### Registrant Security Requirements

**Verification** prevents cybersquatting and makes it impossible for bad actors to register a domain name or contact your customers while posing as your organization.

- **Approved registrars**

**Zone**

1. **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**

2. **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**

**Encryption**

1. **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**

2. **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**

**Email Authentication**

1. **Publish in DNS as a text record:**
   - Domain-based Message Authentication, Reporting, and Conformance (DMARC) record;
   - 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**

2. **Ensure** any vendors utilizing DNS resource records are currently using DNSSEC (#2) and TLS (#4).
   - 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 of these requirements, please consult fTLD’s Implementation Hub. [go.fTLD.com/Implementation-Hub](http://go.fTLD.com/Implementation-Hub)