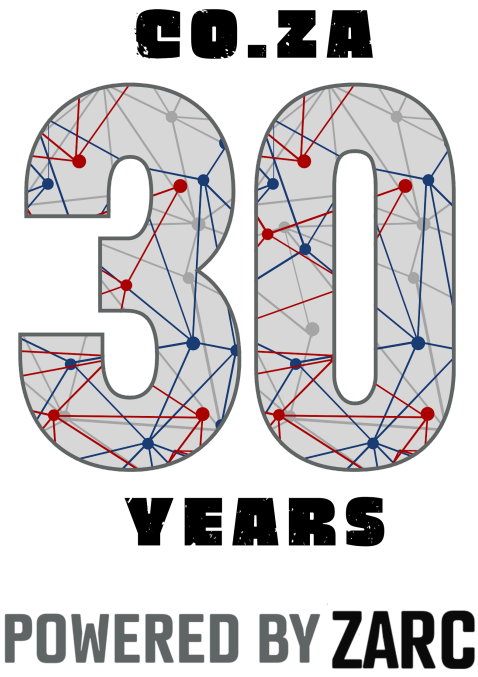
COMPLAINTS, DOMAIN NAME ABUSE AND TAKEDOWN CHARTER



Published Date: January 2026
Version: 002
Author: ZARC Policy Team

1. Purpose

The purpose of this Charter is to define the framework within which the ZA Registry Consortium (ZARC) receives, manages, investigates, and resolves complaints and reports of abusive or unlawful domain name activity within the .ZA Second Level Domains (SLDs) under its administration, namely co.za, org.za, net.za, and web.za. The Charter ensures compliance with the Registry Operator Agreement (ROA) with the .ZA Domain Name Authority (ZADNA) and applicable legislation, including the Electronic Communications and Transactions Act 25 of 2002, the Protection of Personal Information Act 4 of 2013 (POPIA), and other relevant laws.

2. Policy Scope

This Charter covers complaints submitted by members of the public, registrars, registrants, law enforcement, or any interested party, and includes complaints regarding inaccurate WHOIS data, unlawful transfers, breaches of published policies, and domain name abuse such as phishing, malware, or other unlawful online content or activity.

3. Definitions

For purposes of this Charter, unless the context indicates otherwise—

3.1 "Abuse" means any use of a domain name that is unlawful, fraudulent, deceptive, misleading, or otherwise harmful to Internet users or to the security, stability, or reputation of the Domain Name System (DNS). Abuse includes, without limitation, phishing, pharming, malware or ransomware distribution, botnet command-and-control, spam, denial-of-service attacks, distribution of child sexual-exploitation material, and illegal access to computer systems.

3.2 "Accredited Registrar" or "Registrar" means a person or entity accredited by ZARC in terms of the Registry–Registrar Agreement and authorised to register .ZA Second Level Domains on behalf of registrants.

3.3 "Applicant" or "Registrant" means the individual or entity in whose domain name is registered within the .ZA-administered namespace/s.

3.4 "Board" means the Board of Directors of ZARC.

3.5 "Charter" means this Complaints, Abuse and Takedown Charter or Policy, as amended and Published on ZARC's official website on https://zarc.web.za/za-sld-policies/ from time to time.

3.6 “Complainant” means any person or organisation submitting a complaint or abuse report under this Charter, including members of the public, registrants, registrars, law-enforcement bodies, or other Trusted Notifiers.

3.7 “Complaint” means a formal written submission made to ZARC alleging breach of registry policy, registrar misconduct, inaccurate WHOIS data, or any other matter within the scope of this Charter.

3.8 “DNS” or “Domain Name System” refers to the hierarchical naming system that translates domain names into IP addresses and enables Internet communication.

3.9 “NIS2 Directive” refers to Directive (EU) 2022/2555 of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, insofar as it applies to DNS service providers and registries handling EU-related data.

3.10 “Personal Information” has the meaning assigned in the Protection of Personal Information Act 4 of 2013 (POPIA) and includes information relating to an identifiable, living natural person or existing juristic person.

3.11 “Registry Operator Agreement (ROA)” means the agreement between ZARC and the .ZA Domain Name Authority (ZADNA) authorising ZARC to operate specific .ZA Second Level Domains.

3.12 “Second Level Domain (SLD)” means a domain directly under the .ZA country-code top-level domain, including co.za, org.za, net.za, and web.za

3.13 “Trusted Notifier” means a law-enforcement agency, regulatory authority, national Computer Security Incident Response Team (CSIRT), or other organisation formally recognised by ZADNA or ZARC as a credible and competent source of verified abuse notifications eligible for expedited handling.

3.14 “WHOIS/RDAP Services” means the public registration-data query services operated by ZARC to provide information about registered domain names, subject to access, privacy, and data-protection provisions contained in ZARC’s WHOIS and RDAP Access Policy.

3.15 “ZADNA” means the .ZA Domain Name Authority established under Chapter X of the Electronic Communications and Transactions Act 25 of 2002.

3.16 “ZARC” or “the Registry” means ZA Registry Consortium (Pty) Ltd, the Registry Operator for the .ZA SLDs under its management.

4. Key Principles and Scope of Complaints

4.1 ZARC manages complaints and abuse reports in accordance with the principles of legality, fairness, transparency, responsiveness, and confidentiality. Personal information obtained in the course of handling complaints is processed in accordance with POPIA and GDPR, and registry operations subscribe to information security measures prescribed by ISO 27001 standards as well as by the NIS2 Directive.

4.2 ZARC will process complaints that relate to, inter alia, one or more of the following Matters:

4.2.1 Inaccurate or incomplete WHOIS information.

4.2.2 Unlawful transfer and updates.

4.2.3 Domain name registration and management services of a .za accredited Registrar and/or reseller.

4.2.4 Violations of ZARC's published Registry Terms and Conditions or Published Policies.

4.2.5 Disputes between Registrars and their resellers in so far as they relate to a breach of possible breach of a the Registrar Accreditation Agreement or any Published Terms and Conditions and/or Published Policies.

4.2.6 Domain Name Abuse Practices as further defined in this policy.

4.3 ZARC will NOT handle complaints that relate to one or more of the following matters:

4.3.1 Generic Top Level Domain Names (example, .com, .africa, .org) or other country code top level domain name (ccTLD) (example, .ng, .zm).

4.3.2 Webhosting, website management or website design services.

4.3.3 Internet connectivity and access or email services.

4.3.4 Alleged violations of the Electronic Communications and Transactions Act of 2002 or any other laws.

4.3.5 Ownership rights to a domain name.

4.3.6 Commercial disputes between a Registrar and reseller and/or or their clients.

5. Powers and Authority

ZARC is authorised under its ROA to investigate complaints and to take appropriate enforcement actions where breaches of policy or law occur. These powers include the ability to request corrective action from registrars, suspend or lock domain names, refer matters to law enforcement, and report non-compliant registrars to ZADNA.

PART I – COMPLAINTS MANAGEMENT

6. Submission of Complaints

6.1 Complaints must be submitted in writing to abuse@registry.net.za using the prescribed Complaint Form available on request from legal@registry.net.za. Complainants may also reach out to the legal department using the aforementioned email should they need assistance in formulating and/or lodging a complaint.

6.2 Each complaint must include the following important information:

6.2.1 The complainant's full name and contact information or registry account information if available.

6.2.2 A clear description of the nature of the complaint, i.e., whether it relates to a specific domain name and category of the complaints (example, whois inaccuracy, phishing, spam etc.).

6.2.3 Clear, verifiable supporting evidence that allows the registry to assess credibility, severity, and jurisdiction, and to take action in line with its policies and applicable law. For example: domain identification (full name, date and time the abuse was observed, relevant urls and IP addresses) are mandatory to start the investigation process. Screenshots and visual proof of the abusive content, fake login pages hash values, URLs or references from law enforcement or trusted hotliners must also be provided. At a technical level, email headers (full headers and not just the message), DNS records, Whois snapshot, network logs may also be provided depending on the nature of the complaint. For phishing matters, the complaint may also submit phishing emails or SMS, chat Messages, payment requests or redirect chains. SAPS case numbers and/or notices from law enforcement agencies, child protection organisations, financial institutions or court orders/subpoenas will also constitute acceptable supporting evidence.

7. Acknowledgement and Timeframes

The Abuse Desk shall acknowledge receipt of the complaint within two (2) business days of submission thereof. ZARC shall endeavour to resolve complaints within thirty (30) calendar days, unless extended due to complexity or third-party involvement or other circumstances.

8. Investigation and Determination

The Abuse Desk shall evaluate whether the complaint falls within ZARC's jurisdiction. If within scope, the matter shall be investigated in accordance with established Standard Operating Procedures (SOPs). ZARC may consult the relevant registrar and/or the registrant to request remedial action. A formal outcome will be communicated in writing to all relevant parties once the investigation is completed and/or a course of action has been executed.

9. Outcomes and Remedies

9.1 Possible outcomes include dismissal of unfounded complaints, correction of registrar breaches, application of lock or server hold statuses, deletion of the domain name in question, redirect nameservers of the domain name in question and/or referral to law enforcement agencies. ZARC shall maintain due process and provide reasons for all Determinations.

9.2 If the Registrar or Reseller fails to comply with ZARC's anti-abuse and takedown management processes (section 13 referrals), ZARC may consider taking the following action:

9.2.1 in the case of a reseller, direct the registrar not to accept any services from that reseller and/or terminate the reseller's licence to provision domain name services for the .za managed domain names falling within the scope of this Policy.

9.2.2 in the case of a registrar, ZARC may suspend or terminate that registrar's accreditation with the registry.

10. Escalation and Appeal

Unresolved or disputed complaints may be escalated to the Chief Executive Officer (CEO) via escalation@registry.net.za.

PART II – ANTI-ABUSE AND TAKEDOWN MANAGEMENT

11. Definition of Abuse

For purposes of this Charter, "Abuse" includes, but is not limited to, phishing, pharming, malware distribution, botnet command and control, spam, denial-of-service attacks, child sexual exploitation material, illegal access to networks, and deceptive or fraudulent activity. Brief definitions of potentially abusive practices and/or uses are inserted below for ease of reference and understanding:

11.1 ***Phishing:*** The use of counterfeit websites to commit theft or fraud by tricking recipients into divulging sensitive information such as usernames, passwords, etc. It is the fraudulent practice of sending deceptive messages (such as emails, SMS, phone calls, or fake websites) that appear legitimate, with the aim of stealing personal data (e.g. passwords, banking details), installing malware, or gaining unauthorised access to systems.

11.2 ***Pharming:*** The redirection of unknown users to fraudulent websites or services, typically through DNS hijacking or poisoning.

11.3 ***Fraudulent websites:*** The use of websites designed to mislead users as part of a fraudulent scheme, such as 'an advance fee fraud'.

11.4 ***Wilful Distribution of Malware:*** The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include but are not limited to computer viruses, worms, Trojan horses, key loggers.

11.5 ***Malicious Fast Flux Hosting:*** Use of fast flux techniques to disguise the location of websites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.

11.6 ***Botnet Command and Control:*** Services run on a domain name that are used to control a collection of compromised computers or 'zombies', or to direct denial-of-service attacks (DDos attacks).

11.7 ***Spam:*** The use of electronic messaging systems to send unsolicited bulk messages, whether commercial in nature or not, and whether transmitted by email, instant messaging, websites or internet forums, or by any other means.

11.8 ***Distribution of Child Pornograhy***: Distribution of child pornography / child sexual abuse material refers to any act of making available, transmitting, selling, sharing, delivering, or otherwise disseminating visual, audio, or digital material that depicts a

child (a person under 18 years) engaged in explicit sexual activity, or focuses on the sexual exploitation of a child.

11.9 ***Illegal Access to Other Computers or Networks:*** Illegal accessing of computers, accounts, or networks belonging to another party or attempting to penetrate security measure of a system to which access has not been granted. This includes any activity that might be used as a precursor, for example, a port scan, stealth scan, or other unlawful information gathering activity.

12. Immediate Action

12.1 ZARC reserves the right to deny, withdraw a domain name delegation, suspend operation of the domain name, implement a domain name lock or transfer the domain name (as the case may be) to:

(i) protect the integrity and stability of the domain name management system;
(ii) comply with applicable laws and regulations or to comply with lawful requests from a competent legal authority (including but not limited to the courts or any alternate dispute resolution process;
(iii) adhere to relevant domain name registration terms and conditions;
(iv) to avoid any liability (civil or criminal) on the part of the Registry, as well as, its affiliates, subsidiaries, directors, officers and employees; and
(vi) correct mistakes made by the Registry or any Registrar relating to a domain name registration.

12.2 Where ZARC determines that domain name abuse poses imminent harm to public safety or DNS stability, it may suspend, lock, or remove delegation of the abusive domain name without prior notice. Notice will follow as soon as reasonably practicable, setting out reasons and possible appeal procedures.

13. Investigation and Registrar Involvement

All abuse reports shall be reviewed within two (2) business days as indicated in section 7 hereof. ZARC may direct the relevant registrar to investigate and remedy the abuse within five (5) business days. Registrars must cooperate fully and maintain appropriate abuse-handling capabilities under their accreditation obligations.

14. Coordination with Law Enforcement and Trusted Notifiers

ZARC recognises the importance of collaboration with competent law enforcement authorities and credible reporting organisations. Accordingly, ZARC may enter into memoranda of understanding with law enforcement agencies, national CSIRTs, or industry bodies recognised by

ZADNA as Trusted Notifiers. Trusted Notifiers may submit verified abuse reports directly to the legal department (legal@registry.net.za) for expedited processing. These reports shall receive priority handling and shall be subject to verification before enforcement.

15. Service Level Commitment for Abuse Response

ZARC commits to responding to all substantiated reports of phishing, malware, or botnet control activity within 48 hours of verification by ZARC or the relevant registrar. Reports involving content-related issues, such as fraud or defamation, will be referred to appropriate authorities or service providers for action within a reasonable timeframe.

16. Registrant Notification and Right to Appeal

Except in cases of imminent risk or criminal investigation, ZARC shall notify affected registrants in writing prior to or immediately after any suspension or takedown. Registrants may lodge an appeal within ten (10) business days of notice, setting out reasons and supporting evidence to object to allegations of unlawful domain name conduct. Appeals shall be reviewed by the legal department and, if necessary, escalated to the CEO's Office. ZARC shall determine appeals within a reasonable timeframe and provide a written outcome to the affected parties.

17. Enforcement Actions

If registrars fail to act on verified abuse notices within the specified period, ZARC may directly suspend or delete the domain. Repeated non-compliance may result in sanctions, including suspension or termination of registrar accreditation credentials.

18. Cross-Reference to WHOIS/RDAP Accuracy Procedures

Where abuse or complaint matters involve inaccurate or incomplete WHOIS or RDAP data, ZARC shall initiate the data accuracy procedures per its published terms and conditions. Registrars shall be required to correct inaccurate data as a precondition for restoring domain/s that may have been suspended.

19. Transparency and Record Maintenance

ZARC shall maintain appropriate records summarising abuse categories, volume of complaints, registrar responsiveness, and enforcement actions. These summaries shall be anonymised to comply with POPIA and GDPR, and the full dataset shall be submitted to ZADNA as part of ZARC's quarterly compliance report.

PART III – GOVERNANCE AND ACCOUNTABILITY

20. Confidentiality and Data Protection

ZARC shall ensure that all personal data processed under this Charter is handled in accordance with POPIA, the EU GDPR, and NIS2 obligations applicable to DNS service operators. Personal information will only be shared where necessary for lawful processing or enforcement.

21. Record-Keeping

All complaints, abuse reports, and enforcement actions shall be recorded in the Central Complaints and Abuse Database maintained by the legal department. Records shall include the date of receipt, parties involved, findings, and actions taken, and shall be retained for at least five (5) years.

22. Governance and Oversight

The legal department is accountable for implementing this Charter and ensuring procedural consistency. The ZARC Board of Directors shall oversee its execution at all times.

23. Review and Amendment

This Charter shall be reviewed annually, or earlier if required by law, regulatory directive, or operational need. The amended versions shall be published on ZARC's official website on https://zarc.web.za/za-sld-policies/ from time to time.