Acceptable Use Policy

This Acceptable Use Policy sets out the prohibited actions by a Registrant or User of every registered .NRW Domain Name.

This Acceptable Use Policy forms part of the Registry Policies that apply to and govern the registration of a .NRW Domain Name. Words in capitals used in this policy have the meaning set out in the Definitions Document.

The current version of this Acceptable Use Policy applies to any .NRW Domain Name registered, no matter when or how registered or renewed. In the event a Registrant licenses or leases a Domain Name or creates any sub-domain or otherwise allows any other person to use the Domain Name, the Registrant shall be responsible for all activity related to the Domain Name and any sub-domain, including compliance with the Registry Policies and the acts of the User shall be deemed to be the act of the Registrant for the purposes of the Registry Policies.

The Registry or Registrar is in no way obliged to review or monitor legality of a specific domain name or the content and/or services offered there under.

1. Lawful Use

The registration and use of .NRW Domain Names must be for lawful purposes. The Registrant is solely responsible for the legality of the Domain Name registration and the content and services made available there under. Further, the Registrant is responsible for ensuring compliance with the Registry Policies.

2. Prohibited Domain Name registrations

A Registrant must not register or attempt to register Domain Names, which:

a) violate applicable law or infringe upon third parties' rights, i.e. names of persons or legal entities, trademarks or otherwise legally protected designations;

b) are identical or confusingly similar to:
   - the names of governmental agencies of the State of North Rhine-Westphalia and their official acronyms and established shortforms;
   - the names of certain companies from which the State of North Rhine-Westphalia holds at least 50% of the shares or has a share on the profits of at least 50%;
   - the names of municipalities in North Rhine-Westphalia;
   - the names of other corporate bodies under public law that are under survey of the State of North Rhine-Westphalia;
   - the names of German Federal Authorities and their official acronyms as well as prevalent short forms;
   - the names of religious groups under German public law;
   - the names of authorities of the European Union; or
   - Country names as listed in the ISO 3166-2 list.

3. Prohibited Content

A Domain Name must not be used to publish, distribute or communicate (including through links forwarding or framing):

a. material that infringes upon the intellectual and/or industrial property rights of another person or entity, including by piracy, counterfeiting, or otherwise. Intellectual and/or industrial property rights include, but are not limited to, current and future: copyrights, design rights, patents, patent applications, trademarks, rights of personality, and trade secret information;

b. images or materials that are prohibited by or constitute an offense under applicable laws;

c. material that includes, by way of example and without limitation, real or manipulated images depicting the sexual exploitation of children, bestiality or comparable;

d. material containing threats or detailed instructions regarding how to commit a crime or encourages conduct that may constitute a criminal offence;

e. defamatory material or material 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,

f. software, technical information or other data that violates applicable export control laws or anti-circumvention provisions; or

g. confidential or personal information or data including confidential or personal information about persons that was collected without their knowledge or consent;

h. content that suggests that the operator is an institution or a party eligible for a designation referred to in section 2.b above.

4. Malicious code, phishing etc

A Domain Name must not be used to publish content or in any other manner:

a. is capable of disruption of systems in use by other Internet users or service providers (e.g., distribution of viruses, malicious botnets, or malware); or

b. seeks or attempts to seek authentication or login details used by operators of other Internet sites, or misleads or deceives visitors to the site that the site has an affiliation with the operator of another Internet site (i.e., phishing, keylogger bots, pharming, DNS cache poisoning).

c. attempts to disguise the location of Internet addresses or Internet services (e.g. fast flux hosting).

5. Electronic Mail

A Domain Name must not be used for any of the following activities:

a. communicating, transmitting or sending unsolicited bulk email messages or other electronic communications (“junk mail” or “spam”) of any kind including, but not limited

to, unsolicited commercial advertising and informational announcements as prohibited by applicable law.

b. communicating, transmitting or sending any material by email or otherwise that harasses another person or that threatens or encourages bodily harm or destruction of property.

c. communicating, transmitting, sending, creating, or forwarding fraudulent offers.

d. adding, removing, modifying or forging any network header information with the effect of misleading or deceiving another person or attempting to impersonate another person by using forged headers or other identifying information (i.e., spoofing).

6. Disruption of the Registry Network

A Domain Name must not be used for the purpose of:

a. restricting or inhibiting any person in their use or enjoyment of the Registry's network or a Domain Name or any service or product of the Registry.

b. actually or purportedly reselling the Registry's services or products without the prior written consent of the Registry.

c. communicating, transmitting, or sending very large or numerous pieces of email or illegitimate service requests (e.g., a DDoS attack).

d. providing false or misleading information to the Registry or any related party.

e. facilitating or aiding the transmission of confidential information, private, personal or stolen data, such as credit card information (without the owner's or cardholder's express written consent).

7. Network Integrity and Security

Registrants are prohibited from:

a. circumventing or attempting to circumvent the security of any host, network or account (i.e., cracking or hacking) on, related to, or accessed through the Registry's network. This includes, but is not limited to:

    i. accessing data not intended for such Registrant;

    ii. logging into a server or account which such Registrant is not expressly authorised to access;

    iii. using, attempting to use, or attempting to ascertain a username or password without the express written consent of the operator of the service in relation to which the username or password is intended to function;

    iv. probing the security of other networks; and/or

v. executing any form of network monitoring which is likely to intercept data, of any nature, not intended for the Registrant.

b. effecting any network security breach or disruption of any Internet communications including, but not limited to:

i. accessing data of which such Registrant is not an intended recipient; and/or

ii. logging onto a server or account which such Registrant is not expressly authorised to access.

For the purposes of this section, “disruption” includes, but is not limited to: port scans; TCP/UDP floods; packet spoofing; forged routing information; deliberate attempts to overload or disrupt a service or host; and/or, using the Registry’s network in connection with the use of any program, script, command, or sending messages with the intention or likelihood of interfering with another user's terminal session by any means, locally or by the Internet.

8. Order of Court of Other Governmental Authority

A Domain Name must not be used in a manner that is in contempt of, or contrary, to the orders of a court or the orders or other direction of a competent governmental authority within Germany or in any other relevant jurisdiction.

9. Failure to Transfer

A Registrant must not fail to transfer a Domain Name to a third party if, as evidenced in writing, the Registrant acted as an agent of the third party when registering for the Domain Name, or as ordered by a court of competent jurisdiction or UDRP provider.

10. Enforcement

The Registry may (but is not obliged to), in its sole discretion (including based on reports made to the Registry by third parties), and without prior notification, suspend, transfer, or terminate a Registrant’s service, including all and any of the Registrant’s Domain Name registrations, if the Registry believes:

a. a violation of this Acceptable Use Policy or any other Registry Policy has occurred or a reasonable indication that such a violation may have occurred; and/or

b. suspension and/or termination may otherwise be in the public interest.

When an incident is reported to the Registry, the Registry will first consider the danger to public security resulting from the specific abuse in its own discretion. The Registry will also consider the interests of the Registrant in the specific instance. In cases of critical abuse where the concrete danger to public security clearly outweighs the interests of the Registrant, decisions on sanctions can be made without obtaining further information.

In cases of other verifiable incidents, the Registry shall give the Registrant the opportunity to respond to the abuse report. In order to do so, the Registry shall contact the Registrant via the Registrar. Registrars will undertake to notify the Registrant involved. The Registrant will be

given a deadline to respond. In case the Registrant fails to respond in a timely manner, a decision will be made based on the facts available. Where the Registrant responds or cures the alleged breach, the Registry will take the Registrant's response into account when making a decision.

11. Modification of Network Data

In the course of its duties to comply with ICANN Policies, UDRP, URS, or CRS decisions, court or other governmental orders, or other duly-qualified law enforcement requests, or to protect the integrity and functioning of its networks, the Registry, in its sole discretion, reserves the right to:

a. remove or alter content, Zone File data and/or other material from its servers that violates the provisions or requirements of this Acceptable Use Policy;

b. re-delegate, redirect or otherwise divert traffic intended for any service;

c. notify operators of Internet security monitoring services, virus scanning services and/or law enforcement authorities of any breach or apparent breach of this Acceptable Use Policy or other Registry Policies; and/or

d. terminate access to the Registry's network by any person or entity that the Registry determines has violated the provisions or requirements of this Acceptable Use Policy.

12. Limitation and Indemnity

THE REGISTRANT'S ATTENTION IS PARTICULARLY DRAWN TO (A) THE LIMITATION OF LIABILITY AND INDEMNITY PROVISIONS SET OUT IN THE DOMAIN NAME REGISTRATION POLICY THAT THE REGISTRANT HAS AGREED TO APPLY TO THE DOMAIN NAME, AND (B) THE FACT THAT THE REGISTRY (AND REGISTRY RELATED PERSONS) CAN DIRECTLY ENFORCE THESE PROVISIONS AGAINST THE REGISTRANT.