.nz Operations and Procedures

Version 2.4

Section 11 contains changes and refers to interim policy put in place on 16 April 2019. Any changes reflecting this interim policy are in bold.

Index

About this policy
Background
Authorisation of Registrars
De-authorisation of Registrars
Structure of a .nz Domain Name
Second Level Domain Names
Process for the Registration of Domain Names
Privacy Option
Registration of Domain Names at the Second Level
Conflicted Name Process
Process for the Management of Domain Names
DNSSEC
The Billing Process
Unique Domain Authentication ID (UDAI)
Transfer of Registrar
Change of Registrant
Cancelling and Re-instating Domain Names
Managing Cancelled Domain Names
Disputes and Complaints
Registrars and Resellers
Domain Registration Data Query
Procedure for Disclosure of Withheld Data
Process for Registrant Info Service search
Zone Data
AOR1 - Application for Authorisation as a Registrar (https://dnc.org.nz/node/75)
DCPI - Complaints Form (https://dnc.org.nz/resource-library/policies/78)
WHO1 - Application for Registrant Info Services Search - own .nz names
WHO2 - Application for Registrant Info Services Search -for DRS Complaint
(https://dnc.org.nz/resource-library/policies/81)
WHO3 - Application for Registrant Info Services Search - for DRS Complaint Assistance
(https://dnc.org.nz/resource-library/policies/82)

1. About this policy

1.1 This policy sets out the operations and procedures that apply to the running of the .nz domain name space and which must be followed by all participants in the .nz domain name space.

2. Background

2.1 InternetNZ has the ultimate responsibility as designated manager within New Zealand for the .nz domain name space, and maintains a shared registry system for the management of .nz domain name registrations. Through an Operating Agreement, InternetNZ has appointed DNCL to manage and administer the .nz domain name space on behalf of InternetNZ.

2.2 The shared registry system is a single register (“Register”) for registered domain names and associated data. InternetNZ operates the Register.

2.3 Registration and management of .nz domain names, as well as management of information provided to the Registry (“Registry”), is effected by Registrars (“Registrars”). Registrars access and manage domain names on behalf of Registrants (“Registrants”) and it is the Registrants to whom individual domain names are licensed.

2.4 The .nz domain name space is governed by .nz policies, which are available on the DNCL website. All participants in the .nz domain name space (including Registrants and Registrars) are bound by the .nz policies, of which this is one.

2.5 Key principles and responsibilities in the .nz domain name space are set out in the .nz Principles and Responsibilities policy.

3. Authorisation of Registrars

3.1 Potential Registrars can make an application to become an authorised Registrar by:

3.1.1 Completing the Application for Authorisation as a Registrar (“Form AOR1”) and all its requirements.
3.1.2 Paying a non-refundable application fee of NZD$3,000.00 (plus GST if applicable) to DNCL.

3.2 DNCL will endeavour to acknowledge applications by email within two working days of receipt. Applications will be processed in the order in which they were received. DNCL will endeavour to process applications within a month of receipt.
3.3 If an application is accepted, DNCL and the potential Registrar may execute the .nz Registrar Authorisation Agreement. A potential Registrar is not an authorised Registrar until the .nz Registrar Authorisation Agreement is executed by both parties.

3.4 If an application is declined, DNCL will provide reasons why. The applicant will be entitled to make a new application in the future if relevant circumstances change.

3.5 A newly authorised Registrar has six months from the date of authorisation to connect to the Registry. If the Registrar has not connected to the Registry within this time, its Authorisation Agreement may, at the Domain Name Commissioner’s sole discretion, be terminated in which case it will no longer be an authorised Registrar.

4. De-authorisation of Registrars

4.1 A Registrar may cancel its authorisation status on two months notice to DNCL.

4.2 The Domain Name Commissioner may cancel a Registrar’s authorisation status where:

- 4.2.1 the Registrar has transferred its authorisation status to another party;
- 4.2.2 the Registrar Connection Agreement with the Registry is cancelled by either party; or
- 4.2.3 the Registrar is in breach of their .nz Registrar Authorisation Agreement or a .nz policy.

4.3 The cancellation of a Registrar’s authorisation does not affect any of its rights and responsibilities which are intended to continue or come into force after de-authorisation.

4.4 Irrespective of who cancels the Registrar’s authorisation, the Registrar will:

- 4.4.1 continue to take all actions necessary to safeguard the rights of their Registrants;
- 4.4.2 immediately discontinue acting as a Registrar;
- 4.4.3 cease to hold themselves out as an authorised Registrar; and
- 4.4.4 work co-operatively with all persons to effect transfers of registered domain names to other Registrars.

4.5 Where a Registrar cancels its authorisation the Registrar must transfer the domain names under its management to another .nz Registrar in accordance with clause 14.

4.6 Where DNCL cancels a Registrar’s authorisation, and the Registrar has not made alternative arrangements for the transfer of domain names under its management:
4.6.1 DNCL will contact all Registrants of those domain names and:

(a) instruct them to transfer their domains to a Registrar of their choice;
(b) provide a list of authorised Registrars, together with contact information;
(c) inform the Registrant of its domain name(s) and the UDAI for those domain name(s); and
(d) inform them of a deadline, that DNCL will set, for completion of the transfer process.

4.6.2 Those domains that are due to be renewed between the date the Registrant is contacted by DNCL and the deadline set by DNCL will be automatically renewed for one month to enable them to be transferred. DNCL will meet the Registry’s renewal fees resulting from this automatic renewal.

4.7 DNCL may, at its sole discretion, extend the deadline for transfer of domain names affected by the cancellation of a Registrar’s authorisation. In such cases it may engage further with the affected Registrant to assist it in transferring to a new Registrar.

4.8 After the deadline has passed DNCL will direct the Registry to cancel those domain names that have not been transferred when their current billing term expires.

4.9 Where a Registrar whose authorisation has been cancelled has been hosting a domain name, and the hosting services have also ceased, DNCL will attempt to contact affected Registrants. Other Registrars must not approach the affected Registrants to offer hosting services as a way of securing transfers of domains to them.

4.10 DNCL may, at its sole discretion, attempt to fill any hosting gaps by making temporary arrangements with other organisations. In those circumstances, DNCL will direct the Registry to update the name server information to reflect the new hosting arrangements.

5. Structure of a .nz Domain Name

5.1 Domain names in the .nz domain name space can be registered at either the second or the third level.

5.2 Each complete name must be unique and comprise at least two levels, with each level separated by a period (.). The following are examples of compliant .nz domain names:
5.2.1 ‘anyname.org.nz’ where:

‘.nz’ is the top level, country code fixed for all domains delegated to, and managed by, DNCL.
‘.org’ is the listed second level domain chosen by the Registrant.
‘anyname’ is the name at the third level the Registrant has chosen to register.

5.2.2 ‘anyname.nz’ where:

‘.nz’ is the top level country code.
‘anyname’ is the name the Registrant has chosen to register at the second level.

5.3 “Second level domain name” is different from “domain name registered at the second level”.

5.3.1 A second level domain name is one of a limited number of listed names that a Registrant can use when registering a domain name at the third level. The ‘.org’ example in clause 5.2.1 is an example of a second level domain name. Second level domain names are explained further in clause 6.

5.3.2 A domain name registered at the second level is a name selected by a Registrant. Instead of registering it at the third level (preceding a second level domain name) it is listed at the second level (preceding the .nz top level country code).

5.4 Sub-domains can be added by the Registrant to any domain name registered at the second or third level. For example, the domain name could be ‘shop.nz’ and the sub-domain could be ‘book’, being in full, ‘book.shop.nz’.

5.5 Except where a complaint is made pursuant to clause 4 of the Dispute Resolution Service Policy, sub-domains are outside the scope of .nz policy and are the responsibility of the Registrant. They must comply with RFC1591 and meet the standards defined in clause 5.6.

5.6 Any new name must conform to the relevant Internet Standards (such as RFCs 1034, 2181, 5890 and 5891) as well as specific .nz policy requirements as follows:
5.6.1 A domain name can consist of only lower case letters (a-z), digits (0-9) and the ‘-’ hyphen.

5.6.2 Internationalised Domain Names (IDNs) are allowed (as specified in RFCs 5890 and 5891), where the characters represented by the IDN are restricted to macronised vowels (ā, ē, ī, ō, ŭ) in addition to the characters specified in clause 5.6.1 (an IDN must include at least one macronised vowel).

5.6.3 Domain names must not commence or end with a hyphen. Hyphens cannot be the third and fourth characters unless used in a valid IDN (when the domain name must commence ‘xn--’).

5.6.4 The maximum length of each name element is 63 characters.

5.6.5 The maximum length of a domain name (including separators) is 253 characters.

5.7 Name server data is not required for a domain name to be registered. If valid name server data is provided it will be published in the DNS when delegation is requested.

5.8 Name server data will be validated when provided to ensure that it meets minimum technical and operational criteria to ensure the security, stability and resilience of the DNS.

5.9 Name server data may be revalidated at any time and may be removed from the DNS should the technical and operational criteria not be met.

6. Second Level Domain Names


6.2 The list of second level domains is closed and no further second level domains are to be created.

6.3 For further explanation of second level domains, the Second Level Domains Policy, which is no longer in force, is available in the policy archives on the DNCL website.

7. Process for the Registration of Domain Names

7.1 Registrars register domain names on behalf of Registrants.

7.2 Registrants must be identifiable individuals over 18 years of age or properly constituted organisations.

7.3 Any eligible Registrant may register an available domain name at the second or third level on a first come, first served basis.

7.4 The person named on the Register is the legal Registrant and therefore holds the licence to use that domain name.
7.5 The applicant, in lodging the request for the domain name, warrants that it is entitled to register the domain name as requested. For example, the applicant warrants that the proposed domain name does not infringe any other parties’ rights.

7.6 Disputes regarding whether an applicant has a legitimate right to a name can be dealt with pursuant to the Dispute Resolution Service policy. DNCL has no role in deciding who has rights in such disputes.

7.7 A registration may be cancelled at any stage where the Registrant does not comply with these requirements or fails to meet any fees or other liabilities in connection with the registration or use of the domain name.

7.8 When registering a new domain name the Registrar supplies the following data:

| 7.8.1 Domain Name |
| 7.8.2 Registrant Name |
| 7.8.3 Registrant Contact Details |
| 7.8.4 Administrative Contact Details |
| 7.8.5 Technical Contact Details |
| 7.8.6 Billing Term; |
| and, if applicable: |
| 7.8.7 Registrant Privacy Option; |
| 7.8.8 Name Server List |
| 7.8.9 DS Record List |
| 7.8.10 Registrant reference. |

7.9 The Registrar must ensure that the domain name is available, that mandatory fields have been supplied, and that the relevant fields have valid formats (e.g. domain name format, e-mail address format).

7.10 The Registrar must pass the details of the registration on to the Registrant. The UDAI, or instructions on how to obtain a UDAI, must also be sent out to Registrants at this time. The Registrar must provide the UDAI to the Registrant on request.

7.11 There is a grace period of five days upon a domain name first being registered, during which time the Registrar may cancel the registration.

7.12 Where the domain name is cancelled during the grace period it will be removed from the Register. The registration and cancellation will still be recorded for audit purposes. The same Registrar is able to re-register the same domain name but it is not able to be cancelled for a second time within one month of the initial registration.

7.13 A Registrant will not be able to transfer the management of its domain name to another Registrar during the grace period.
7.14 Except as set out in clause 7.15, Registrars must identify the full billing term.

7.15 Registrars’ terms and conditions may provide that they are entitled to register for an initial period until they have received the monies from the Registrant and then update the domain name billing term as soon as those monies are received by the Registrar.

7.16 The operating principles for moderated domains are:

7.16.1 Approval for registration of the moderated name can only be made by the Moderator and occurs prior to the Registrar registering the domain name in the Register.

7.16.2 Moderators must either establish themselves as a Registrar or set up a relationship with one or more Registrar(s) to act as their approved Registrar(s).

7.16.3 Moderators are responsible for notifying the DNCL and the Registry of their accredited Registrar(s).

7.16.4 Only an approved Registrar will be able to register domain names in that moderated domain

8. Privacy Option

8.1 Registrants who are individuals are able to elect a privacy option. If this option is elected, and the Registrant is eligible, the only contact information displayed in the results returned from a Query (refer Section 22) is the name, email and country. Detailed address and phone information will be withheld (“Withheld Data”) and not be displayed.

8.2 Registrants are able to elect the privacy option at the time of registering the domain name or at any later time. Registrants are able to change their selection at any time through their Registrar.

8.3 To be eligible for the privacy option, Registrants must be:

8.3.1 Natural persons (“individuals”); and.

8.3.2 Not using the domain name to any significant extent in “Trade” as that term is defined and used in the Fair Trading Act 1986.

8.4 DNCL may remove the privacy option from a particular domain name where it determines the Registrant does not meet the criteria specified in clause 8.3. The Registrant will be notified before this action is taken.

8.5 This privacy option is optional for Registrars to offer until 28 March 2018 at which date all Registrars must offer this option.

9. Registration of Domain Names at the Second Level

9.1 In order to avoid confusion the names ‘gov’, ‘government’, ‘com’, ‘edu’, and ‘nic’ cannot be registered at the second level.
9.2 An Equivalent Name was a name at the second level which matched the name registered at the third level (for example, anyname.nz was the Equivalent Name for anyname.co.nz); a Conflicted Name is a name which appears at the third level in more than one second level meeting the criteria in clause 9.1.

9.3 Registrants who were either a councillor of InternetNZ or a director of DNCL or a director of NZRS Limited or a staff member or contractor of any of those three entities, or were from 1 September 2011 to 30 May 2012, qualified for the Conflicted Name process only if the Registrant has a Conflicted Name as at 1 September 2011, that at 1pm 30 September 2014 was registered and whose registration has been continuous.

9.4 The reason there is a different date for eligibility for the Registrants defined in 9.3 is to ensure there is no conflict of interest. 1 September 2011 pre-dates any discussion about a possible change to the .nz registration structure.

10. Conflicted Name Process

10.1 Registrants holding a domain name that meets the following criteria can use the Conflicted Name process:

10.1.1 a name registered as at 9.00am 30 May 2012; and
10.1.2 that at 1pm 30 September 2014 was registered and whose registration has been continuous; and
10.1.3 is not subject to clause 9.3; and
10.1.4 the name is conflicted,
10.1.5 by following the process outlined in clause 10.1 to 10.9.

10.1.6 For example, as at the time given, ‘anynname.co.nz’ is not the only domain name for the term ‘anynname’; ‘anynname.org.nz’ is also registered. The names ‘anynname.co.nz’ and any other ‘anynname’ registration are conflicted, and Registrants must follow the Conflicted Name process described in clauses 10.1 to 10.9.

10.2 Where there is a Conflicted Name, each Registrant of the Conflicted Name must indicate by 18 October 2017 via a nominated DNCL website that they either:
10.2.1 would like the opportunity to register the Equivalent Name for possible registration as a .nz domain name at the second level; or

10.2.2 do not want to register the Equivalent Name for possible registration as a .nz domain name at the second level, and do not want any other party to register the Equivalent Name as a .nz domain name at the second level; or

10.2.3 do not want to register the Equivalent Name for possible registration as a .nz domain name at the second level, and do not object to another Registrant registering the Equivalent Name as a .nz domain name at the second level.

10.3 If a Registrant of a Conflicted Name did not indicate a preference by 18 October 2017 (clause 10.2) then that Conflicted Name ceased to be a Conflicted Name and has no involvement in the Conflicted Name process.

10.4 Where all Registrants in the Conflicted Name process for the Equivalent Name have indicated the preference of ‘do not want and do not object to another’, as specified in clause 10.2.3, then DNCL will deem the conflict resolved and the Equivalent Name released for registration on a first come, first served basis at a time determined by DNCL.

10.5 A Registrant of a Conflicted Name may register the Equivalent Name once the conflict is resolved. DNCL will advise the Registrant of the opportunity to register the Equivalent Name. The Registrant will have 2 months from the date of advice to register the Equivalent Name at the second level.

10.6 Where the Registrants of a Conflicted Name have come to an agreement, the Registrants will advise DNCL of the agreement via a nominated DNCL website. DNCL will advise the agreed Registrant of the opportunity to register the Equivalent Name.

10.7 Proof of the consent of the other Registrants may be required as part of the application for registration. Consent will be recorded through a nominated DNCL website. DNCL may make such inquiry as it thinks necessary to verify that consent has been given to the Registrant by the other Registrants of the Conflicted Name.

10.8 DNCL may decline the Equivalent Name at the second level if the DNCL is satisfied that the consent of any of the Registrants with the Conflicted Name:

10.8.1 has been obtained through a breach of any law; or

10.8.2 is inconsistent with any DNCL policy.

10.9 It is the responsibility of the Registrant with a Conflicted Name seeking registration at the second level to obtain the consent of the other Registrants with the Conflicted Name. DNCL will offer advice and information to the Registrant if required and may also offer the use of a facilitator to assist in the process.
10.10 The Conflicted Names Process is intended for conflicted parties. Where DNCL can demonstrate that the same entity is the Registrant of each of the domain names in the Conflicted Names process DNCL will contact the Registrant to direct them to resolve the conflict within a time specified by DNCL. Failure to resolve the conflict once notified by DNCL may result in DNCL deeming the conflict resolved and the Equivalent Name released for registration on a first come, first served basis.

10.11 For clarification purposes, if a name has been identified as a Conflicted Name and more than one Registrant of the Conflicted Name has expressed an interest in registering the Equivalent Name, then the Registrants of the Conflicted Name are not required to resolve the conflict. The Conflicted Name may remain unavailable for general registration indefinitely unless clause 10.10 applies.

10.12 The Conflicted Names process will be regularly reviewed in line with normal .nz policy development and review processes.

11. Process for the Management of Domain Names

*All wording in bold in this section refers to interim policy put in place on 16 April 2019.*

11.1 Registrars are required to maintain the details of the domain names for which they act as Registrar of record. They are able to amend/update the following fields:

| 11.1.1 Name Server List; |
| 11.1.2 Registrant Name; |
| 11.1.3 Registrant Contact Details; |
| 11.1.4 Registrant Reference; |
| 11.1.5 Administrative Contact Details; |
| 11.1.6 Technical Contact Details; |
| 11.1.7 Billing Term; |
| 11.1.8 DS Record List. |

11.2 The Registrar cannot amend the domain name itself. If there is an error in the spelling of a domain name, it must be cancelled and a new registration created.

11.3 Transactions able to be undertaken on the Register by Registrars will be those specified by the Registry.

11.4 Moderators of second level domain names must designate the Registrars that are permitted to register their second level domains. No other Registrars will be permitted to register these second level domains.

11.5 Only the Registrar-of-record for a domain name may send a renewal notice to a Registrant. A Registrar who is not the Registrar-of-record may not send any notice that is, or may reasonably be considered to be, a renewal notice to any Registrant.

11.6 Subject to clause 11.7 and 11.8, DNCL does not have jurisdiction to consider complaints relating to the following:
11.6.1 illegal or malicious use of a domain name, for example spam or phishing;
11.6.2 objectionable or offensive website content; or
11.6.3 possible breaches of legislation.
More information on these issues is contained in the FAQ section of DNCL’s website.

11.7 DNCL may cancel, transfer or suspend a domain name registration where maintaining the registration would put DNCL in conflict with any law, including the terms of an Order of a Court or Tribunal of competent jurisdiction.

11.8 In emergency or exceptional circumstances (for example, terrorist attack, cyber security attack, or force majeure event) where the Domain Name Commissioner reasonably considers that use of the .nz domain name space is causing, or may cause, irreparable harm to any person or to the operation or reputation of the .nz domain space, the Domain Name Commissioner may take action to mitigate or minimise that harm. Action taken under this clause shall be proportionate to the harm and is limited to the temporary transfer, suspension or locking of a domain name registration.

11.9 Neither DNCL or the Domain Name Commissioner shall be liable for any direct or indirect loss or damage suffered by a registrant or any third party, arising out of any act or omission in connection with the exercise in good faith of the powers provided for in clauses 11.7 and 11.8.

11.10 Any action taken by the Domain Name Commissioner under these provisions will be made public as soon as possible, including the nature of the incident being dealt with and the timeframe for which the temporary approach is anticipated. Use of this power will also be included in the Commission’s transparency reporting.

12. DNSSEC

12.1 In relation to managing DNSSEC (domain name system security extensions) signed domain names, Registrants (or their DNS Operator) and Registrars are responsible for:

12.1.1 generating and managing their keys;
12.1.2 generating the DS Record; and
12.1.3 determining how often they perform key rollovers.

12.2 When a Registrant elects to un-sign a DNSSEC signed name, the Registrar will remove the DS Records for that name as soon as practicable.

12.3 Registrants can elect to operate their own DNS or they can delegate this responsibility to a third party called a ‘DNS Operator’. The DNS Operator may be the Registrar for the domain name, a Registrar who does not manage the domain, a hosting provider, an ISP, or other third party that offers DNS management services.
12.4 When a change of DNS Operator for a signed domain name is required and both the current and proposed DNS Operators are Registrars, then the cooperation and participation set out in 12.5 is required.

12.5 The following applies to domain names which are DNSSEC enabled:

12.5.1 Prior to a name server update, the relinquishing DNS Operator must provide the zone information for the domain name when requested to do so, and accept and add the new DNSKEY to the zone for the domain name, re-sign it and continue to serve this until they are notified the change is complete.

12.5.2 The gaining DNS Operator then provides the new DS Record to the relinquishing DNS Operator who provides it to the Registry. The name servers for the domain name can then be updated with the Registry.

12.5.3 Following the name server update, the gaining DNS Operator must delete the old DS Record and DNSKEY provided by the relinquishing DNS Operator.

12.5.4 The relinquishing DNS Operator must remove the domain name from its name servers when requested, but must not remove it before being requested to do so.

12.5.5 All of the steps referred to in this clause shall be undertaken as soon as practicable.

12.6 DNCL will establish and maintain a contact repository of .nz DNS operators who offer DNSSEC services.

13. The Billing Process

13.1 The Registry will bill for the registration and renewal of domain names on a monthly billing period.

13.2 Registrars are obliged to disclose the billing term arranged between a Registrar and a Registrant to the Registry through the registration transaction, so they are billed for the same period that they have billed their Registrants, on an individual domain name basis.

13.3 A domain name's billing period will begin at the time it is registered, or renewed and extend for the number of monthly increments indicated by the billing term. The Registrar who administered the domain name at the start of the period will be billed.

13.4 The billing extraction will not occur until after the registration or renewal grace period (five days) for each billing term.

13.5 If the domain name is cancelled during the grace periods, the registration or renewal will not be billed.
13.6 Registrars may initiate the renewal process at any time during a domain name's current term, in advance of the normal renewal date. Advance renewals must be handled in the same manner as normal renewals, although they will not be accepted if the end of the new term is more than 120 months from the current date. Registrars will be billed for advance renewals.

13.7 Immediately following the billing of a domain name for a multiple number of months, the billing term will be re-set to one month.

13.8 To continue billing the domain name for a multiple term at renewal, the Registrar must re-set the billing term again, using the standard update process. This prevents domain names which have been billed for a longer term being automatically renewed for the same term, before the Registrar has determined the terms of the renewal, or even if a renewal is required.

13.9 The billing extraction process does not generate credits. In the event that credits are required, these must be handled outside the Register, through the Registry’s invoicing system.

13.10 If a cancelled domain name that is pending release becomes due for renewal, it will not be renewed (and therefore not billed).

13.11 If a cancelled domain name is re-instated during its pending release period the renewal process will be applied retrospectively, as if the name had not been cancelled, thus effectively 'catching up' with all the billing that would otherwise have occurred during the period of cancellation.

13.12 The Registrar may set the billing period to "0" where it has received a specific instruction from the Registrant not to renew the domain name registration. The Registrar may not set the billing period to "0" to circumvent the automatic renewal function of the Registry.

13.13 The billing extraction process will not occur for domain names that have been locked. Once a domain name is unlocked, billing 'catch-up' transactions will be generated in the normal manner.

14. **Unique Domain Authentication ID (UDAI)**

14.1 Registrars and the Registry may generate a new UDAI at any time.

14.2 A function will be provided for Registrars to check that a UDAI is valid.

14.3 Registrars must pass on the UDAI to Registrants whenever a new UDAI is generated. This applies from the time a Registrar first connects to the shared registry system. As stated in clause 7.10, the UDAI must also be provided to Registrants on request. If the Registrar fails to provide a UDAI to the Registrant, DNCL may do so.

14.4 For security reasons, UDAIs will expire at the end of a set period.

15. **Transfer of Registrar**

15.1 The Registrant may transfer its domain name to another Registrar at any time other than during the five day registration grace period.

15.2 The Registrant’s UDAI is required to enable a transfer of a domain name from one Registrar to another.

15.3 A Registrar must not decline or delay a Registrant’s request to transfer its domain name to another Registrar (by withholding the UDAI or otherwise).
15.4 Neither the releasing Registrar nor the Registry is entitled to charge any fees for the transfer of a domain name. For the avoidance of doubt, this clause does not oblige the releasing Registrar to reimburse the Registrant for the remaining term of its domain name agreement.

15.5 A domain name that is locked cannot be transferred except through a manual transaction undertaken by the Registry. An application must be made to DNCL for this to occur.

15.6 A batch transfer facility is provided for use by the Registry for situations in which, for example, a Registrar’s business is sold to another authorised Registrar. The only circumstance in which DNCL will authorise the transfer is when the relinquishing Registrar demonstrates that the affected Registrants are aware of the transfer and have signed up to the gaining Registrar’s agreements.

15.7 The process to transfer a domain name from one Registrar to another is as follows:

15.7.1 The Registrant asks the gaining Registrar to have its domain name(s) transferred to it.

15.7.2 If the gaining Registrar agrees to the transfer, it must disclose its terms and conditions and provide a contract.

15.7.3 If the Registrant accepts the terms and conditions of the gaining Registrar’s contract, then it will supply its domain name and its UDAI to the gaining Registrar.

15.7.4 The gaining Registrar will submit a "transfer" transaction to the Registry.

15.7.5 The Register will immediately be changed.

15.7.6 The Registry will inform the releasing Registrar of the change.

15.7.7 If, as the result of the transfer, other domain name details need changing (e.g. Name Server List, Registrant Customer ID, Administrative and Technical Contact Details), the gaining Registrar will initiate an update transaction in the standard manner.

16. Change of Registrant

16.1 A Registrant may transfer its domain name to another Registrant.

16.2 Registrars must have a process in place to deal appropriately with the change of Registrant, which must be clearly identified to the Registrant.

16.3 Before transferring a domain name to a new Registrant, the Registrar must ensure that the transfer is properly authorised by the existing Registrant.

16.4 Registrars must ensure the prospective Registrant signs up to the Registrar’s terms and conditions and agrees to be bound by the .nz policies.

16.5 Registrars must retain all documentation and correspondence relating to the transfer.

16.6 Registrars may require the current Registrant to provide a statutory declaration where they have concerns about its authority to effect the change in Registrant details.
16.7 Registrars may seek an indemnity for any costs, losses, or liabilities incurred in the reasonable performance of their duties in processing the Registrant’s request, or in dealing with claims arising from the allocation or use of the domain name.

17. Cancelling and Re-instating Domain Names

17.1 Domain names are automatically renewed and do not lapse unless cancelled.

17.2 Domain names may be cancelled by the Registrar at the request of the Registrant, where the Registrar has given 14 days notice due to non-payment, or where the Registrant has breached its agreement with the Registrar, and the agreement specifies domain name cancellation as a sanction for the breach.

17.3 Cancelled domain names will be assigned a status of ‘pending release’ and will not become available for reuse for a period of 90 days. Cancelled domain names, either pending release or released, will not be included in the next zone file pushed to the DNS.

17.4 During the pending release period, the Registrar may fully re-instate the domain name for the Registrant, so that it becomes active again. The domain name may also be transferred to a new Registrar and be reinstated by that new Registrar.

17.5 The billing process is unaffected by the cancellation and any re-instatement. Although the domain name will not have been billed for the period that it was pending release, once it has been re-instated the billing process will generate ‘catch-up’ transactions, from the original cancellation date.

18. Managing Cancelled Domain Names

18.1 If the domain name has passed out of its pending release period, it will be released, thus becoming available for anyone else to register.

18.2 When they are released, domain names will be removed from the Register.

18.3 Registrars must release all cancelled domain names back to the Registry and are not permitted to retain domain names for on-sale to a third party.

19. Disputes and complaints

19.1 In the event of a dispute between a Registrant and a Registrar, the parties should attempt to resolve matters between themselves before seeking DNCL’s assistance.

19.2 DNCL will generally be involved in a dispute or complaint if there is a prima facie breach of a .nz policy, or an agreement between participants.

19.3 DNCL may become involved on the receipt of a complaint, or of its own initiative.

19.4 DNCL will abide by the principles of natural justice when investigating complaints and disputes and when making determinations and imposing sanctions.

20. Registrars and Resellers

20.1 Registrars are responsible for all actions of any person or organisation acting as a reseller through the authorised registrar. Resellers are required to meet the same obligations and standards as registrars in their dealings with domain names and registrants. If a registrar does not offer registry services to what the DNC, in the DNC’s sole discretion, may decide is the public, or any section of the public however that section is selected, then all users of the registrar’s services will be resellers for
the purposes of the .nz policies. For these purposes “the public” can include government departments, offices or agencies. Ensure that any organisation, whether a reseller or not, working in any way through or with the registrar's systems operates in a manner consistent with the .nz policies.
20.1.1 The registrar will raise the issue with the reseller as soon as possible after the breach is identified setting out the reasons they are in breach and what remedies are required. They should also specify the timeframe the reseller has to remedy and the consequences if the remedies are not completed within the required timeframe. The registrar is encouraged to seek the guidance of the DNC before specifying such activities.

20.1.2 The timeframe to remedy the breach or breaches must be reasonable and reflect the seriousness of the non-compliance. That is, more urgent changes will be needed if the breach actions are serious with major consequences for the registrants.

20.1.3 Where the breach has not been remedied by the deadline, the registrar will advise the DNC of the situation and apply for approval to proceed to invoke the consequences of the non-compliance. Such consequences may include transferring responsibility for managing the .nz names involved from the reseller account to the direct responsibility of the registrar.

20.1.4 Transferring responsibility of the names from the reseller to the registrar is a significant step that impacts the relationship the registrant has with their provider so will only be considered where the registrar can demonstrate to the satisfaction of the DNC that:

(a) the resellers actions are in breach of the .nz policies such that registrants are being negatively impacted; and

(b) the reseller has been advised of its breach or breaches of the .nz policies, what it needs to do to remedy the situation by a defined timeframe and what the consequences are of failing to make the remedies in the timeframe; and

(c) the timeframe given is fair and fits with the seriousness of the non-compliance; and

(d) the registrar has a contract / agreement with the reseller that sets out the possibility of the control of the names transferring to the direct control of the registrar in the case of a breach.

20.1.5 In exceptional circumstances, even if no formal agreement between the reseller and the registrar exists, the DNC may order the names transferred to the direct control of the registrar. This action will only be undertaken after the DNC has also taken steps with the reseller to assist
them in becoming compliant and after following due process in any investigation that could lead to their names being transferred to the registrar.

20.1.6 For the purpose of this policy, any organisation or person working in any way through or with the registrar’s systems in registering or managing .nz domain names on behalf of a third party can be considered a reseller and be required to operate in a manner consistent with the .nz policies.

21. Domain Name Registration Data Query

21.1 The public is entitled to access information about a .nz domain name through a domain name registration data query ("Query"). However, automated bulk access through the Query service, or misuse of the Query data (for example, to make unsolicited communications to a Registrant) is not authorised.

21.2 At all times the priority of the Registry and the DNCL under this policy will be to protect the security of the data in the Register from unauthorised or abusive use, while as much as is practicable preserving public access to the Query service.

21.3 The Registry shall ensure the integrity of the Register and take reasonable steps to prevent unauthorised automated access, including bulk harvesting through the Query service.

21.4 If unauthorised use of the Query service is detected, the Registry and/or DNCL, at their discretion, may take any of the following courses of action:

21.4.1 remove or limit any party's access to the Query service on a permanent or temporary basis;
21.4.2 suspend a Registrar's access to the shared registry system;
21.4.3 apply a sanction to a Registrar under any applicable agreements or .nz policies; or
21.4.4 in extreme circumstances, suspend the Query service.

21.5 The Query service will respond to a Query for a specified domain name. If the domain name is registered, the details as set out in clause 21.7 will be available. If the domain name is not registered, the Query service will show that it is available for registration.

21.6 A Query may not be undertaken using wild card searches.

21.7 The following details will be available in response to a Query:
Domain Name;
Registration status;
Date registered;
Date registered/billed until;
Date last modified;
Include in DNS;
Registrar of Record (including contact details);
Registrant Contact Details;
Administrative Contact Details;
Technical Contact Details;
Name Servers;
Domain Signed;
and, if applicable:
DS Records;
Date cancelled; and
Date locked.

21.8 Where an individual Registrant has elected the privacy option (refer Section 8), the contact information displayed for the Registrant, Administrative and Technical Contacts will be limited to the name, email and country. Detailed address and phone information will be withheld and not displayed.

21.9 Requests for the Withheld Data can be made. The process for this is specified in Section 22.

22. Procedure for Disclosure of Withheld Data

22.1 DNCL's default position is that a Registrant’s Withheld Data will not be disclosed.

Application to request disclosure of Withheld Data

22.2 Any person, entity or organisation (“Requestor”) may make a written request (“Request”), using the PRI1 application form (“Application Form”), to DNCL for the disclosure of a Registrant’s Withheld Data.

22.3 In order for DNCL to disclose Withheld Data, the Requestor must:

22.3.1 Establish that there is a legitimate need (as set out in clause 22.4 of this Policy) for the disclosure of the Withheld Data; and

22.3.2 Meet the further requirements set out in this Policy.

22.4 When determining whether a Requestor has established a legitimate need, DNCL will apply the relevant provisions of the Privacy Act 1993, including the Information Privacy Principles (and in particular Principle 11) as well as sections 21 and 22 of that Act.
22.5 Requestors must provide, in a timely manner, supporting documentation as may be required by DNCL in processing the Request. A failure to provide the requested information in a timely manner will be considered by DNCL a withdrawal of the application.

22.6 Subject to section 22.7 of this Policy, the Requestor must, in its Application Form, declare that an attempt to contact the Registrant by email was made no less than 10 working days prior to making the Request and that the Registrant has either not responded to the contact or has refused to divulge the Withheld Data.

22.7 DNCL may excuse the Requestor’s compliance with clause 22.6 in circumstances where:

- **22.7.1** The matter is so urgent that it is not practicable or reasonable for the 10 working day time limit to apply; or

- **22.7.2** Attempted contact with the Registrant would likely prejudice the purpose for which the Withheld Data is sought

22.8 In the event of non-compliance with clause 22.6, the Requestor must explain, in its Application Form, to DNCL’s satisfaction, how either of the exceptions in clauses 22.7.1 and 22.7.2 apply.

22.9 The Requestor must declare that any use of Withheld Data will be limited to the purposes for which it is sought and that the Withheld Data will not be used, disclosed, published or disseminated for any other purpose.

**DNCL decision making process**

22.10 DNCL will acknowledge Requests by email and will endeavour to process Requests as soon as is practicable.

22.11 DNCL shall consider the Request against the criteria and requirements of this Policy before making a preliminary decision as to whether to disclose the Withheld Data.

22.12 When considering its preliminary decision, DNCL may refuse a Request based on any previous misuse by the Requestor of Withheld Data or breach of .nz policies notwithstanding that the Request meets the criteria and requirements of this Policy.

22.13 Subject to section 22.18 of this Policy, where DNCL’s preliminary decision is to disclose the Withheld Data, DNCL shall, before disclosing the Withheld Data, notify the Registrant of the following information:

- **22.13.1** That a Request for the Registrant’s Withheld Data has been made;
- **22.13.2** The Requestor’s name and email address;
- **22.13.3** The reason for the Request;
- **22.13.4** That DNCL’s preliminary decision is to disclose the Withheld Data
22.14 Where the Registrant has been notified of a preliminary decision in accordance with clause 22.13 of this policy, the Registrant shall have five working days to comment on DNCL’s preliminary decision.

22.15 After considering the Registrant’s comments (if any), DNCL shall make a Final Decision as to the disclosure of the Withheld Data.

22.16 Where the Registrant satisfies DNCL that there are legitimate grounds for non-disclosure, DNCL may in its absolute discretion decline the Request notwithstanding that the Request meets the criteria and requirements of this Policy.

22.17 DNCL may at its discretion make a final decision that differs from the request where DNCL considers it would better protect privacy. For example, disclosure of Withheld Data to a Requestor’s lawyer for service of documents on condition it isn’t disclosed further.

22.18 DNCL shall communicate its Final Decision to both the Registrant and Requestor and provide reasons in writing for its decision.

22.19 DNCL shall not provide the Registrant with an opportunity to comment on its preliminary decision where DNCL reasonably considers that this would prejudice the purpose for which the Withheld Data is being requested. Where the Registrant is not given an opportunity for comment, the DNCL’s preliminary decision shall constitute the Final Decision.

22.20 Where section 22.19 of this Policy applies, DNCL shall only provide reasons for its Final Decision to the Requestor.

22.21 Where a Registrant is not given an opportunity for comment before the disclosure of the Withheld Data, DNCL shall notify the Registrant of the disclosure, and reasons for it, as soon as practicable. Not all of the Withheld Data may be provided at the discretion of DNCL.

---

**Misuse of Withheld Data**

22.22 DNCL may refuse to accept further requests from Requestors who misuse Withheld Data and/or breach .nz policies. Misuse may also lead to formal complaints laid with any other appropriate agencies such as the Privacy Commissioner.

---

**Disclosure where court order or requirement of law**

22.23 DNCL shall disclose Withheld Data where the disclosure is ordered by a court of competent jurisdiction or is required by any other order with the force of law.

22.24 Where section 22.23 of this Policy applies, the Registrant shall not be consulted before the Withheld Data is disclosed but the Registrant shall be notified as soon as practicable after the disclosure, unless such notification would prejudice the purpose for which the Withheld Data is sought.

---

**DNCL to enter into MOUs**
22.25 DNCL may enter into Memorandums of Understanding ("MOU") with entities which DNCL considers have a legitimate need for access to Withheld Data. Such MOUs shall provide either automatic access to Registrants' Withheld Data or streamlined access to Registrants' Withheld Data.

22.26 All executed MOUs will be published on DNCL's website and will be regularly reviewed by DNCL.

Entities with automatic access

22.27 DNCL may enter into MOUs granting automatic access to Withheld Data to approved entities tasked with maintaining the integrity of the Internet. DNCL will ensure these entities have procedures in place to protect the Withheld Data.

22.28 Where an entity has automatic access, the Registrant will not be consulted before the entity accesses the Withheld Data.

22.29 Subject to section 22.28 of this Policy, the Registrant will be notified of the disclosure of the Withheld Data as soon as practicable after its release.

22.30 The Registrant will not be notified of the disclosure where DNCL reasonably considers that disclosure would prejudice the purpose for which the Withheld Data was accessed.

22.31 DNCL will be notified on each occasion an entity accesses a Registrant's Withheld Data.

22.32 At its discretion, DNCL shall monitor the entity’s use of Withheld Data to ensure that the MOU is being complied with.

22.33 It will be in DNCL’s sole discretion to terminate an MOU where an entity is non-compliant with the terms of the MOU.

Entities with streamlined access

22.34 DNCL may enter into MOUs with certain entities granting streamlined access to Registrants’ Withheld Data.

22.35 Under those MOUs, entities shall be required to make written requests to DNCL for Withheld Data. There will be a presumption of disclosure of the Withheld Data where requests satisfy the criteria for disclosure as set out in the MOU.

22.36 Where an entity has streamlined access, the Registrant will not be consulted before the Withheld Data is disclosed.

22.37 Subject to section 22.36 of this Policy, the Registrant will be notified of the disclosure of the Withheld Data as soon as practicable after its disclosure.

22.38 The Registrant will not be notified of the disclosure where DNCL reasonably considers that disclosure would prejudice the purpose for which the Withheld Data was requested.

22.39 At its discretion, DNCL shall monitor the entity’s use of Withheld Data to ensure that the MOU is being complied with.

22.40 It will be in DNCL’s sole discretion to terminate an MOU where an entity is non-compliant with the terms of the MOU.
22.41 DNCL will publish regular reports relating to applications made for release of the Withheld Data and those approved/declined.

### 23. Process for Registrant Info Service search

23.1 DNCL shall offer a Registrant Info Service providing a list of domain names matching the Registrant’s search criteria.

23.2 The application for a Registrant Info Service search is made to DNCL using the following form:

23.2.1 Form WHO1 for a search for the applicant’s own domain names.

23.2.2 Form WHO2 for a search to support a complaint pursuant to the .nz Dispute Resolution Service policy.

23.2.3 Form WHO3 for pre-registration for registrant info service searches to support a complaint pursuant to the .nz Dispute Resolution Service policy.

23.3 Information required in an application to search for a Registrant’s own domain name includes, but is not limited to, the following:

23.3.1 Name and contact details of applicant.

23.3.2 Details of the search parameters sought.

23.3.3 Evidence as to the applicant’s identity (for example, a photocopy of a driver’s licence) and, where appropriate, evidence as to the applicant’s authority to apply for a search on behalf of a company (for example, written authorisation signed by a director of the applicant company).

23.3.4 An undertaking that any information provided as a result of a Registrant Info Service search is for the applicant’s own use and will not be inappropriately disseminated.

23.4 Information required in an application for a Registrant Info Service search to support a complaint pursuant to the Dispute Resolution Service policy includes, but is not limited to, the following:
23.4.1 Name and contact details of applicant.

23.4.2 The domain name(s) that are the subject of the proposed complaint (limited to maximum of five).

23.4.3 The Registrant name(s) on the Register for the domain names(s) specified in clause 23.4.2 above will be used as the search parameter.

23.4.4 An undertaking that any information provided as a result of a Registrant Info Service search is for the exclusive purpose of supporting a complaint pursuant to the Dispute Resolution Service policy and will not be used for any other purpose.

23.5 DNCL, at its sole discretion, may either approve or decline the Registrant Info Service application, or seek further information from the applicant.

23.6 All search applications will be recorded by DNCL and any previous searches will be taken into account when deciding whether to approve the search application.

23.7 If DNCL considers, on reasonable grounds, that a Registrant has misused the information arising from a Registrant Info Service search, it may ban the Registrant from using the Registrant Info Service search for such period as DNCL deems appropriate.

24. Zone Data

24.1 In certain circumstances, .nz zone data may be released to third parties not directly involved in the management of the Registry and/or the .nz domain name space.

24.2 The zone data may not be released to third parties unless there is sufficient reason to justify such release. DNCL will retain sole discretion regarding whether or not to release zone data.

24.3 Zone data may be released where it can be demonstrated that there is a “public good” aspect to the release of the information that outweighs any adverse effect on Registrant's privacy.

24.4 DNCL may grant an application on such conditions it thinks fit, including (but not limited to) requiring the applicant to enter into an agreement with DNCL as to the terms of release. The agreement may:

24.4.1 reflect the information provided in the application;
24.4.2 confirm that the applicant agrees to be bound by the .nz policies;
24.4.3 require deletion of the zone data after use or after a prescribed time;
24.4.4 include sanctions in the event of a breach of the agreement; and
24.4.5 include any other conditions that DNCL, in its sole discretion, consider appropriate.
24.5 DNCL and the Registry may use the zone data to ensure the efficient management and operation of the .nz zone and .nz domain name space, for reasons of “public good”, and for developing new services.

24.6 An application to request .nz zone data may be made to DNCL on form ZTP1.

24.7 Information required in support of the application includes, but may not be limited to, the following:

24.7.1 The purpose the applicant will be using the information for.
24.7.2 The reason the applicant needs to obtain the information from the zone data.
24.7.3 How often the applicant wishes to receive the zone data and the period of time the zone data will be required, i.e. a single file, up to a specified date or indefinitely.
24.7.4 What information will be made public.
24.7.5 How long after receipt of the zone data the information from it will be publicly released.
24.7.6 The “public good” purpose the information will be put to.
24.7.7 Whether the applicant intends to retain the information and, if so, why.
24.7.8 The measures that are in place to protect Registrants’ privacy.
24.7.9 Any confidentiality agreements in place with its staff or contractors.

24.8 DNCL, at its sole discretion, may either approve or decline the .nz zone data application, or seek further information from the applicant. In making its decision DNCL may consult with the Registry.

Latest news

Sue Chetwin announced as chair to review .nz domain name space (/news/sue-chetwin-announced-chair-review-nz-domain-name-space)

InternetNZ is excited to announce that Sue Chetwin has been appointed as...
Johnny Foreigner and our elections (/blog/johnny-foreigner-and-our-elections)

Last week we submitted to Parliament's Justice Committee on the topic of...

How to stop the 'Christchurch Call' on social media and terrorism falling flat (/blog/how-stop-christchurch-call-social-media-and-terrorism-falling-flat)

Jacinda Ardern this morning announced that New Zealand and France are...

Subscribe to dotNews, our monthly newsletter

Subscribe (/subscribe-our-monthly-newsletter-dotnews)