar accepts responsibility for any damage or loss suffered by the Registry Operator where the Registrar instructs the Registry Operator to effect a transfer and the Registry Operator effects the transfer except due to any act, omission or negligence of the Registry Operator.

6. Each Registrar must pass the Acceptable Use Policy on to its resellers (if applicable) and ensure ultimately that the Acceptable Use Policy is binding on the gTLD registrants.

7. Registrants must also agree that they will not use their domain for any purposes which are prohibited by the laws of the jurisdiction(s) in which they do business or any other applicable law, namely, that the registrant may not use the domain for any purpose or in any manner which violates a statute, rule or law governing use of the Internet and/

[1] An ICANN accredited registrar currently subject to the terms of a registry registrar agreement with the gTLD Registry Operator.

or electronic commerce, including those statutes related to gaming and ⁄ or online gambling.

8. The Registry Operator's Acceptable Use Policy may incorporate a certification by the registrant that the domain will be used only for licensed, legitimate activities, and not to facilitate piracy or infringements (or an APM Seal).

9. In the case where a URS Complainant[2] under a URS procedure has prevailed the Registry Operator is obliged to offer the option for the URS Complainant to extend a URS Suspended domain name's registration for an additional year and the Registrar is obliged to pay the renewal fee for such domain name extension to the Registry Operator.

What happens to your complaint?

We operate a policy of **Rapid Domain Compliance**, meaning we will provide a timely response to abuse complaints concerning all names registered in the gTLD by Registrars and their resellers.

The Registry Operator's customer support team is operational 24⁄7⁄365. We will endeavour (but cannot guarantee) to address and potentially rectify the issue as it pertains to all forms of abuse and fraud within 24 hours.

Once abusive behaviour is detected or reported, the customer support centre immediately creates a support ticket in order to monitor and track the issue through resolution.

A preliminary assessment will be performed in order to determine whether the abuse claim is legitimate. The Registry Operator will use commercially reasonable efforts to verify the information in the complaint.

If that information can be verified to the best of the ability of the Registry Operator, the sponsoring Registrar will be notified and Registrar will endeavour to investigate the activity within 12 hours and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety, or to provide a compelling argument to the Registry Operator to keep the name in the zone.

If the Registrar has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry Operator may place the domain on "hold".

We will classify each incidence of legitimately reported abuse into two categories based on the probable severity and immediacy of harm to registrants and Internet users.

2 The URS rules and procedures and all URS related definitions used in this policy are available on ICANN's website at http://newgtlds.icann.org/en/applicants/urs/

Category 1:

- Probable Severity or Immediacy of Harm: Low
- Examples of types of abusive behaviour: Spam, Malware
- Mitigation steps:
  - Investigate
  - Notify registrant
- Response times – up to 3 days depending on severity.

Category 2:

- Probable Severity or Immediacy of Harm: Medium to High
- Examples of types of abusive behaviour: Fast Flux Hosting, Phishing, Illegal Access to other Computers or Networks, Pharming, Botnet command and control
- Mitigation steps:
  - Investigate
  - Notify registrant
- Response times – up to 5 days depending on severity.

Uniform Rapid Suspension system ("URS")

We are obliged to follow ICANN's requirements in respect of URS[3]. All definitions in this section are as per the website.

URS Lock: If a URS Provider has instructed us to set up a URS Lock, we are obliged to activate the following EPP-statuses in respect of the affected domain name:

- ServerUpdateProhibited
- ServerTransferProhibited
- ServerDeleteProhibited

URS Suspension: If a URS Provider has instructed us to set up a URS Suspension, we are obliged to redirect the suspended domain name to a webpage that mentions that the URL has been suspended due to a URS Complaint.

URS Rollback: If a URS Provider instructs us to "roll-back" a suspended or locked domain name, we will restore the original information on the domain name at the time of the suspension or lock.

Domain Name Life Cycle: We are obliged to follow the normal domain name life-cycle for a URS Locked domain name. If a domain name that is subject to a URS procedure is purged (if we operate a Redemption Grace Period) or deleted, the URS procedure will automatically terminate.

Extension In the case where a URS Complainant has prevailed, the Registry Operator MUST offer the option for the URS Complainant to extend a URS Suspended domain name's registration for an additional

3 URS High Level Technical Requirements for Registries and Registrars, Version 4_23 September 2013. The URS rules and procedures and all URS related definitions used in this policy are available on ICANN's website at http://newgtlds.icann.org/en/applicants/urs/

year. The Registrar MUST pay the renewal fee for such domain name to the Registry Operator.

What we can do.

We reserve the right for the Registry Operator, at our sole discretion and without notice to any other party, to take the appropriate actions (whether administrative, operational or otherwise) based on the type of abuse, including but not limited to:

lock down of the domain name preventing any changes to the contact and name server information associated with the domain name.

placing the domain name "on hold" rendering the domain name non-resolvable or transferring the domain name to another Registrar.

substituting name servers in cases in which the domain name is associated with an existing law enforcement investigation in order to collect information about the DNS queries and when appropriate, we will share information with law enforcement to assist the investigation.

cancelling or transferring or taking ownership of any domain name, either temporarily or permanently.

denying attempted registrations from repeat violators (see the Section on registrant Disqualification, below).

using relevant technological services, whether our own or third party, such as computer forensics and information security.

sharing relevant information on abuse with other registries, Registrars, ccTLDs, law enforcement authorities (see , security professionals, etc not only on abusive domain name registrations within its own gTLD, but also information uncovered with respect to domain names in other registries to enable such parties to take appropriate action.

We may also take preventative measures at our sole discretion including (without limitation):

DNSSEC deployment which reduces the opportunity for pharming and other man-in-the-middle attacks.

Why will we act?

We will always endeavour to act with reasonable cause. Some examples of where we might act (not limited):

protecting the integrity and stability of the Registry Operator.

complying with any applicable laws, government rules, ICANN or court orders or requirements, requests or orders of law enforcement, or any dispute resolution process.

avoiding any liability, civil or criminal, on the part of the Registry Operator as well as its affiliates, subsidiaries, officers, directors, and

employees.
if required by the terms of the registration agreement or the Registry Registrar Agreement or ICANN.

to correct mistakes made by the Registry Operator or any Registrar in connection with a domain name registration.

during resolution of a dispute of any sort whether or not the dispute appears to be unmerited or unsubstantiated.

What to do if you feel we have taken inappropriate action to deal with abuse or alleged abuse.

We take our goal of tackling abuse extremely seriously and we will always endeavour to take prompt action as set out in this Acceptable Use Policy to deal with abuse or alleged abuse when we believe that there is reasonable justification for the complaint.

However, we are not an adjudicator of any dispute between parties and cannot and do not accept any responsibility for any loss or damage you or anyone else may suffer as a result of any action or omission by us or by anyone else under this Acceptable Use Policy.

If you have an issue with abuse that we are unable to assist with, please approach the appropriate forum for dispute resolution. We will be able to act in the case that you are able to provide:

(i) the final determination of an internationally recognised dispute resolution body or a court of law, settling the inter-parties dispute in your favour or which otherwise mandates us to act as you request.

(ii) any requirement of ICANN or other recognised authority which mandates us to act as you request.

In the case of a wrongful transfer of a domain name, you may also provide written agreement of the Registrar of record and the gaining Registrar sent by email, letter or fax that the transfer was made by mistake or procedural error or was unauthorised (http://archive.icann.org/en/transfers/policy-12jul04.htm)

All notices served under this section should be served by email to legal@grs.domains or otherwise addressed to:

Chief Legal Officer
Global Registry Services Limited
327 Main Streeet,
Gibraltar GX11 1AA

Proof of posting is not proof of delivery. You are responsible for all costs, fees, damages and other expenses relating to any action you take, or which you require us to take, under this section.

How we work with law enforcement.

The Registry Operator will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such a response shall include, at a minimum, an acknowledgement of receipt of the request, questions or comments concerning the request, and an outline of the next steps to be taken by the Registry Operator for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by the Registry Operator and involves the type of activity set out in the Acceptable Use Policy, the sponsoring Registrar will endeavour to further investigate the activity within 24 hours and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the Registry Operator to keep the name in the zone.

If the Registrar is not able to take the requested action after 24 hours or if the matter is urgent, (i.e., is unresponsive to the request or refuses to take action), the Registry Operator may place the domain on "hold".

How we disqualify registrants.

Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations, through the possible loss of all registrations.

Registrants, their agents or affiliates found through the application of the Acceptable Use Policy to have repeatedly engaged in abusive registration may be disqualified from maintaining any registrations or making future registrations.

This will be triggered when the Registry Operator backend services provider's records indicate that a registrant has had action taken against it an unusual number of times through the application of our Acceptable Use Policy.

In addition, name servers that are found to be associated only with fraudulent registrations may be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.

The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to engage in such behaviour from registering domain names.

For a registrant to be placed on a list of bad actors, the Registry Operator will examine the factors noted above, and such determination shall be made by the Registry Operator at its sole discretion.

Once the Registry Operator determines that a registrant should be placed onto the list of bad actors, the Registry Operator will notify its Registry Operator backend services provider, who will be instructed to cause all of the registrant's second-level domains in the gTLD to resolve to a page which notes that the domain has been disabled for abuse-

related reasons.

The second-level domains at issue will remain in this state until the expiration of the registrant's registration term or a decision from a UDRP panel or court of competent jurisdiction requires the transfer or cancellation of such domains.