Brent Carey
Domain Name Commissioner
Domain Name Commission Ltd
PO Box 11881
Wellington

28 March 2019

Jamie Baddeley
President
InternetNZ
PO Box 11881
Wellington

Dear Jamie

**Emergency response to Christchurch Terrorist Attacks**

In the wake of the attacks in Christchurch on 15 March 2019, I have been liaising closely with Department of Internal Affairs staff and other officials in dealing with the aftermath of the attacks.

This is an exceptional event and justifies an exceptional, and proportional, response. This letter sets out our response.

In particular it sets out

1. the factors that make this an exceptional situation that justifies the exceptional response. Nothing in our approach is designed to change InternetNZ’s responsibility for policy for the .nz domain name space, nor to preclude or shape ongoing work to follow up debates arising from the Domain Name Abuse forum in November 2018. InternetNZ’s process to conduct a full review of the .nz policy framework will inevitably deal with the issues raised by the attack in the fullness of time.
2. What our exceptional response is, given the factors applying.
3. Our request for InternetNZ to make an urgent short-term change to the .nz policy framework.

This letter follows a conversation among the Board of DNCL, and has been discussed with InternetNZ staff as well. It is not intended to pre-judge any matters that InternetNZ may do or not do.

**An exceptional situation demanding an exceptional response**

Urgent amendment of an existing policy to preserve the integrity of the Register (for example, security related issues) is expressly permitted by clause 7.1 of the .nz Policy Development Process.

The following factors are all at play, and have together created a situation where DNCL feels justified in an exceptional response.

1. There has been a violent terrorist attack in New Zealand.
2. The national security alert level has been set at “High”.
3. There is content the Chief Censor has deemed “objectionable material” under the FVPC Act 1993 relating to the attack in circulation on the Internet.
4. There are domain names that have been or could yet be registered in the .nz ccTLD contemporaneous with or recently following the attack.
5. Some of these domain names may be assessed by DIA or CERT NZ to be primarily intended to propagate the “objectionable material”.
6. The authorities involved in enforcing the legislation have sought DNCL assistance in limiting access to some domain names.
7. The terms and conditions of registration of a .nz domain name require the registrant to not use the name for unlawful purposes, and registrars may cancel names where this is not followed.

It is the presence of all of these factors at once that justifies a response. In other words, we are not opening a precedent to dealing with:

* Objectionable material or strings
* Content relating to terrorist incidents overseas
* Domain names that have not recently been registered
* An ongoing interest in content in the .nz domain name space.

While the .nz policy framework does not directly contemplate DNCL action in the current circumstances, DNCL feels obliged to act as a proper and responsible industry self-regulator of the .nz domain name space. We wish to work as closely as possible with our MOU related trusted notifiers, DIA and CERT NZ, in dealing with this situation.

**Our exceptional response**

In the wake of the attacks, we were in regular touch with DIA. We communicated with ccTLD managers globally. We are monitoring domain name registrations on a daily basis. We did all that we could to deal with the immediate situation.

Reflecting on the activity to date, we are now taking a further step.

**To protect the security and integrity of the .nz ccTLD and domain name space, the Board has agreed that the Domain Name Commissioner may, on the request of the Department of Internal Affairs or CERT NZ , suspend a registered domain name.**

**This discretion is only to be exercised where the National Terrorism Threat Level is High or Extreme as set by the Combined Threat Assessment Group, and by written application DIA or CERT NZ demonstrates to the satisfaction of the Domain Name Commissioner, that it has reasonable grounds to believe that internet content propagates or publishes material relating to that elevated threat level, then; DNC may suspend relevant domain names.**

We justify this action in a narrow sense that in the presence of all the factors set out above, we will in this emergency situation treat the requests of DIA or CERT NZ as if they were orders of a Court or competent tribunal. A residual discretion whether or not to act on a DIA/CERT NZ request should remain with  the DNC but the primary investigation of offending content should remain with the DIA/CERT NZ.

Suspend in this context means to lock the domain name record after setting it to delegate=no.

The impact of this action would be to make the domain name unable to be edited by the registrar or registrant, and would withdraw the name from the DNS without breaking the DNS, and without resorting to DNS poisoning. It is the lowest-impact way of removing the domain name from the Internet in the short run.

This form of action will only be taken on the request of authorities from the Department of Internal Affairs.

It will only be taken where all of the factors in the previous section of this letter are in place.

The DNC or any staff from DNCL will not review content.  The primary investigation of offending content should be left to the DIA/CERT NZ.

It will be reported on in transparency reporting that will start with a year-ending report to 1 April 2019, and thereafter on a quarterly basis.

We are aware that taking this action:

* does not remove any objectionable content from the Internet
* does not prevent any other domain name being used to address the same content
* does not mean we will prevent any .nz domain name from being used to address this content

Nonetheless we believe it to be the right thing to do.

**An urgent policy process**

We believe that InternetNZ should make an interim change to the .nz policy framework to explicitly grant the Commission the power to deal with situations of terrorist objectionable material where the factors listed above in this letter are present.

We are aware there is to be a meeting of the .nz Policy Committee on Tuesday where this issue will be discussed.

We wish to support InternetNZ in its consideration of this approach and promulgation as soon as possible of an appropriate interim policy.

We will review this emergency response on our part on or before 15 April, and will advise you of the outcome of that review.

We welcome any questions or response from the Council at this difficult time.

On behalf of the company and the Board,

Brent Carey
Domain Name Commissioner