**DNSSEC Policy**

Public Interest Registry is dedicated to an online experience for the .NGO community, and the entire Internet, with less phishing, spamming and malware.

In our effort to bolster Internet security and stability, we have implemented Domain Name System Security Extensions (DNSSEC) within the .NGO Top Level Domain. DNSSEC is designed to protect Internet servers from domain name system attacks, such as DNS cache poisoning by malicious users. It is a set of DNS extensions which provide 3 basic functions:

* **Data Origin Authentication** – assures that data is received from the authorized DNS server; can protect from impersonation attacks
* **Data Integrity** – assures that data received matches data on the origin DNS server, and is not modified during transit; protects from man-in-the-middle type pollution attacks.
* **Authenticated Denial of Existence** – assures that a “Non-existent” response is valid.

In June 2010, Public Interest Registry launched the production of DNSSEC, stemming from a two-year effort starting with the [Public Interest Registry proposal](http://www.icann.org/en/groups/board/documents/resolutions-26jun08-en.htm#_Toc76113174) to implement DNSSEC within the .ORG zone. As the first open generic Top Level Domain to implement DNSSEC, Public Interest Registry launched a cross industry coalition to execute an industry wide education and adoption plan within the Internet infrastructure community.

Believing this issue to be critical in the overall security and longevity of the Internet, Public Interest Registry plays a strategic role in efforts to understand and mitigate these implementation challenges, including active participation in ongoing DNSSEC design and deployment initiatives.