



## Anti-Abuse and Takedown Policy, Version 001, October 2022

The ZA Registry Consortium (Pty) Ltd (“ZARC”) is a for-profit company currently tasked with the management and administration of the following .ZA Second Level Domain Names:

- ▶ co.za
- ▶ web.za
- ▶ net.za
- ▶ org.za

ZARC is responsible for ensuring that its Registry Operations are conducted in a manner that safeguards the stability and integrity of its domain name management system and consequently the need to protect the interests of Registrars, Registrants, and the greater Internet community. Pursuant to this responsibility the ZARC hereby announces that it finds the following abusive practices, including without limitation, abusive uses(s) of domain names under its management and/or infringement of third party’s’ rights in breach of applicable laws, government rules or requirements, to be undesirable.

For purposes of this Policy, abusive practice and/or use(s) means a practice that is alleged to constitute one or more of the following:

- ▶ **Phishing**: The use of counterfeit websites to commit theft or fraud by tricking recipients into divulging sensitive information such as usernames, passwords or
- ▶ **Pharming**: The redirection of unknown users to fraudulent sites or services, typically through DNS hijacking or poisoning.
- ▶ **Fraudulent Websites**: The use of websites designed to mislead users as part of a fraudulent scheme, such as an ‘advance fee fraud’.
- ▶ **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.
- ▶ **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. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves.
- ▶ **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).

- ▶ **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.
- ▶ **Distribution of Child Pornography.**
- ▶ **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 information gathering activity.

All registrants of domain names within the aforementioned second level domain name ecosystem have a contract with their registrars and/or resellers and warrant that they will not use the domain name for any unlawful purpose whatsoever, including, without limitation, distribution of malware, abusively operating botnets, defamation, unfair competition, passing off, phishing, piracy, counterfeiting, fraudulent or deceptive practices or generally for the purpose of confusing or misleading any person.

Registrants further accept that, in addition to the Registry's Rights recorded in its Complaints Management Policy document, it 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) to 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) to 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;(vi) to correct mistakes made by the Registry or any Registrar relating to a domain name registration.

ZARC will make every attempt to adhere to the procedure recorded in its Complaints Management Policy and Procedure Document, Version 001, October 2022 as amended from time to time to address complaints pertaining to abusive practice(s) but also reserves the right to take immediate action if the integrity and stability of its domain name management system is imminent or where harm to the greater Internet user community is significant or imminent, with or without notice to the relevant registrar, reseller and/or registrant.