REGISTRANT SECURITY REQUIREMENTS

REQUIREMENTS	✓ ACTION NEEDED	+ BENEFIT	WHO CAN HELP
PRELIMINARY VERIFICATION	**Verify:** 1. The domain name corresponds to your organization's legal name or brand; 2. Your organization is eligible to apply for the domain name; 3. The employee requesting the domain name on behalf of your organization is authorized to do so.	Verification prevents cybersquatting and makes it impossible for bad actors to register a domain name or contact your customers while posing as your organization.	• **Symantec (fTLD's verification partner)** • **Approved registrars**
1 **ZONE**	**Implement** Domain Name System Security Extensions (DNSSEC).	DNSSEC ensures that internet users are reaching your organization online and have not been redirected to a fraudulent website.	• **DNS provider** • **Approved registrars**
2 **ZONE**	**Ensure** authoritative name server host names are within the .INSURANCE domain zone.	In-zone name servers place the same security requirements on the name server as the .INSURANCE domain itself.	• **DNS provider** • **Approved registrars**
3 **ENCRYPTION**	**Obtain** a digital identity certificate.	Your .INSURANCE domain will resolve to HTTPS, which ensures all data is secure in transit.	• **Certificate authority** • **Registrar** • **Web host** • **Email provider**
4 **ENCRYPTION**	**Ensure** Transport Layer Security (TLS) has been implemented using version 1.1 or greater where possible.	TLS creates an encrypted connection, protecting your website and visitors, securing email communications, and supporting the safe and secure transmission of information and transactions.	• **Certificate authority** • **Registrar** • **Web host** • **Email provider**
5 **ENCRYPTION**	**Ensure** any URL redirections to a non-.INSURANCE domain begin from the HTTPS version of your .INSURANCE domain.	.INSURANCE domains are an HTTPS-only community, which ensures your customers and visitors get the security they expect, even during redirects to non-.INSURANCE domains.	• **DNS provider**
6 **EMAIL AUTHENTICATION**	**Publish in DNS as a text record:** 1. Domain-based Message Authentication, Reporting, and Conformance (DMARC) record; 2. Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) records when domain is used for email.	DMARC helps protect against phishing and spoofing, and increases the deliverability of email to your customers, especially when used in combination with SPF and/or DKIM.	• **Email security provider** • **Approved registrars**
7 **THIRD-PARTY PROVIDER**	**Ensure** vendors utilizing DNS resource records are currently using TLS and will implement DNSSEC by January 1, 2018.	Services provided by vendors working with a .INSURANCE domain will be more secure as they are held to the same security requirements as your organization.	• **Third-party providers (e.g., hosted email, content delivery networks, security and fraud services)**

For more detailed information on any required actions, please consult **fTLD's Technical Guide to Security Requirements**.
www.register.insurance

Created August 2017