COMPLAINTS, DOMAIN NAME ABUSE AND TAKEDOWN POLICY FOR gTLDs

© 2026 ZA Central Registry NPC. All rights reserved.
Published Date: October 2026
Version: 001
Author: ZACR Legal and Policy Team

1 Purpose

1.1 This Policy establishes a unified, ICANN-aligned framework for the receipt, assessment, investigation, and enforcement of complaints and Domain Name System (DNS) abuse across the .africa and the ZACities gTLDs (.capetown, .durban and .joburg). It is designed to safeguard the security, stability and resilience of the DNS, ensure compliance with the Internet Corporation for Assigned Names and Numbers contractual framework, including the Registry Agreement and Specification 11 (Public Interest Commitments), and align with all applicable Consensus Policies, including the Registry Data Policy(effective 21 August 2025).

1.2 This Policy further establishes a globally consistent, risk-based and proportionate enforcement framework, ensuring predictability for registrars and registrants while enabling timely and effective mitigation of domain name abuse in accordance with international best practice.

2 Policy Scope

2.1 This Policy applies to:

2.1.1 All domain names registered within the .africa and ZACities namespaces;

2.1.2 All ICANN-accredited registrars and resellers interacting within these Namespaces;

2.1.3 All registrants and third parties submitting complaints or abuse reports regarding inter alia inaccurate WHOIS data, unlawful transfers, breaches of published policies, and domain name abuse such as phishing, malware, or other unlawful online content or activity.

2.2 For avoidance of doubt, this Policy applies strictly within the coordinated role of the registry operator and does not extend beyond registry-level authority as defined in the ICANN framework.

3 Governance and Operating Entities

3.1 The .africa gTLD is operated by ZA Central Registry NPC (ZACR) trading as Registry Africa Ltd in terms of the ICANN Registry Agreement whilst the ZACities are operated under the direct governance of the ZACR.

3.2 This Policy applies uniformly across all the operated gTLDs and is enforced by the relevant registry operator strictly within the authority conferred under the ICANN Registry Agreement, applicable Consensus Policies, and associated contractual instruments.

4 Definitions

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

4.1 "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 distribution or ransomware distribution, botnet Command-and-control, pharming spam, denial-of-service attacks, distribution of child Sexual abuse material, and illegal access to computer systems. The Registry may also consider other forms of harmful activity where such activity demonstrably threatens the security, stability or resilience of the Domain Name System (DNS).

4.2 "Accredited Registrar" or "Registrar" means a person or entity accredited by ZACR in terms of the Registry–Registrar Agreement and authorised by ICANN to register gTLD domains on behalf of registrants.

4.3 "Applicant" or "Registrant" means the individual or entity in whose name the domain is registered within the gTLD namespace(s).

4.4 "Board" means the Board of Directors of ZACR and Registry Africa Ltd.

4.5 Child Sexual Abuse Material (CSAM) Abuse means the use of a domain name or associated service to host, distribute, facilitate, promote, provide access to, or redirect users to material depicting or facilitating the sexual abuse or sexual exploitation of Children.

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

4.7 "Complaint" means a formal written submission made to the ZACR that alleges a breach of registry policy, registrar misconduct, inaccurate WHOIS data, or any other matter within the scope of this Policy.

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

4.9 “gTLDs’ means the .africa, .capetown, .durban and .joburg (latter four hereinafter referred to as ZACities) top level domain names.

4.10 “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.

4.11 “Personal Information” or “Personal Data” means any information relating to an identified or identifiable natural person (“data subject”), where an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

For purposes of this Policy, Personal Information includes registration data processed within the Domain Name System, including but not limited to registrant, administrative, technical, and billing contact details, IP addresses, and any associated metadata, to the extent that such data relates to an identifiable natural person.

Personal Information shall be interpreted in a manner consistent with applicable data protection laws and frameworks, including the General Data Protection Regulation, the EU GDPR, the Protection of Personal Information Act, 2013, and the Registration Data Policy of the Internet Corporation for Assigned Names and Numbers, as amended from time to time.

4.12 “Policy ” means this Complaints, Abuse and Takedown Policy, as amended and Published on the company’s official websites from time to time.

4.13 “Registration Data” means all data elements collected, generated, received, or maintained by the Registry or an ICANN-accredited registrar in connection with the registration, administration, and technical management of a domain name within a gTLD.

Registration Data includes, without limitation:

(a) domain name and associated domain status information;
(b) registrant, administrative, technical, and billing contact details;
(c) nameserver and DNS configuration data;
(d) registration, creation, update, expiry, and transfer dates;
(e) registrar identification and transaction records; and
(f) any additional data elements required to be collected or processed under applicable ICANN Consensus Policies.

Registration Data may include both **Personal Data** and **non-personal data**, and shall be processed, disclosed, retained, and protected in accordance with the Registration Data Policy and applicable contractual obligations of the Internet Corporation for Assigned Names and Numbers, as well as applicable data protection laws.

For clarity, Registration Data encompasses both publicly accessible and non-public data elements made available through WHOIS or RDAP services, subject to applicable access controls, data minimisation principles, and lawful disclosure frameworks.

4.14 "Registry Agreement (RA)" means the agreement between ZACR and ICANN authorising ZACR to operate the gTLDs.

4.15 "Suspension of services" means operational restrictions on access to the Registry and Registry Services, such as restricting new domain registrations, blocking inbound transfers, or suspending access to specific EPP functions.

4.16 "Trusted Notifier" means a recognised entity (e.g., law-enforcement agency, regulatory authority, national Computer Security Incident Response Team (CSIRT), or other lawful organisation) authorised to submit verified abuse reports eligible for expedited processing.

4.17 "WHOIS/RDAP Services" means the public registration-data query services operated by The Registry to provide information about registered domain names, subject to access, Privacy and data-protection provisions contained in ZACR's WHOIS Policies.

4.18 "ZACR" or "the Registry" means ZA Central Registry NPC, the contracted Registry Operator for the gTLDs under its management.

5 Key Principles and Scope of Complaints

5.1 The Registry manages complaints and abuse reports in accordance with internationally recognised principles of:

- 5.1.1 legality and due process.
- 5.1.2 proportionality and risk-based enforcement.
- 5.1.3 transparency and accountability.
- 5.1.4 timeliness and operational responsiveness.
- 5.1.5 protection of registration data and privacy.

5.2 All enforcement actions are undertaken within the layered responsibility model of the DNS, recognising that primary responsibility for registrant conduct rests with accredited registrars and hosting content or issues lie outside the remit of the Registry.

5.3 The Registry shall process complaints that relate to, inter alia:

5.3.1 DNS abuse as defined under the ICANN frameworks.

5.3.2 Inaccurate or incomplete registration data (WHOIS/RDAP).

5.3.3 Unlawful transfer or registry-level operational issues.

5.3.4 Domain name registration and management services of a gTLD-accredited Registrar and/or reseller.

5.3.5 Breaches of the Registry's policies or Registrar obligations under the Registry-Registrar Agreement as amended from time to time.

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

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

5.4 The Registry will NOT adjudicate complaints or disputes relating to the following as such matters remain subject to appropriate dispute resolution mechanism (e.g. UDRP/URS) or recourse to other competent authorities:

5.4.1 Generic Top Level Domain Names that are outside of the gTLDs operated by the Registry (example, .com, .org etc.) or other country code top level domain name (ccTLD) (example, .ng, .zm).

5.4.2 Services outside of the registry's control (hosting, connectivity, email services).

5.4.3 Website content disputes that are unrelated to DNS abuse.

5.4.4 Internet connectivity and access or email services.

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

5.4.6 Matters such as defamation, intellectual property disputes, or general legality of website content, or ownership rights fall outside the scope of the registry enforcement and will be referred to appropriate authorities.

5.4.7 Commercial disputes between registrars, resellers and/or registrants.

6 Powers and Authority

6.1 The Registry is authorised in terms of its Registry Agreement with ICANN to investigate complaints and to take proportionate enforcement actions where necessary to preserve the security, stability and integrity of the DNS; and address domain name abuse matters.

6.2 Such actions may include a request for corrective action from registrars, placing domain names on serverhold, suspending resolution, removing delegation, or referring the matters to competent authorities (e.g. law enforcement) or ICANN Contractual Compliance.

PART I – COMPLAINTS MANAGEMENT

7 Submission of Complaints

7.1 Complaints must be submitted in writing to abuse@registry.africa using the prescribed Domain Name Abuse Complaint Form available on request from the legal department using the email contact above. Complainants may also reach out to the legal department using the aforementioned email for assistance in formulating and/or lodging a complaint.

7.2 Each complaint must include the following important information.

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

7.2.2 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.).

7.2.3 Clear, verifiable supporting evidence that allows the registry to assess credibility, severity, and jurisdiction, and to act 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 or equivalent case numbers and/or notices from law enforcement agencies, child protection organisations, financial institutions or court orders/subpoenas will also constitute acceptable supporting evidence.

7.2.4 Date and time of the observed activity.

7.2.5 Complainant's contact details.

7.3 The Registry may request additional information and/or reject incomplete or unsubstantiated complaints.

8 Abuse Classification Framework

In order to support a proportionate and risk-based response to reported activities, the Registry adopts a risk-tiered classification model to prioritise response actions. This classification framework is intended to guide prioritisation, assessment, and potential response measures, but does not limit the Registry's discretion to escalate matters based on contextual risks.

8.1 Higher-Risk Abuse Indicators

Certain forms of activity may, depending on the circumstances, be treated as presenting a heightened risk to internet users, public safety, or the stability and security of the Domain Name System. These may include, without limitation, phishing campaigns, malware distribution, and the operation or facilitation of botnet command-and-control infrastructure. Such cases may warrant expedited assessment and, where appropriate, urgent intervention.

8.2 Moderate-Risk Abuse Indicator

Other forms of activity may be assessed as presenting a moderate level of risk, particularly where they are linked to broader malicious campaigns or evasive techniques. These may include, for example, spam activity associated with phishing or malware distribution, or the use of techniques such as fast-flux hosting designed to obscure the origin of malicious services. These matters will generally be subject to prioritised review and appropriate follow-up actions.

8.3 Lower-Risk or Administrative Issues

Certain matters may be assessed as lower risk in nature, particularly where they relate to administrative or compliance issues rather than active harm. These may include, for instance, inaccuracies in WHOIS or RDAP data, or potential breaches of registry policies. While such matters remain important for overall ecosystem integrity, they may be addressed through standard compliance and remediation processes. The Registry reserves the discretion to assess each case on its merits, taking into account the specific facts, potential impact, and applicable legal and policy considerations, and may adjust its response accordingly.

9 Acknowledgement and Timeframes

9.1 The Registry's Abuse Desk shall acknowledge receipt of complaints within 2 (two) business days of submission thereof unless the abuse has been categorised as a high risk one, then action will take place within an expedited timeframe.

9.2 Resolution timelines are target-based and may vary depending on complexity, registrar responsiveness, and third party dependencies. Notwithstanding, the Registry shall endeavor to resolve complaints within 30 (thirty) calendar days or in accordance with timelines aligned with ICANN's expectations of 'prompt and appropriate action', rather than rigid time constructs.

10 Investigation and Determination

10.1 The Abuse Desk shall:

10.1.1 Evaluate whether the complaint falls within the Registry's jurisdiction. If within scope, the matter shall be investigated in accordance with established Standard Operating Procedures (SOPs).

10.1.2 Independently verify abuse using internal systems and third party intelligence.

10.1.3 ZACR shall consult the relevant registrar and/or the registrant to request remedial action.

10.1.4 Formally communicate in writing to all relevant parties once the investigation is completed and/or a course of action has been executed.

11 Outcomes and Remedies

11.1 The Registry may:

11.1.1 Dismiss unfounded complaints.

11.1.2 Apply serverhold or disable resolution.

11.1.3 Remove delegation.

11.1.4 Correct registration information.

11.1.5 Refer matters to law enforcement.

11.1.6 Escalate registrar non-compliance to ICANN.

12 Escalation and Appeal

Unresolved or disputed complaints may be escalated to the Chief Executive Officer (CEO) via escalations@registry.africa.

PART II – ANTI-ABUSE AND TAKEDOWN MANAGEMENT

13 Definition of Abuse

For purposes of this Policy, "Abuse" is defined in section 4.1 hereof and includes, but is not limited to, phishing, pharming, malware distribution, botnet command and control, spam, denial-of-service attacks, Child Sexual Abuse 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:

13.1 *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.

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

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

13.4 *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, keyloggers.

13.5 *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.

13.6 *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).

13.7 *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.

13.8 *Distribution of Child Sexual Abuse Material* as defined in section 4.5 hereof.

13.9 *Illegal Access to Other Computers or Networks:* Illegal accessing of computers, accounts, or networks belonging to another party or attempting to penetrate security measures 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.

14 Immediate Action

14.1 The Registry 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:

14.1.1 protect the integrity and stability of the domain name management system;

14.1.2 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;

14.1.3 adhere to relevant domain name registration terms and conditions;

14.1.4 to avoid any liability (civil or criminal) on the part of the Registry, as well as its affiliates, subsidiaries, directors, officers and employees; and

14.1.5 correct mistakes made by the Registry or any Registrar relating to a domain name registration.

15 Investigation and Registrar Involvement

15.1 All abuse reports shall be reviewed within 2 (two) business days as indicated in section 9 hereof. ZACR may direct the relevant registrar to investigate and remedy the abuse within five (5) business days.

15.2 The Registry shall, as a first principle, engage with the sponsoring registrar to investigate and remediate abuse complaints. Registrars are required, under their accreditation obligations to:

15.2.1 cooperate fully and maintain appropriate abuse-handling capabilities under their accreditation obligations.

15.2.2 Maintain a functional abuse contact.

15.2.3 Investigate abuse reports promptly.

15.2.4 Take appropriate action against abusive registrations.

15.2.5 Retain registration data in line with ICANN requirements.

15.3 Failure to comply may result in suspension of services, accreditation review and/or referral to ICANN compliance.

15.4 Where the Registry determines that a domain name poses an immediate and demonstrable threat to the security or stability of the DNS or to Internet users, it may take urgent action, including suspension or removal of delegation, with or without prior

notice, consistent with Specification 11 obligations. Such action shall be justified, proportionate, documented and subject to post-action notification and appeal.

16 Coordination with Law Enforcement and Trusted Notifiers

16.1 The Registry recognises the importance of collaboration with competent law enforcement authorities and credible reporting organisations.

16.2 The Registry may enter into memoranda of understanding with law enforcement agencies, national CSIRTs, or industry bodies recognised by ICANN as Trusted Notifiers.

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

17 Service Level Commitment for Abuse Response

17.1 The Registry commits to responding to all substantiated reports of phishing, malware, or botnet control activity within 2 (two) business days of verification by the Registry or the Sponsoring registrar unless more immediate responses are required based on abuse categorization.

17.2 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.

18 Registrant Notification and Right to Appeal

18.1 Except in cases of imminent risk or criminal investigation, the Registry shall notify affected registrants in writing prior to or immediately after any suspension or takedown.

18.2 Registrants may lodge an appeal within 10 (ten) business days of notice, setting out reasons and supporting evidence to object to allegations of unlawful domain name conduct.

18.3 Appeals shall be reviewed by the legal department and, if necessary, escalated to the CEO's Office. Otherwise, appeals shall be determined with a reasonable timeframe.

18.4 The Registry shall determine appeals objectively based on evidence provided, within a reasonable timeframe and provide a written outcome to the affected parties.

19 Cross-Reference to WHOIS/RDAP Accuracy Procedures

Where abuse or complaint matters involve inaccurate or incomplete WHOIS or RDAP data, the Registry 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.

20 Transparency and Record Maintenance

The Registry shall maintain appropriate records summarizing abuse categories, volume of complaints, registrar responsiveness, and enforcement actions. These summaries shall be anonymized to comply with applicable data protection laws, regulations, policies and directives, and the full dataset shall be submitted upon request to ICANN.

21 Confidentiality and Data Protection

All processing of registration data shall be conducted in accordance with the ICANN Registration Data Policy and any applicable data protections laws, including cross-border transfer obligations where relevant. Access to WHOIS/RDAP data shall remain subject to applicable access policies and legitimate purpose frameworks.

22 Record-Keeping

The Registry shall:

22.1 Maintain record of all complaints, abuse reports, and enforcement actions, which shall include the date of receipt, parties involved, findings, and actions taken.

22.2 Retain records for at least five (5) years.

22.3 Produce anonymized reports to ICANN and internal governance.

23 Governance and Oversight

The legal department is responsible for implementing this Policy and ensuring procedural and Substantive consistency. The Registries' Board of Directors shall oversee its execution at all times.

24 Review and Amendment

This Policy shall be reviewed annually, or earlier if required by law, ICANN policy changes, regulatory directive, or operational requirements. The amended versions shall be published on the Registry’s official websites from time to time.