RNIDS

Pursuant to Article 4 of the Statute of the Serbian National Internet Domain Registry Foundation (hereinafter: **RNIDS**), Article 8, paragraphs 9 and 10 of the General Terms and Conditions for National Domain Name Registrations (hereinafter: "General Terms"), on 22 December 2025, the RNIDS Board of Governors has passed these:

RULES ON PROCEDURES AND MEASURES FOR CASES OF INTERNET DOMAIN ABUSE

Subject matter of the Rules

Article 1

These Rules on Procedures and Measures for Cases of Internet Domain Abuse (hereinafter: "Rules") lay down procedures to be followed and measures to be taken in reporting, verifying and resolving cases of abuse of national internet domains (.rs and .срб).

The Rules set out the rights and obligations of RNIDS, accredited registrars, registrants and third parties in relation to the detection and reporting of abuses, as well as appropriate measures to be taken when necessary, as further laid down by these Rules.

These Rules define the types of abuse of national internet domains, the criteria for assessing abuse, reporting and report processing mechanisms, as well as measures that may be taken against abuses.

Terms and definitions

Article 2

For the purposes of these Rules, the following terms shall have the following meanings:

Domain name abuse (malicious use) shall refer to any action whereby a domain name is used, maintained, or transferred contrary to laws, regulations and RNIDS Rules, that is, in any way that compromises the security and stability of information systems and the security of other internet users.

Internet domain (internet domain name) shall refer to a textual designation representing a collection of devices and services connected into a single administrative and technical unit.

DNS (Domain Name System) shall refer to the foundational Internet service that permits the translation of textual addresses into numerical ones and vice versa.

RNIDS / Serbian National Internet Domain Registry) shall refer to an organization that manages and maintains a unified electronic database of registered national internet domain names and other data corresponding to them, as well as a system of authoritative DNS servers for national internet domains.

Registrant shall refer to a legal entity or natural person who, in accordance with the provisions of the General Terms, registers a domain name with the Registry.

Administrative contact shall refer to a legal entity or natural person authorised by the Registrant to receive from RNIDS and supply to RNIDS data of significance for the registration of the domain name, for and on their behalf.

RNIDS accredited registrar (heretofore and hereinafter: "**accredited registrar**") shall refer to a legal entity or sole proprietorship with a registered office in the Republic of Serbia that has been authorised by RNIDS to provide domain name registration services within the national internet domain registry for and on behalf of RNIDS. An accredited registrar provides domain name registration services at the request of the registrant or administrative contact in accordance with the General Terms.

Interested party shall refer to any legal entity or natural person who has a legitimate interest in connection with the registered internet domain and/or who reports abuse of the internet domain and/or who suffers consequences from its abuse, i.e. any person who has a legitimate interest in connection with the reported abuse of the internet domain.

WHOIS shall refer to the **publicly accessible domain name database** containing information about registered internet domains as laid down in the General Terms.

Types of abuse of internet domains

Article 3

Abuses of an internet domain as addressed by these Rules shall include:

- Use of a domain for the purposes of deception, fraud, identity or data theft, distribution of malicious software, or other similar forms of fraud;

- Impersonation with the aim of deceiving users and obtaining confidential information, such as passwords, credit card numbers or other personal information (phishing);

- Providing incorrect, incomplete or false information during registration or in connection with the use of a domain name.

RNIDS shall assess whether a specific action constitutes abuse of an internet domain in proceedings following receipt of a report, or based on information from other sources, in accordance with these Rules, applicable regulations and adopted standards and

practices in the area of internet domain management, after which it shall decide on appropriate measures to be taken.

In cases where abuse of the internet domain is repeated, either in terms of the same act or in terms of multiple abuses by the same person (or related persons), RNIDS shall take the repetition into account as an aggravating circumstance when assessing the severity of the abuse and deciding on the measure to be taken. In such cases, RNIDS may apply more severe measures, including permanently prohibiting the registration of new domains, notifying the relevant authorities, and other measures provided for in these Rules and detailed in Article 5.

Reporting abuse of internet domains

Article 4

RNIDS may collect information on the registration and use of malicious internet domains and the abuse of internet domains, both on its own initiative and based on reports filed by third parties, i.e. interested parties.

Internet domain abuse can be reported by the means listed below.

By filling in an online form or by email: the form should be downloaded from the RNIDS website, filled in properly and sent to the email address designated for that purpose.

A report may also be submitted to the accredited registrar, in which case the accredited registrar shall forward the report to RNIDS immediately, within 48 hours at the latest.

RNIDS may also receive reports via specialised services that detect and report malicious registrations.

An internet domain abuse report must comprise the following information:

- **Information on the reporting party**:
  - first and last name or name of legal entity,
  - contact information (phone number and/or email address).

- **Information on the internet domain** being reported:
  - name of internet domain,
  - date and time when the abuse was observed,
  - the specific URLs or subdomains on which the abuse has occurred, if applicable,
  - the web hosting provider, if known.

- **Description of the abuse**:
  - a detailed description of the abuse, including the type of abuse (e.g. phishing, malware, fraud), and any damage that has occurred.

- **Evidence and information** supporting the allegations in the report, such as:

- screenshots, log files, emails, links to malicious sites and other relevant evidence.

- **Other information** that the interested party considers relevant for a proper understanding of the abuse or will facilitate faster, easier and more expedient resolution of the case.

A report of internet domain abuse may be submitted by an interested party, that is, any natural person or legal entity who believes that abuse has occurred, including, but not limited to, persons whose rights have been violated.

RNIDS may, on its own initiative, or based on other sources of information, observe or suspect the misuse of an internet domain and initiate proceedings in accordance with the provisions of these Rules, even if a report was not filed by a specific person. In such cases, RNIDS shall take appropriate actions, including verification of the internet domain data, and notification of the accredited registrar and registrant, as well as taking measures such as suspension of the domain.

Acting on a report

Article 5

I Investigation of the report

Upon receipt of a report on the abuse of an internet domain, RNIDS shall conduct an investigation into the matter, including the following actions:

- **Reviewing the report** – RNIDS shall review the data submitted in the report, including the facts stated in it, the evidence provided and any additional information that may be relevant to assessing whether abuse has taken place.

- **Investigation of the domain name abuse and the registrant's activities** – RNIDS shall conduct an examination of the internet domain in question, including reviewing all known activities connected with the domain, and analysis of data available about the registrant in its database or from other sources, in order to determine whether the domain has been misused or there is a reasonable suspicion that abuse has occurred. RNIDS may use available technical and analytical tools and services for this purpose, in order to identify security risks or detect malware, phishing and other forms of abuse of internet content and infrastructure.

- **Additional verification** – if necessary, RNIDS may request additional information from the applicant, the Accredited Registrar with whom the domain was registered, as well as from other relevant persons or institutions in order to make a decision regarding further action.

RNIDS shall not act on a report if:

- it does not contain all the necessary data and evidence to facilitate the investigation of the report,
- contains incorrect, imprecise or contradictory information,
- RNIDS cannot determine that abuse has occurred based on the submitted data,
- it refers to abuses that do not fall under the definitions of these Rules.

Depending on the form and estimated scope of the threat or the type of violation, RNIDS shall also inform the relevant authorities regarding the report and the internet domain abuse, and coordinate further steps with them.

II Suspension of the domain and identification of the registrant

1. Domain suspension

After RNIDS has received a report and conducted the formal verification per section I, and if the report has been filed in good order and it is determined that there has been abuse of the internet domain or suspicion of abuse is well-founded, RNIDS shall take the following steps:

- **Temporary suspension of the domain**:

  Depending on the nature of the abuse, RNIDS distinguishes between:

  a) **abuses that pose an immediate danger to the security of users and information systems**, such as, for example, the distribution of malware, phishing and compromising critical infrastructure. In such cases RNIDS may immediately, without delay, and before starting the registrant identification procedure or moving forward with its investigation, suspend the abusive domain in order to prevent further harm;

  b) **lower-risk abuses**, such as incomplete data, cessation of trading prior to provision of evidence of a successor entity, etc. In such cases the domain name shall not be suspended until it is determined that the data is incorrect and until expiry of the deadline referred to in the General Terms;

  Temporary suspension of the internet domain that is abused, shall disable its further use. This measure shall be preventive and shall aim to preclude possible further abuses until all relevant facts are established and data is updated.

- **Notification of the registrant**: RNIDS shall, via the accredited registrar, notify the registrant using the available contact details regarding suspension of the internet domain. The notification shall state the reasons for the suspension

and provide instructions on the further steps that the registrant must take in order to resolve the situation.

- **Notification of the accredited registrar:** RNIDS shall also inform the accredited registrar with whom the internet domain, that is abused, was registered regarding the suspension, and if there is any doubt regarding the registrant's identity ask that they contact the registrant requesting a statement confirming their identity, as further defined in section 2 of this article.

2. Identification of the registrant

In order for the identity of the registrant to be confirmed, further steps to be taken in resolving the dispute and the domain potentially reinstated, the registrant must identify themselves to the accredited registrar as follows:

- **Filling in and notarising the statement**: The registrant shall be provided with a statement form by the accredited registrar, which they need to fill in with accurate and up-to-date information. After filling in the statement, the registrant must get it notarised by a notary public to confirm the authenticity of the information provided. For foreign registrants this statement should be certified by the competent authority of the country of citizenship of the registrant and submitted to RNIDS, officially translated into English.

- **Submitting the statement to the accredited registrar:** The registrant should submit the notarised statement within 15 days to their accredited registrar, who will forward it to RNIDS. This step is crucial for verification of identity and enables the Registry to update or confirm existing information about the registrant.

III Actions taken with domains suspended by RNIDS

1. Domain activation

If the registrant confirms their identity in the manner provided for in these Rules and submits a notarised statement, RNIDS may, considering the circumstances of the specific case, return the domain to an active state if, based on the available facts, it determines that the risk is not significant or there is no risk, or that the malicious content or service located on that internet domain name has been removed.

The accredited registrar/registrant may only request reactivation of the domain after having provided evidence that the domain no longer hosts any malicious content.

In cases where there is only a suspicion of abuse, RNIDS may decide not to take further measures, but to leave resolution of the dispute to the interested party, to whom it may provide relevant data about the registrant at their request, in accordance with the General Terms and applicable laws.

2. Continuation of suspension

If the circumstances of the specific case so dictate, and especially in the cases outlined below, RNIDS shall reserve the right to continue suspension of the internet domain without explanation:

- if the registrant fails to confirm their identity in accordance with these Rules, until identification is provided or until such time as the domain's registration period expires;

- if, on the basis of an abuse report or information received by RNIDS by other means, and analysis carried out by RNIDS, it is clearly determined that specific abuse of the internet domain has taken place, that the abuse is ongoing, until such time as the abuse is stopped or until the competent authority renders a decision on the matter.

IV Record-keeping

RNIDS shall keep records of internet domains suspended due to abuses under these Rules. RNIDS may put an internet domain that is frequently abused on the list of reserved domains, thereby preventing registration of the specific domain.

V Repeated abuse

Abuse of an internet domain per these Rules shall be considered repeated abuse if:

- the same person (registrant), or a person associated with them, abuses the same or a different internet domain multiple times;
- the same type of abuse is repeated on the same internet domain even after the measures taken by RNIDS;
- there is data in RNIDS' records indicating that the person concerned had previously been reported under proceedings that ended with a determination of abuse.

In the event that repeated abuse is identified, RNIDS may take one or more of the following measures:

- decline to restore the domain to an active state;
- extend suspension of the internet domain or suspend it until its expiration;
- notify the competent authorities (e.g. police, public prosecutor, etc.) for their further action;
- put the domain on the list of reserved domains.

Repeated abuse shall be considered an aggravating circumstance when deciding on measures to be taken, with no further warnings required to be given to the registrant.

Final provisions

Article 6

These Rules shall come into force on the eighth day after their publication.

In the event that any provision of these Rules should be made void or invalid, this shall not affect the other provisions of these Rules, which shall in such case remain in force.

Other relevant general enactments of RNIDS, if applicable, as well as relevant regulations and procedures pursuant to applicable laws of the Republic of Serbia, shall apply to all subject matter not addressed by these Rules.

Belgrade, December 22, 2025

Nenad Orlić

Chair of the BoG