SECURITY REQUIREMENTS

For insurance providers and distributors, their customers and Internet users, .INSURANCE is a trusted, verified, more secure location online, free from many of the malicious activities that occur in other Internet web extension.

fTLD maintains high standards of security and takes an active approach to working with the global insurance community to enhance trust in the online financial system. fTLD employs enhanced consumer protection safeguards designed to mitigate cybersquatting, typosquatting, phishing and other harmful activities.

fTLD's Security Requirements were developed by its community-based Security Requirements Working Group, and are reviewed and updated as needed to address evolving community concerns.

fTLD's Security Requirements include:

- **Mandatory Verification and Re-Verification of Charter/Licensure for Regulated Entities** to ensure that only legitimate members of the global insurance community are awarded domain names.
- **Domain Name System Security Extensions** (DNSSEC) to ensure that Internet users are landing on participants' legitimate websites and not being misdirected to malicious ones.
- **Email Authentication** to mitigate spoofing, phishing and other malicious activities propagated through emails to unsuspecting users.
- **Multi-Factor Authentication** by registry and registrars to ensure that any change to registration data is made only by authorized users of the registered entity.
- **Strong Encryption** (i.e., TLS/SSL) to ensure security of communications over the Internet.
- **Prohibition of Proxy/Privacy Registration Services** to ensure full disclosure of domain registration information so bad actors cannot hide.
- **.INSURANCE domain names must use .INSURANCE DNS Name Servers** to ensure compliance with technical requirements.

# # #