

Zone Transfer Policy Review Submission

From: NZLinks.com (Paul McDonald)
Received: 16 October 2003

It is my belief that organizations should be permitted to obtain a copy of the total .NZ zone file list. Each individual organization should present reasons to why access should be granted and what the zone file list will be used for.

This will present a boundary for what the list will be used for and formulates part of a contract which could be used by the DNC overview team thus outlining what boundaries the applying company can use the information for, if accepted.

Upon acceptance of an organization to obtain the total zone lists, any Updates, Modifications, and Deletions should be made available to each organization, as soon as domain names are registered, modified, or deleted.

A security policy should also be designed and set in place to ensure that the organization does not make the total Zone List available to 3rd parties, with the exception that if information is passed to a third party then information should only be allowed to be passed in the same format as how the who's function within the DNC currently operates.

This would protect the list/information and restricts any third party accessing mass information without the approval of the DNC or the company who has access to this information.

The policy should also state that information obtained should not be on sold, or published in mass form.

Applications could be considered via the following.

Access to information for an approved organization should be done via a levelling scale.

1. Access to new domain names being registered for example, could be classed as level 1.
2. Access to new domains registered, and modifications, would be level 2 access.
3. Access to new domains, modifications, deletions, level three,
4. Access to all three plus company details, level 4,
5. And so on.....

Applications would be submitted to justify why each level is required and each level would have to be approved under a consideration aspect; basing approval on what the company is using the information for and why the company requires it.

Additional Security

As an extra security option, the following should be done at the registration level.

Some www addresses are not suitable for public access or public knowledge; this should be expressed at the **registration level** and requested by the user when purchasing the domain name. Activation of a view details or hide details should be available for modification at any time by the domain holder.

The usage of mail servers and other secure computers that operate via a domain names should be classed as a non public information access requirement and should be addressed at the registration level via a tick box to exclude details within the who's search enquires or lists passed to other organizations outside of the DNC.

The owner of the domain is then responsible for there own public display of details/Security and it takes the responsibility away from the DNC if a domain is passed within a list, which is deemed sensitive.

In Total the included information within this document is really all that needs to be done to ensure organizations are still able to apply for access to the .nz information. Restriction of the.nz zone lists to just authorised registers would only restrict growth and potential growth for all who own a domain name.

Thankyou for allowing input to this topic, if there is an unclear statement please contact Paul McDonald for further comment at Paul@NZLinks.com.