. RUHR Rapid Takedown Policy

The present conditions, which apply to registrars and registrants of [.RUHR] domains define clearly and unambiguously how the registry will proceed if abuses are brought to its notice. These positions do not replace the Uniform Dispute Resolution Policy (UDRP) or Uniform Rapid Suspension (URS) or other proceedings for resolving disputes between third parties. Instead, the conditions are aimed at abuses which pose a threat to public safety and, as a result, to all .RUHR users.

1. Abuses

a An abuse for the purpose of these conditions is defined as follows:

- **Violation of applicable laws or regulation, in particular the provisions of the German Criminal Code (StGB), the German Youth Protection Act (JuSchG) and the German Interstate Treaty on the Protection of Minors in the Media (JMStV),**
- **Use of a domain to publish content which incites to hatred against parts of the population or against a national, religious or ethnic group, content which glorifies violence, content which violates the human dignity, content which denies or plays down acts committed under the National Socialist regime,**
- **Distribution of child abusive material,**
- **Use of a domain name for the dissemination of spam, i.e. unsolicited bulk electronic communication (e-mail, instant messaging, on websites, in forums or mobile messaging) or advertising a domain name by means of spam,**
- **Use of a domain name for Distributed Denial-of-service attacks ("DDoS attacks"),**
- **Use of domain names in phishing activities, tricking Internet users into divulging personal data such as names, addresses, usernames, passwords, or financial data,**
- **Use of domain names in pharming, such as DNS hijacking and DNS cache poisoning,**
- **Use of domain names for the intentional distribution of malicious code such as spyware, malware, keylogger bots, viruses or trojans,**
- **Use of domain names to command and control botnets, i.e. a network of compromised computers or "zombies,"**
- **Use of domain names in activities intended to gain illegal access to other computers or networks ("hacking"), as well as any activity to prepare for such a system penetration, or**
- **Use of a domain name fast flux hosting, disguising the location of Internet addresses or Internet services."**

b The list of abuses in these conditions is not exhaustive and does not exclude other conceivable abuses.

c Violations of these conditions also constitute violations of the .RUHR Acceptable Use Policy.

d The registry is entitled to identify and pursue abuses at its own initiative by evaluating blacklists, malware and phishing feeds and/or similar sources.

2. Reporting abuses

a The registry provides a website at www.dotruhr.de which gives third parties an opportunity to report suspected abuses at .RUHR domains. The registry provides a contact form for this

purpose. The registry also provides a phone number for use during normal business hours and an e-mail contact.

b Third parties using these contact opportunities are obliged to describe and evidence the situation covered by the abuse report as fully as possible. They are also obliged to give the registry at least one contact (e.g. e-mail address and/or phone number). The registry will use this data exclusively for the purposes of the reported abuse and will not in any event forward it to any third party. An exception to this is forwarding to government agencies (e.g. policy and/or public prosecutors) if the registry initiates criminal proceedings in connection with a specific abuse.

c Reported abuses are immediately assigned a unique case number which is notified to the third party, preferably by e-mail. The registry is entitled but not obliged to request further information from the third party which is needed to resolve the situation.

3. Review of abuses, threat levels

a The registry will use the forwarded data to determine if there is an abuse which results in the consequences specified in the present conditions. The registry is entitled to review and evaluate the situation based on the forwarded data. The registry is further entitled but not obliged to make independent investigation to clarify a reported situation.

b In case of doubt, the registry is entitled – regardless of the threat level and the person or agency reporting the abuse – to have the abuse investigated by qualified third partíes.

c Third parties involved in a specific abuse will be notified as far as possible by the registry of the current status, classification and measures taken.

d The registry will classify abuses as one of three threat levels, depending on which the registry will determine further measures and response times in the specific instance.

- **Threat level 1:** A serious abuse posing concrete danger to public security: the registry will process the case within 48 hours after the report.
- **Threat level 2:** A serious abuse which does not immediately pose a concrete threat to public security, but gives reason to fear that such danger is imminent; the registry will process the case within 72 hours after the report.
- **Threat level 3:** An abuse which the registry could not confirm on the basis of the forwarded data and its own investigations; the registry will close the reported abuse case.

e For classification purposes, the registry will first consider the danger to public security resulting from a specific abuse (the registry's decision). The registry will also consider the interests of the registrant in the specific instance, as far as possible. The registry will document the material stages and results of the investigation electronically. This also applies to measures taken by the registry under (6) below.

f A critical abuse where the concrete danger to public security clearly outweighs the interests of the registrant **always** (but not exclusively) arises if the registry is notified by an investigatory body (e.g. police, public prosecutor), courts or government agencies of a

concrete issue. The registry classifies such ases as **threat level 1**. A critical abuse also arises if third parties other than a public agency notify the registry that .RUHR domains are being used for

- offensive, indecent, sexually explicit, obscene or defamatory material suitable for promoting or supporting racism, fanatacism, hate, physical violence or illegal acts (explicitly or implicitly);
- pornographic content, services and/or products which violate criminal law and/or other law;
- dissemination of malware and/or other damaging software (viruses, trojans, keyloggers etc);
- pharming and/or phising websites.

g Other verifiable abuses reported to the registry where concrete danger does not as yet clearly outweight the interests of the registrant are classified as threat level 2. Before the registry takes measures, the registrant involved is asked to respond to the abuse report.

h Abuses where no danger to public security is apparent and which cannot be verified by the registry are classified as threat level 3. In such cases the registry will not take any measures against the registrant involved. The registrant and third party are notified of the registry's decision by e-mail.

i The registry notes that if there is suspicion of illegal or criminal activities it is entitled and possibly also obliged to report such cases to the public prosecutor's office.

4. Notification of responsible registrar

a If the registry has determined there is an abuse under (3) above, this is notified to the registrar for the .RUHR domain in question. The registrar generally has further information through the direct contractual relationship with the registrant which can help resolve the abuse.

b The registry will notify the registrar involved if and within what period notification of the registrant in question is required, or whether such notification must be omitted (cf. 4e below).

c Registrars are obliged to resolve the abuse or take the necessary measures within a set period, as determined by the registry's threat level under (3) above. If the registrar does not reply within the set period, the registry is entitled to take measures under (6) below.

d The registrar in question will notify the registrant involved of the reported abuse by e-mail and/or phone whenever possible. The registrant is notified of the concrete abuse and threat level.

e The registry notes that in certain cases it might be illegal to notify the registrant in advance of an abuse. In such cases the registrant will not be given the information under 4c above. In these cases the registrant is notified as far as legally permissible of the measures taken by the registrar and/or registry.

5. Registrant's right of response

a The registrant in question may be entitled to respond by e-mail to the accusation of abuse. This does not apply to a case under 4e above. The period for a registrant's response to the registrar involved is determined by the threat level set by the registry:

- For threat level 1 the registrant must respond within 24 hours of the e-mail being sent to the registrant. The registrar can set a shorter period if the concrete case requires.
- For threat level 2 the registrant must respond within 48 hours of the e-mail being sent to the registrant. The registrar can set a shorter period if the concrete case requires. The registrar is further entitled to require the registrant to carry out specific measures (e.g. remove content posted on a .RUHR domain).

b If the Registrant fails to respond to a concrete abuse in a timely manner or at all, **or if the measures required by the registrar or registry are not carried out, the registrar or registry is entitled to determine and take the measures required under (6) below.**

c If the registrant responds to the concrete abuse, the registry notes that this response does not affect the classification made under (3) above. The registry will take the registrant's response into account in the context of the measures under (6) below.

d If the registrant responds and carries out the measures required by the registrar or registry and/or otherwise remedies the identified abuse, the registrar or registry will take this into account in the context of the measures to be taken under (6) below. Measures under 6a generally do not apply in such cases.

6. Measures by the registrar/Registry/escalation levels

a The registrar or registry is also entitled to take measures for the .RUHR domain in question which are suitable for reliably ending a concrete abuse in accordance with the classification. If the violation of the AUP is not obvious from the available documentation or the content made available under the .RUHR domain in question, the registry will have the case reviewed by a specialist law firm and will carry out its recommendations. For notifications by public authorities, the review is limited to obvious illegality of the required measure. The registrar or registry is also entitled e.g.

- to deactivate the nameservers for the domain in question, or
- to delete the .RUHR domain in question, or
- to set a registry lock, hold or similar status for the .RUHR domain in question.

A domain should only be deleted if the domain in question is itself the cause of the legal violation. Otherwise, it must only be deactivated for the time required to remedy the abuse or a third party order to deactivate it is rescinded. In any case the registry will always implement legally enforceable rulings of a German court or an order legally enforceable in Germany.

b In the event of one or more abuses, the registrar or registry is further entitled with regard to the registration agreement in question

- to require the registrant to remove the content leading to the abuse report, or
- to warn the registrant of their violation of their obligations under the registration agreement, or
- to terminate the registration agreement summarily for important reason, or
- to file a criminal complaint against the registrant, or
- to make reactivation of a .RUHR domain conditional on signature of a cease and desist declaration with penalties under which the registrant undertakes to refrain from abusive use in future.

c The measures under 6a and 6b are set by the registrant ***[sic – registrar]*** or registry at their due discretion and taking into account the registrant's response under (5) above. The registry will specifically take into account in their decision the number of abuse cases reported for the registrant in question.

7. Other

a This does not affect further claims for damages and/or indemnification by the registrar or registry.

b Regardless of the preceding provisions the parties reserve the right to use other arbitration proceedings or apply to the regular courts.