

1. INTRODUCTION

This document explains the basis, scope and structure of Te Kāhui Raraunga Charitable Trust's .aio TLD policy suite. It accompanies the appended policies and is intended to support the preparation of the .aio TLD application for the ICANN New gTLD Program: 2026 Round.

The document explains why the appended policies have been selected, how they operate together and why other policies commonly published on generic top level domain (gTLD) registry websites are not reproduced in this suite.

The appended policies are intended to provide the substantive registry rules needed to protect the purpose and integrity of the .aio TLD namespace at launch. Other relevant obligations will need to be implemented separately, including through the Registry-Registrar Agreement, registrar registration agreements, registry procedures and technical systems. The policy suite does not replace those instruments.

2. ICANN REQUIREMENTS, REGISTRY POLICY AUTONOMY, AND THEIR RELATIONSHIP TO THE APPLICATION

The authoritative requirements for the 2026 Round are contained in the current Applicant Guidebook, the form of Base Registry Agreement approved for the round, its specifications, applicable Consensus Policies and Temporary Policies, and other binding ICANN requirements. Successful applicants will enter into a Registry Agreement that defines the registry operator's rights and obligations and the technical and operational standards for operating a top level domain (TLD). These requirements establish a mandatory baseline. They do not, however, prescribe every rule governing participation in a particular namespace.

Subject to the Registry Agreement, applicable ICANN policy and law, a registry operator may adopt additional requirements and restrictions that are consistent with and appropriate to the purpose of its TLD. However in the context of the 2026 round, this policy autonomy must be exercised consistently with any community commitments made in its application and embodied in the Registry Agreement.

3. INDUSTRY TRENDS AND EVIDENCE BASE

The appended policy suite has been informed by the 2026 Round materials, commentary on the 2012 application round, comparative review of registry policy suites and engagement with .aio TLD.

The research indicates that registry policies are most effective when the principal obligations are consolidated into a manageable number of documents, abuse requirements are stated clearly, registration-data obligations are aligned with the

current ICANN framework, and enforcement processes are transparent, proportionate and capable of consistent administration.

Community-oriented and culturally specific TLDs also demonstrate the value of eligibility requirements, nexus or intended-use commitments, restrictions on misleading use, and culturally protective naming controls.

4. ASSUMPTIONS AND EXCLUSIONS

The policy suite is developed assuming that .aio TLD will operate as a dedicated, limited-purpose community namespace rather than a general-purpose open gTLD. Its policies must therefore protect the .aio TLD mission, give effect to the relevant community's authority to define participation, and establish requirements that are clear, measurable and capable of consistent administration through registry and registrar processes.

.aio TLD's instructions and community inputs are the starting point for the policy design. Comparative research and industry practice may inform drafting, but do not displace those instructions.

The policy suite is confined to registry-level domain-name governance. The test applied here is whether a standalone .aio TLD instrument is necessary to state a registry-specific rule, implement a .aio TLD community commitment, or provide a registry-controlled process that is not adequately supplied by an existing binding instrument. It does not purport to replace binding ICANN policies, contractual instruments or specialist operational documentation.

The following are excluded:

Registry-Registrar Agreement. The Registry-Registrar Agreement is the contract through which the registry imposes relevant obligations on registrars and requires appropriate flow-down to registrants. It must be prepared separately and reviewed against the final Registry Agreement, the registry service model and applicable law. The policies inform that agreement but are not a substitute for it.

Uniform Domain Name Dispute Resolution Policy and Uniform Rapid Suspension system. The Uniform Domain Name Dispute Resolution Policy (UDRP) is an ICANN Consensus Policy and the Uniform Rapid Suspension (URS) is an ICANN-mandated rights-protection mechanism. They apply through the ICANN contractual framework and their own rules. Reproducing or redrafting them as .aio TLD policies would risk inconsistency and could imply a power to amend instruments that .aio TLD must apply as issued. The suite therefore refers to them where relevant but does not restate them.

Registration Data Policy and privacy materials. The Registration Data Policy is an ICANN Consensus Policy applying directly to gTLD registry operators and ICANN-

accredited registrars. .aio TLD will nevertheless require separate implementation documentation, including any data-protection agreement, privacy notice, disclosure procedure, retention schedule and internal controls required by the ICANN policy and applicable privacy law. Those documents concern legal compliance and operational processing rather than the community-registration rules addressed by this suite.

Other ICANN and operational materials. Data escrow specifications, registry continuity arrangements, DNSSEC practice statements, registry service provider procedures, incident-response plans, technical service documentation and detailed complaints manuals are excluded because they are governed by ICANN requirements or require specialist legal, privacy, security or operational input. Organisational policies not specific to domain-name governance, including employment, procurement, supplier, ESG and corporate risk policies, are also outside scope.

5. FRAMEWORK FOR TECHNICAL AND CULTURAL POLICY DEVELOPMENT

The policy-development process requires a clear distinction between technical-operational responsibilities and community-governance authority.

InternetNZ serves as the primary drafter of the registry policy suite and is responsible for developing the mechanisms by which policies are administered and enforced. This includes registrar flow-down requirements, compliance processes, technical standards, registry operations, and alignment with applicable ICANN requirements.

.aio TLD and the relevant community authorities retain responsibility for defining the substantive values, eligibility requirements, naming principles, cultural safeguards, and broader policy objectives of the TLD. These inputs establish the community mandate that the registry policies are intended to reflect and protect.

This allocation of responsibilities creates a practical policy development model. .aio TLD and its community determine the purpose, scope, and substantive criteria of the namespace, while InternetNZ translates those requirements into a coherent policy framework and drafts the individual policies.

6. .AIO TLD POLICY SUITE

6.1 Policy Objectives and features

The appended policy suite contains the registry-specific instruments required to express the .aio TLD community-registration model and its launch.

.aio TLD is intended to operate as a dedicated community namespace. The suite must therefore do more than regulate ordinary registration mechanics. It must support Indigenous community self-identification, cultural connection, collective benefit and

the authority of the .aio TLD community to determine participation in the .aio TLD namespace. Those objectives are implemented through five connected functions: eligibility; name selection; validation; acceptable use; and compliance and operational enforcement.

6.2 Proposed Policy Taxonomy

The policies have been consolidated where possible so that each document has a distinct function and the suite can be read as a whole.

The following are included:

.aio TLD Registration Policy. The .aio TLD Registration Policy states who may register, the evidence and attestations required, the pre-registration validation process, name-selection requirements, continuing obligations and available compliance measures. It is the key feature of the community-registration model.

.aio TLD Reserved and Restricted Names Policy. The .aio TLD Reserved and Restricted Names Policy gives effect to ICANN reserved-name requirements and establishes .aio TLD controls for operational, legal, community and culturally significant or sensitive names. A separate policy is justified because these controls may apply independently of ordinary eligibility review and may require distinct approval or allocation processes.

.aio TLD Acceptable Use Policy. The .aio TLD Acceptable Use Policy states prohibited uses and the registry's reporting, assessment and enforcement framework. It supplements ICANN's DNS Abuse baseline by recording .aio TLD-specific obligations concerning community integrity, impersonation and misleading use.

.aio TLD Internationalised Domain Name Policy. The .aio TLD Internationalised Domain Name Policy sets the registry rules for IDN labels, tables, variants and technical validation. It is required because IDN implementation depends on registry-specific language or script choices and must operate consistently with ICANN IDN requirements and the .aio TLD naming framework.

.aio TLD Launch Policy. The .aio TLD Launch Policy establishes the start-up sequence, Sunrise, Trademark Claims, any pre-registration phase, allocation and contention rules, publication requirements and launch enforcement arrangements. These matters are time-limited but require a clear public instrument before launch.

.aio TLD Sunrise Alternative Dispute Resolution Policy. The .aio TLD Sunrise Alternative Dispute Resolution Policy provides the required mechanism for challenging failures to comply with .aio TLD's Sunrise allocation and registration rules. It is separate from the UDRP, URS and Trade Mark Clearing House (TMCH) procedures because its scope is limited to Sunrise compliance and registry implementation.

The appended policies should be read together with the final Registry Agreement, Registry-Registrar Agreement, registrar registration terms, applicable ICANN Consensus Policies and operational procedures. Where a binding ICANN requirement applies directly, that requirement prevails. Where .aio TLD has adopted a more specific community rule that is consistent with ICANN requirements, the .aio TLD rule forms part of the conditions for registration and use.

.AIO TLD Acceptable Use Policy

Version 1.0 - Effective 11 August, 2026.

Introduction

This Policy sets out acceptable use requirements for all .aio TLD Domain Names and the measures .aio TLD may take to prevent or address prohibited use.

Interpretation

In this Policy:

“Abuse Report” means a report that a .aio TLD Domain Name is being used in breach of this Policy.

“DNS” means the Domain Name System.

“DNS Abuse” means malware, botnets, phishing, pharming, spam when used as a delivery mechanism for another form of DNS Abuse, or another activity recognised as DNS Abuse under the .aio TLD Registry Agreement or applicable ICANN requirements.

“.aio TLD” means Te Kāhui Raraunga Charitable Trust as registry operator for the .aio TLD top-level domain.

“.aio TLD Domain Name” means a domain name registered at the second level under .aio TLD.

“Policy” means this .aio TLD Acceptable Use Policy.

“Registrar” means an ICANN-accredited registrar authorised by .aio TLD to offer .aio TLD Domain Names.

“Registrant” means the person or entity recorded as the holder of a registered .aio TLD Domain Name.

1. Scope

1.1 This Policy applies to the registration and use of every .aio TLD Domain Name.

2. Registrant obligations

2.1 A Registrant must throughout the registration term:

- a. comply with the Registration Agreement and all .aio TLD policies;
- b. use the .aio TLD Domain Name consistently with the Registrant’s eligibility attestation and stated intended use;
- c. take reasonable steps to secure systems and credentials associated with the .aio TLD Domain Name;

- d. respond promptly to a compliance enquiry; and
- e. cease, remedy or mitigate prohibited use when directed by .aio TLD or the Registrar.

3. Prohibited use

3.1 A .aio TLD Domain Name must not be registered or used to:

- a. distribute, control or facilitate malware, ransomware, malicious code or unauthorised access;
- b. operate or facilitate a botnet, denial-of-service attack, fast-flux network, DNS hijacking, DNS poisoning or pharming;
- c. conduct phishing or otherwise fraudulently obtain credentials, personal information, money or property;
- d. send spam where it delivers or facilitates DNS Abuse, or use the name for other unlawful unsolicited electronic messaging;
- e. commit fraud, deception, counterfeiting, piracy or another unlawful act;
- f. impersonate another person or entity or falsely imply authority, representation, sponsorship, endorsement or affiliation;
- g. infringe intellectual property, privacy, confidentiality or other legal rights;
- h. interfere with the operation, security or stability of the DNS, .aio TLD, a Registrar or another network or service;
- i. evade enforcement, conceal prohibited conduct or repeatedly facilitate prohibited use by another person;
- j. use unlawfully obtained, materially inaccurate or misleading registration information; or
- k. engage in any activity contrary to applicable law, a binding court order, the .aio TLD Registry Agreement or a .aio TLD policy.

4. .aio TLD community and cultural requirements

4.1 A .aio TLD Domain Name must not be used in a manner that materially undermines the safe, valued and trusted character of the .aio TLD namespace, including by:

- a. misrepresenting Indigenous community identity, authority, mandate or affiliation;
- b. exploiting a culturally significant or culturally sensitive name, expression, knowledge or association; or
- c. causing material harm to the dignity, cultural integrity, collective benefit, authority to control, responsibility or ethical interests of the .aio TLD community.

5. Abuse reporting and assessment

- 5.1 .aio TLD must provide a published channel for Abuse Reports concerning DNS Abuse, eligibility, name selection and acceptable use.
- 5.2 A report should identify the .aio TLD Domain Name, alleged conduct, supporting evidence and the reporter's contact details where available.
- 5.3 .aio TLD must assess an Abuse Report on its merits and take prompt, reasonable and proportionate action where .aio TLD determines that action is required. The assessment may consider the domain name, registration data, attestations, stated and actual use, technical indicators, complaint evidence, information from the Registrant or Registrar, applicable law and all relevant .aio TLD policies.
- 5.4 .aio TLD should acknowledge a report within five business days where contact details are provided.

6. Notice and response

- 6.1 Unless immediate action is reasonably necessary to address DNS Abuse, serious legal risk, security or stability risk, or material community harm, .aio TLD must give the Registrant notice of the alleged breach and not less than 14 calendar days to respond or remedy the breach.

7. Enforcement

- 7.1 .aio TLD may take one or more proportionate measures, including requiring remediation, restricting a transaction, placing the name on lock or hold, suspending resolution, redirecting where lawful and appropriate, transferring, deleting or declining renewal of the registration.
- 7.2 .aio TLD may take immediate interim action without notice where reasonably necessary to stop or otherwise disrupt DNS Abuse, comply with law or a binding order, protect the DNS or registry, prevent material harm, correct an operational error or enforce a dispute-resolution outcome.
- 7.3 .aio TLD must consider the likely effectiveness, urgency and risk of collateral harm when undertaking immediate interim action without notice.

8. Monitoring, cooperation and review

- 8.1 .aio TLD is not required to continuously monitor websites, applications, email or other content associated with .aio TLD Domain Names. .aio TLD may use automated monitoring, trusted-notifier reports, risk-based review, complaints, audits and information from Registrars, hosting providers, competent authorities and other relevant parties.

- 8.2 .aio TLD may share information and cooperate with a Registrar, registry service provider, hosting provider, law-enforcement agency, competent authority or other relevant person where lawful and reasonably necessary to investigate or mitigate prohibited use.
- 8.3 A Registrant may request review of an enforcement decision under the procedure published by .aio TLD.

9. Records and policy changes

- 9.1 .aio TLD must retain material reports, evidence, investigation records, determinations and enforcement documentation relating to an Abuse Report for the duration of the registration term and for any additional retention period specified in .aio TLD's Privacy Policy, subject to applicable laws.